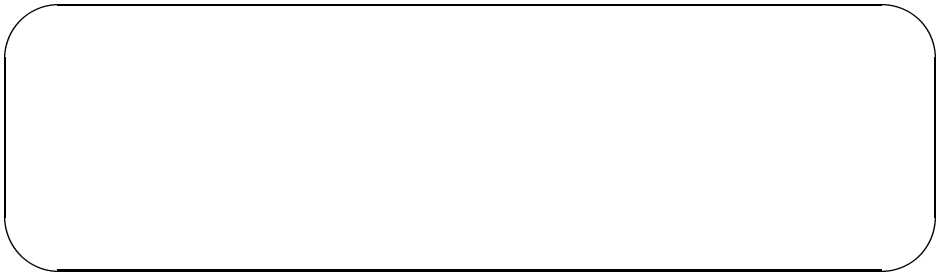
Universidade Estadual de Campinas
Instituto de Física Gleb Wataghin

Estados Quânticos Emaranhados

por

Gustavo Garcia Rigolin

Orientador: Carlos Ourivio Escobar



Tese submetida ao Instituto de Física Gleb Wataghin como parte dos requisitos necessários para a obtenção do título de Doutor em Física

Campinas, 15 de Abril de 2005.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IFGW - UNICAMP

R449e

Rigolin, Gustavo Garcia
Estados quânticos emaranhados / Gustavo Garcia Rigolin. -- Campinas, SP : [s.n.], 2005.

Orientador: Carlos Ourivio Escobar.
Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Física "Gleb Wataghin".

1. Emaranhamento quântico. 2. Teoria quântica da informação. 3. Mecânica quântica. I. Escobar, Carlos Ourivio. Universidade Estadual de Campinas. Instituto de Física "Gleb Wataghin". III. Título.

(vsv/ifgw)

- **Título em inglês:** Entangled quantum states
- **Palavras-chave em inglês (Keywords):**
  1. Quantum entanglement
  2. Quantum information theory
  3. Quantum mechanics
- **Área de concentração:** Física
- **Titulação:** Doutor em física
- **Banca examinadora:**
  Prof. Carlos Ourivio Escobar
  Prof. Amir Ordacgi Caldeira
  Prof. Guillermo Gerardo Cabrera Oyarzun
  Prof. Francisco Castilho Alcaraz
  Prof. Miled Hassan Youssef Moussa
- **Data da defesa:** 15.04.2005

UNICAMP
PÓS GRADUAÇÃO
IFGW
Instituto de Física Gleb Wataghin
C.P. 6165
CEP: 13083-970
Tel. (19) 3788-5305
e-mail: secpos@ifi.unicamp.br

MEMBROS DA COMISSÃO JULGADORA DA TESE DE DOUTORADO DE **GUSTAVO GARCIA RIGOLIN – RA 970790,** APRESENTADA E APROVADA AO INSTITUTO DE FÍSICA "GLEB WATAGHIN", DA UNIVERSIDADE ESTADUAL DE CAMPINAS, EM 31/03/2005.

COMISSÃO JULGADORA:

Prof. Dr. Carlos Ourivio Escobar (Orientador do Candidato)
DRCC/IFGW/UNICAMP

Prof. Dr. Francisco Castilho Alcaraz – IF/ UFSCAR/SP

Prof. Dr. Miled Hassan Youssef Moussa – DF/UFSCAR/SP

Prof. Dr. Amir Ordacgi Caldeira – DFMC/IFGW/UNICAMP

Prof. Dr. Guillermo G. Cabrera Oyarzún – DFMC/IFGW/UNICAMP

Agradecimentos

Não encontrei nenhum modo de fugir do lugar comum a todos os agradecimentos de teses e livros. Sendo assim, já começo por ele: Àqueles cujos nomes não estejam aqui, peço perdão. Nomes são muitos para serem lembrados e o esquecimento de alguns é natural. E também uma boa desculpa para evitar possíveis aborrecimentos oriundos daqueles cujos nomes realmente não merecem estar aqui. Por outro lado, existem alguns poucos cuja mera listagem de seus nomes não seria suficiente para exprimir o quão importantes foram na elaboração dessa tese. Para realçar a relevância dessas pessoas em minha vida, apresentá-los-ei grafando seus nomes com letras maiúsculas.

WILSON RIGOLIN e MARLI GARCIA RIGOLIN, meus pais. Agradeço pela confiança e incentivos depositados nessa minha aventura pelo mundo da Física. Não fosse por eles, não estaria aqui escrevendo essas linhas convicto de ter feito a escolha certa. Meus irmãos, GUILHERME e JULIANA GARCIA RIGOLIN, os quais sempre estiveram ao meu lado apoiando todas as minhas decisões.

CARLOS OURIVIO ESCOBAR, meu orientador, o qual me apresentou à Mecânica Quântica e a todos os seus desdobramentos, mostrou-me os melhores caminhos a serem seguidos e sempre esteve a meu lado mesmo quando optava por vielas não tão seguras. LÉA FERREIRA DOS SANTOS, que junto com meu orientador, ajudou-me a construir parte dos resultados apresentados nesta tese.

Não posso deixar de agradecer a todos meus professores da UNICAMP, tanto da graduação quanto da pós-graduação. Em especial, MARCUS ALOIZIO MARTINEZ DE AGUIAR e GUILLERMO G. CABRERA OYARZUN, por terem ensinado grande parte daquilo que sei sobre Mecânica Quântica.

Não poderia esquecer de meus amigos que, de um modo ou de outro, fizeram com que minha passagem por Campinas fosse a mais agradável possível. Faço questão de explicitar alguns nomes que sempre serão lembrados por mim: ANGEL PONTIN GARCIA, GABRIELA BEVILAQUA, RICARDO RANGEL BARRETO, JOÃO MARCELO SHIROMA, ROBERTO SOUZA GLÓRIA, CLÁUDIO CALAÇA JÚNIOR, LEANDRO OLIVEIRA, MARCO ANTÔNIO LEÃO, PAULO ABREU e DANILO BARRETO DE ARAÚJO, meus amigos e 'família' em Campinas. Também não poderia deixar de lembrar meus grandes amigos e colegas de formatura ou de curso, cuja companhia foi e é fundamental para mim: ALEXAN-

DRE REILY ROCHA, ANDRÉS ANIBAL RIEZNIK, CELSO CHIKAHIRO NISHI, DANIEL FERREIRA SILVA, FERNANDO DA ROCHA VAZ BANDEIRA DE MELO, JOSÉ ABEL HOYOS NETO, LUCIANA HENAUT e RODRIGO ANDRÉ CAETANO. E meus amigos de Cuiabá: ANDRÉ FRIZO BARBOSA, ARON MESQUITA PAIVA, AUGUSTO CÉSAR SILVA, JULIANO JUNDI e VILMAR BARBOSA JÚNIOR.

Finalmente, agradeço a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) por ter financiado, nestes quatro anos, meus estudos de doutoramento.

Estados Quânticos Emaranhados

por

Gustavo Garcia Rigolin

Resumo

Nesta tese estudamos em detalhes uma das características da Mecânica Quântica que mais destoa de nosso senso comum: o Emaranhamento Quântico. Apresentamos uma revisão dos principais resultados obtidos no entendimento do emaranhamento, em especial do emaranhamento bipartite. Definimos formalmente o que é um estado quântico emaranhado e, em seguida, apresentamos maneiras de qualificar e quantificar este emaranhamento. Mostramos uma nova maneira de se discernir entre estados emaranhados e não emaranhados agindo apenas localmente em um dos constituintes do sistema. Apresentamos dois limitantes inferiores que nos permitem estimar o grau de emaranhamento de qualquer estado Gaussiano de dois modos. A partir de uma generalização do protocolo de teletransporte de um qbit para N qbits, criamos uma medida de emaranhamento para sistemas multipartites que possui fácil interpretação física. Estudamos também as implicações do emaranhamento na dedução das relações de incerteza de Heisenberg para sistemas de partículas idênticas. Investigamos uma possível relação entre caos e emaranhamento bipartite, onde obtemos um decréscimo no emaranhamento conforme o sistema se torna mais caótico. Finalizamos essa tese apresentando um estudo sobre o comportamento do emaranhamento a temperaturas finitas, em especial para um sistema de dois qbits descritos pela Hamiltoniana de Heisenberg XYZ.

Entangled Quantum States

by

Gustavo Garcia Rigolin

Abstract

In this dissertation we study in details one of the most astonishing features of Quantum Mechanics which totally departs from our common sense: Quantum Entanglement. We review most of what is known in the study of entanglement, specially bipartite entanglement. We formally define entanglement and, whereupon, present how to qualify and quantify entangled states. We show a novel way to distinguish between entangled and non-entangled states acting locally onto one of the constituents of the system. Then, we present two lower bounds for the entanglement of formation for arbitrary two-mode Gaussian states. Generalizing the teleportation protocol to N qubits, we create a multipartite measure of entanglement which has a simple physical interpretation and is easily computed from the state describing the system. We also study the implications of entanglement in deducing uncertainty relations for identical particles. In addition to this, we investigate the influence of chaos on the degree of bipartite entanglement in spin chains. We show that chaos decreases entanglement. We end this dissertation presenting a study about the behavior of entanglement at finite temperatures, focusing at two qubits interacting via the Heisenberg XYZ Hamiltonian.

Notação e Convenção

A unidade fundamental de informação quântica é o qbit. Ele nada mais é do que um sistema quântico de dois níveis. Representamos o qbit $|\phi\rangle$ usando a notação já amplamente consagrada por todos que trabalham com Teoria Quântica de Informação:

$$|\phi\rangle = a|0\rangle + b|1\rangle,$$

onde $|a|^2 + |b|^2 = 1$ e

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

A matriz identidade e as matrizes de Pauli são

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ao nos referirmos a um produto tensorial ou soma direta de muitos termos usaremos as abreviações

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_N \quad \longrightarrow \quad \bigotimes_{j=1}^{N} \mathcal{H}_j,$$

$$S_1 \oplus S_2 \oplus \cdots \oplus S_N \quad \longrightarrow \quad \bigoplus_{j=1}^{N} S_j.$$

Sempre que um operador A for positivo, i. e., possuir todos seus autovalores positivos, escreveremos

$$A \geq 0.$$

Sumário

Lista de Figuras

Lista de Tabelas

Parte I

Fundamentos

Capítulo 1

Emaranhamento Quântico

1.1 Origens históricas

Após o final da década de 1920 a maioria dos princípios fundamentais, ou postulados, que norteiam a Mecância Quântica já estavam bem conhecidos. Dentre todos estes princípios existe um que chamou a atenção de alguns dos maiores pensadores da época. Modernamente este postulado pode ser assim resumido [25]:

> *A todo estado de um sistema físico podemos associar um vetor pertencente a um espaço de Hilbert. Esse vetor caracteriza completamente o sistema físico em questão.*

O conceito chave deste postulado é *espaço de Hilbert*. Um espaço de Hilbert é definido matematicamente como um espaço vetorial complexo, completo e provido de uma métrica (distância entre vetores), a qual é obtida por meio de um produto escalar. Concentremo-nos em analisar detalhadamente o fato de o espaço de Hilbert ser um espaço vetorial. Num espaço vetorial $\mathcal{H}$ qualquer combinação linear entre dois elementos deste espaço, $|\psi_1\rangle$ e $|\psi_2\rangle$ por exemplo, é também um elemento pertencente a este espaço vetorial. Em símbolos temos:

> Se $|\psi_1\rangle$ e $|\psi_2\rangle \in \mathcal{H}$, então $|\psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle \in \mathcal{H}$, onde a e b são números complexos.

Devido a sua extrema importância na Física, essa propriedade recebeu status de princípio. Ela é conhecida como *princípio da superposição* ou da *linearidade* da Mecânica Quântica. As conseqüências experimentais e até mesmo filosóficas oriundas deste princípio são impressionantes. Ainda hoje especialistas se espantam com estes resultados e 'disputas' sobre sua interpretação física não são difíceis de ocorrerem de tempos em tempos.

A situação se torna mais fantástica quando aplicamos o princípio da superposição a um sistema físico composto por mais de uma parte. Em 1935, Albert Einstein, Boris Podolsky e Nathan Rosen apresentaram num belíssimo artigo [30] as implicações lógicas do princípio da superposição quando aplicado na descrição de um sistema composto. Fazendo uso desse princípio, de uma definição muito razoável de realidade física e da impossibilidade de transmissão de sinais superluminais (hipótese de localidade), Einstein, Podolsky e Rosen (EPR) demonstraram a incompletude da Mecânica Quântica. Apesar da clareza da análise de EPR, Niels Bohr, num artigo muito hermético [18], tentou refutar os argumentos expostos por EPR.[1]

Também em 1935, e motivado pelas idéias de EPR, Erwin Schrödinger apresentou [82] de maneira eloqüente as conseqüencias do princípio da superposição quando aplicado a um sistema composto de duas partes. Fazendo-se uso de um experimento imaginário, Schrödinger realçou que poderíamos ter situações bizarras num mundo macroscópico descrito pela Mecânica Quântica. Para entender o argumento de Schrödinger, imaginemos uma situação na qual uma gata se encontre dentro de uma caixa completamente fechada. A gata pode ou estar viva ($|\text{Viva}\rangle$) ou morta ($|\text{Morta}\rangle$). Dentro desta caixa, há também um átomo instável ($|\text{átomo } 1\rangle$), o qual pode ter decaído para um átomo mais estável ($|\text{átomo } 2\rangle$). Suponhamos que a energia liberada nessa transição seja suficiente para ativar um mecanismo que libere um gás altamente tóxico, o qual mata rapidamente a gata. A Mecânica Quântica nos diz apenas a probabilidade de o isótopo decair, nos proibindo de prever deterministicamente quando isso ocorre. Dessa forma, aceitando a validade do princípio da superposição chegamos a conclusão de que o estado do sistema composto pela gata e pelo átomo é

$$|\Psi\rangle = a|\text{átomo } 1\rangle\,|\text{Viva}\rangle + b|\text{átomo } \ 2\rangle\,|\text{Morta}\rangle.$$

Interpretamos o módulo quadrado dos coeficientes a e b como sendo a probabilidade de o átomo não decair ou decair, respectivamente.

Este resultado nos diz que temos uma superposição de dois estados macroscópicos distintos da gata: gata viva e gata morta.[2] Para realçar a ligação íntima entre os dois subsistemas (gata mais átomo) que compõem o estado $|\Psi\rangle$, Schrödinger usou o termo *Verschränkung*. Este termo foi traduzido do alemão para o inglês como *entanglement* e para o português como emaranhamento.

[1] Acredito que Bohr, em sua resposta [18] a EPR, abdicou da possibilidade de uma realidade física independente de um observador, a fim de conseguir restituir a completude da Mecânica Quântica. Hoje é mais razoável abandonar a idéia de localidade absoluta da Mecânica Quântica para restaurar sua completude. Há algo de não-local nesta teoria que, no entanto, não pode ser usado para transmissão superluminal de informação clássica.

[2] Essa situação surreal de uma superposição macroscópica de dois estados distintos pode ser evitada se lançamos mão de uma interpretação estatística da Mecânica Quântica. Esse 'paradoxo' só ocorre se insistimos na visão de que um estado quântico descreve sistemas individuais [6].

Apesar de todas estas implicações, os argumentos utilizados por EPR e Schrödinger, muito provavelmente por não proporcionarem nenhuma previsão quantitativa, ficaram restritos a discussões sobre os aspectos ontológicos da Mecânica Quântica. E por muito tempo se pensou que questões como realismo e não-localidade ficariam restritas apenas ao mundo da filosofia. Contudo, no ano de 1964, John S. Bell [9] provou o contrário. Por meio de uma construção muito engenhosa, Bell mostrou que o princípio da superposição aplicado a sistemas compostos produz previsões quantitativas que, se confirmadas experimentalmente, provariam aspectos não-locais da Mecânica Quântica.

Bell só conseguiu quantificar esse aspecto da não-localidade pois utilizou em sua análise, influenciado por David Bohm [17], um sistema composto mais simples do que o usado por EPR. O sistema físico utilizado por EPR era impossível de ser produzido na prática e introduzia complicações desnecessárias, obscurecendo os aspectos realmente relevantes em sua prova da incompletude da Mecânica Quântica. Na verdade, Bell usou em sua análise o sistema quântico composto mais simples possível, i. e., um par de sistemas de dois níveis. Ao estudarmos, por exemplo, o spin de dois elétrons ou a polarização de dois fótons, lidamos com pares de sistemas de dois níveis.

Apenas no início da década de 1980 foram realizadas as primeiras verificações experimentais que confirmaram esses aspectos não-locais da Mecânica Quântica. Em particular, experimentos decisivos foram realizados por Alain Aspect e colaboradores [4, 5], comprovando quase[3] que definitivamente a não-localidade da Mecânica Quântica.

Por fim, a partir da década de 1990, ficou claro que o emaranhamento, além de propiciar discussões quantitativas sobre os fundamentos da física, pode ser encarado como um *recurso* disponível na Natureza [63, 19]. Os estados emaranhados são também ferramentas que podem ser utilizadas para realizar mais eficientemente tarefas que até então eram implementadas usando-se apenas recursos clássicos. Dois exemplos muito famosos e que serão discutidos nesta tese são a codificação superdensa [12] (*superdense coding*) e o teletransporte quântico [11] (*quantum teleportation*).

1.2 O que é emaranhamento

Conforme exposto na Sec. 1.1, o emaranhamento surge naturalmente ao aplicarmos o princípio da superposição a sistemas físicos compostos. Assim como um sistema composto pode ter dois ou mais constituintes, costuma-se também classificar o emaranhamento de um sistema pelo número de subsistemas que estão emaranhados.

[3] Digo 'quase' pois, devido a baixa eficiência dos detectores, é possível a construção de modelos locais, porém muito artificiais, que expliquem os resultados empíricos.

Por exemplo, o singleto [19], $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$, é um caso típico de estado emaranhado formado por dois subsistemas, ou emaranhamento bipartite.[4] Para emaranhamento de mais de dois subsistemas usamos a notação emaranhamento multipartite. Em especial, ao lidarmos com três subsistemas emaranhados, podemos usar a terminologia tripartite. O exemplo mais famoso dessa classe de emaranhamento é o estado Greenberger-Horne-Zeilinger [40], $|GHZ\rangle = (1/\sqrt{2})(|000\rangle - |111\rangle)$.

O conceito de emaranhamento se aplica também a sistemas de mais de dois níveis e, em especial, a sistemas descritos por variáveis contínuas. O exemplo mais famoso de estado emaranhado pertencente a esta classe foi apresentado por EPR em seu célebre artigo [30]:

$$\Psi(x_1, x_2) = \int_{-\infty}^{\infty} \mathrm{e}^{(2\pi \mathrm{i}/h)(x_1 - x_2 + x_0)p} \mathrm{d}p,$$

onde h é a constante de Planck e x_0 é uma constante qualquer. Este estado corresponde a duas partículas que se afastam com momento p. Um outro exemplo de emaranhamento de estados descritos por variáveis contínuas é o estado espremido de dois modos (*two-mode squeezed state*):

$$|\Psi_s(r)\rangle = \frac{1}{\cosh(r)} \sum_{n=0}^{\infty} \tanh^n(r)\, |n\rangle_1 \otimes |n\rangle_2 \,,$$

onde $|n\rangle$ é o n-ésimo estado de Fock e $r > 0$ é o parâmetro de *squeezing*. Veremos no Cap. 3 que o estado EPR acima é um estado espremido com $r \to \infty$.

Formalmente, define-se emaranhamento para estados puros da seguinte forma:

Definição 1 *Seja um sistema quântico composto de N subsistemas tal que o espaço de Hilbert associado a ele é $\mathcal{H} = \bigotimes_{j=1}^{N} \mathcal{H}_j$, onde $\mathcal{H}_j$ é o espaço de Hilbert associado a cada subsistema. Se $|\Psi\rangle \in \mathcal{H}$ é o estado que descreve este sistema, então ele não está emaranhado se, e somente se, podemos escrevê-lo como $|\Psi\rangle = \bigotimes_{j=1}^{N} |\psi_j\rangle$, onde $|\psi_j\rangle \in \mathcal{H}_j$.*

Alguns exemplos de estados puros não-emaranhados são:

$$\begin{aligned} |\psi\rangle &= |00\rangle = |0\rangle_1 \otimes |0\rangle_2, \\ |\phi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1) \otimes \frac{1}{\sqrt{2}}(|0\rangle_2 - |1\rangle_2), \\ \chi(x_1, x_2) &= \left(\frac{2}{\pi a^2}\right)^{1/4} \mathrm{e}^{\mathrm{i}k_c x_1} \mathrm{e}^{-x_1^2/a^2} \otimes \left(\frac{2}{\pi a^2}\right)^{1/4} \mathrm{e}^{-\mathrm{i}k_c x_2} \mathrm{e}^{-x_2^2/a^2}. \end{aligned}$$

[4] A nomenclatura em inglês é *bipartite entanglement*. Uma tradução aceitável seria emaranhamento bipartido. No entanto, como a Academia Brasileira de Letras reconhece o vocábulo bipartite como sendo legítimo, optei por este último para diferenciar a separação física dos dois subsistemas (bipartido) do estado quântico (bipartite) que os descreve.

O estado χ acima representa dois pacotes Gaussianos com largura da ordem de a, onde o primeiro move-se com momento $\hbar k_c$ e o segundo com momento $-\hbar k_c$.

A definição acima, como podemos ver, não se aplica a estados mistos. Para remediar essa situação precisamos de uma formulação mais geral de emaranhamento, válida tanto para estados puros quanto mistos [65]:

Definição 2 *Seja um sistema quântico composto de N subsistemas descrito por uma matriz densidade $\rho \in \bigotimes_{j=1}^{N} \mathcal{A}_j$, onde $\mathcal{A}_j$ é o espaço de Hilbert formado por todos os operadores que atuam em $\mathcal{H}_j$. Dizemos que ρ representa um sistema não emaranhado se, e somente se, ela pode ser escrita, para algum k, como uma soma de produtos diretos:*

$$\rho = \sum_{i=0}^{k} p_i \bigotimes_{j=1}^{N} \rho_i^j = \sum_{i=0}^{k} p_i \left(\rho_i^1 \otimes \rho_i^2 \otimes \cdots \otimes \rho_i^{N-1} \otimes \rho_i^N \right),$$

onde $p_i > 0$, $\sum_{i=0}^{k} p_i = 1$, e $\rho_i^j \in \mathcal{A}_j$.

O estado acima é o estado mais geral que pode ser preparado por N sujeitos separados e que recebem instruções de uma fonte comum. Dizemos que a matriz ρ acima é a mais geral que pode ser construída via LOCC (Operações Locais e Comunicação Clássica). Por operações locais entendemos todas as manipulações permitidas pela Mecânica Quântica que o observador j possa realizar no seu subsistema. Exemplos de operações locais são transformações unitárias, medidas projetivas de von Neumann e medidas valoradas por operadores positivos (POVM)[5]. Agora, ao nos referirmos à comunicação clássica, entendemos que os N sujeitos podem se comunicar utilizando-se de qualquer mecanismo clássico (não-quântico). Exemplos de canais clássicos de comunicação são o telégrafo, o telefone e o e-mail. Alguns exemplos de estados mistos não emaranhados são:[6]

$$\begin{aligned} \varrho &= \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|), \\ \sigma &= \frac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|), \\ \varsigma &= \frac{1}{3}(|000\rangle\langle 000| + |111\rangle\langle 111| + |001\rangle\langle 001|). \end{aligned} \tag{1.1}$$

É interessante observar que ambas as definições anteriormente apresentadas dizem o que é emaranhamento definindo, na verdade, um estado não emaranhado ou separável. E mais, essas duas definições não são muito práticas para julgar se um dado estado quântico está ou não emaranhado. Muitas vezes, quando lidamos com estados separáveis, percebemos ser muito difícil encontrar uma decomposição de $|\Psi\rangle$

[5] Veja Apêndice A para uma breve introdução sobre POVM.

[6] De agora em diante, simplificarei a notação representando matrizes densidade do tipo $|0\rangle_1 \otimes |1\rangle_2 \, {}_1\langle 0| \otimes {}_2\langle 1|$ como $|01\rangle\langle 01|$.

(ou de ρ) retratando explicitamente este fato. Dizemos, por isso, que as definições acima de emaranhamento não são operacionais. Mas felizmente existem critérios práticos que nos dizem se temos ou não emaranhamento. Discutiremos, com calma, alguns desses critérios no Cap. 2, onde também apresentaremos vários exemplos de estados emaranhados.

1.3 Qual a utilidade do emaranhamento

Além de ajudar no entendimento da Mecânica Quântica, muitas vezes provocando discussões acirradíssimas, os estados quânticos emaranhados são extremamente úteis. Se sabiamente manipulados, eles produzem resultados práticos fantásticos. Muitas tarefas até então consideradas intratáveis classicamente, ou até mesmo impossíveis de serem realizadas, tornaram-se, devido ao uso de estados emaranhados, factíveis.

Apesar da existência de algumas discussões [62] sobre a real importância do emaranhamento na implementação de algoritmos quânticos, como o da fatoração de números primos (algoritmo de Shor [84]) ou o de busca (algoritmo de Grover [41]), é cada vez mais consensual que o emaranhamento é um ingrediente indispensável na construção de um computador quântico escalável [22].[7]

Mas existem, no entanto, tarefas quânticas onde é inegável a importância do emaranhamento.[8] Apresentamos, a seguir, algumas das mais úteis e interessantes aplicações dos estados emaranhados. Queremos lembrar, também, que algumas dessas aplicações serão mais extensivamente discutidas em capítulos vindouros.

1.3.1 Codificação superdensa

Em 1992 Bennett e Wiesner [12] propuseram um protocolo que permitia condensar a transmissão de informação clássica (cbits, ou simplesmente bits) usando estados quânticos emaranhados. Posteriormente este protocolo ficou conhecido como codifição superdensa. Ele mostra de maneira clara como estados maximamente emaranhados podem aumentar a capacidade de comunicação entre dois pares. Num canal ideal clássico de comunicação, a transmissão de dois bits de informação requer a manipulação e a transmissão de pelo menos duas partículas ou entidades físicas, as quais são usadas na codificação da informação transmitida. Isto significa que se Alice deseja transmitir dois bits a Bob, ela precisa enviar duas partículas a ele. No entanto, caso Alice e Bob compartilhem um estado de Bell, i. e., um estado maxima-

[7] Um computador quântico é escalável se podemos aumentar o número de qbits utilizados em sua confecção mantendo suas propriedades originais.

[8] Muitas delas são de fácil assimilação e devem, na minha opinião, serem incorporadas no ensino de Mecânica Quântica elementar, pois realçam belamente aspectos fundamentais da teoria.

mente emaranhado, ela pode transmitir dois bits de informação a Bob manipulando e enviando apenas um qbit. Veja Fig. 1.1.

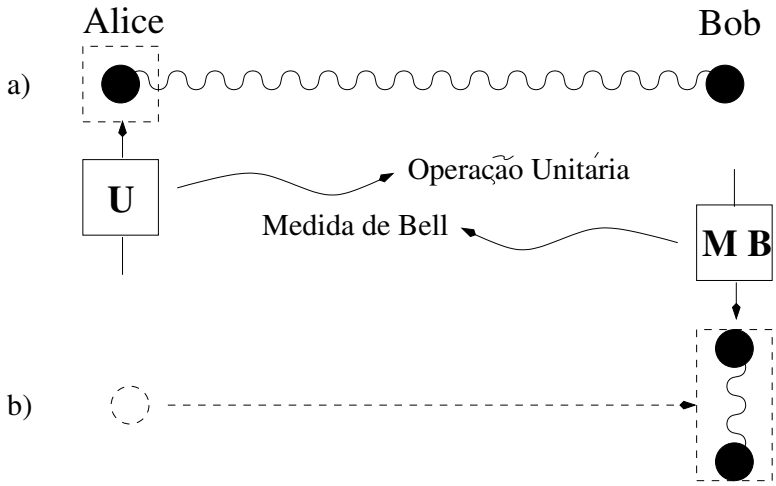


Figura 1.1: a) Alice opera localmente em seu qbit, gerando um dos quatro estados de Bell, e o envia a Bob. b) Bob, por sua vez, faz uma medida de Bell nos dois qbits, lendo a mensagem de dois bits enviada por Alice. No final do processo, Alice enviou apenas um qbit.

Suponha que Alice e Bob inicialmente compartilhem o estado de Bell $|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$, o qual pode representar, por exemplo, a polarização de dois fótons. O primeiro fóton está com Alice e o segundo com Bob. Operando localmente sobre seu fóton, Alice pode gerar quatro estados ortogonais. Estes estados são, na verdade, os quatro estados de Bell. As transformações unitárias locais e os estados gerados por estas transformações são: $I|\Phi^+\rangle = |\Phi^+\rangle$, $\sigma_1^z|\Phi^+\rangle = |\Phi^-\rangle$, $\sigma_1^x|\Phi^+\rangle = |\Psi^+\rangle$, e $i\sigma_1^y|\Phi^+\rangle = |\Psi^-\rangle$. Aqui σ são as matrizes de Pauli, I é a matriz identidade e o subíndice indica que o qbit 1 está com Alice. Os estados de Bell são:

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{1.2}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{1.3}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{1.4}$$

Após implementar uma dessas quatro operações unitárias locais, Alice envia seu qbit a Bob, o qual, realizando uma medida de Bell nos dois qbits descobre qual estado Alice enviou. Uma medida de Bell é aquela que permite diferenciar entre os quatro estados de Bell. Dessa forma Bob, usando a convenção da Tab. 1.1, lê a mensagem de dois bits.

Tabela 1.1: Nas colunas ímpares temos os estados de Bell e nas colunas pares a codificação preestabelecida entre Bob e Alice, associando cada estado de Bell a uma mensagem de dois bits.

Estado	Convenção	Estado	Convenção
$\|\Phi^+\rangle$	00	$\|\Phi^-\rangle$	01
$\|\Psi^+\rangle$	10	$\|\Psi^-\rangle$	11

1.3.2 Teletransporte quântico

Um ano após à apresentação da codificação superdensa, Bennett *et al.* [11] descobriram uma das mais espantosas aplicações da Mecânica Quântica, a qual recebeu o nome de teletransporte quântico. Através de um estado de Bell, apelidado por eles de canal EPR ($|\Phi^+\rangle = (1/\sqrt{2})\ (|00\rangle + |11\rangle)$, por exemplo), estes autores mostraram que é possível transmitir toda informação contida em um qbit $|\phi\rangle = a|0\rangle + b|1\rangle$ de uma região do espaço-tempo (Alice) para outra (Bob).

Na verdade, não ocorre um teletransporte como vislumbrado por muitos escritores de ficção científica. Ou seja, o qbit de Alice não é 'desmaterializado' e em seguida 'materializado' onde Bob se encontra. A entidade que é teletransportada neste processo é o estado quântico, ou numa visão de teoria de informação, toda informação nele contida. Alice inicialmente dispunha de uma partícula descrita pelo estado $|\phi\rangle$ e, no final do protocolo, esse estado passa a descrever uma partícula de Bob. A partícula de Alice, por sua vez, passa a ser descrita não mais por esse estado, mas por uma mistura estatística máxima. Mais ainda, essa transmissão não é instantânea, pois Bob necessita receber dois bits clássicos de Alice para finalizar o protocolo. E como informação clássica não viaja mais rápido do que um sinal luminoso, a causalidade relativística é preservada. Também após o término do processo, Alice e Bob não mais compartilham um estado de máximo emaranhamento. Este estado é gasto para efetuar o teletransporte. Podemos entender o processo como se toda informação de um qbit fosse separada em duas partes, uma clássica e outra quântica. A parte clássica é transmitida pelos dois bits enviados por Alice, e a parte quântica viaja pelo canal EPR , consumindo um estado de Bell ou um ebit (*entangled bit*).

$$1 \text{ qbit} \prec 1 \text{ ebit} + 2 \text{ bits}. \tag{1.5}$$

O símbolo 'precede' foi usado para realçar que não se trata de uma igualdade, muito menos uma equivalência. Queremos apenas realçar que o estado de um qbit num determinado local é 'destruído' e transmitido a outra região às custas de um ebit e dois bits de informação. A Fig. 1.2 faz uma representação esquemática do protocolo de teletransporte.

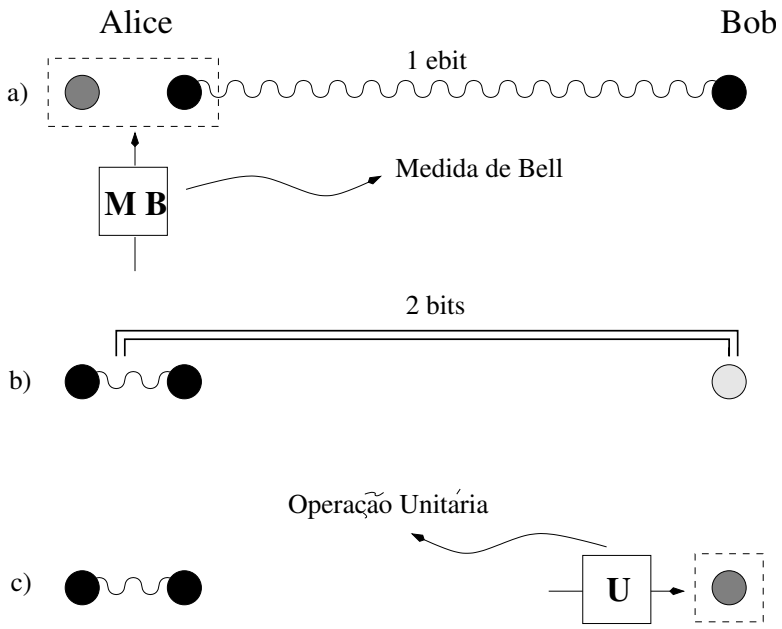


Figura 1.2: a) Alice faz uma medida de Bell nos seus dois qbits. b) Alice envia dois bits de informação a Bob. c) Após receber a mensagem de Alice, Bob opera localmente em seu qbit, completando o protocolo.

Formalmente o teletransporte de um qbit $|\phi\rangle = a|0\rangle + b|1\rangle$ é realizado do seguinte modo. Alice e Bob inicialmente compartilham um estado bipartite de máximo emaranhamento, i. e., um estado de Bell: $|\Psi^-\rangle = (1/\sqrt{2})\ (|01\rangle - |10\rangle)$. Este é o canal quântico necessário para o teletransporte. O sistema composto pelo qbit cujo estado será teleportado e pelo estado EPR antes de qualquer medida feita por Alice é escrito como

$$\begin{aligned} |\Phi\rangle &= |\phi\rangle \otimes |\Psi^-\rangle, \\ |\Phi\rangle &= \frac{a}{\sqrt{2}}\left(|001\rangle - |010\rangle\right) + \frac{b}{\sqrt{2}}\left(|101\rangle - |110\rangle\right), \end{aligned} \tag{1.6}$$

onde convencionamos que os primeiros dois qbits pertencem a Alice e o terceiro a Bob ($|AAB\rangle$, $A \rightarrow$ Alice e $B \rightarrow$ Bob). Reescrevendo a Eq. (1.6) em termos dos quatro estados de Bell $|\Phi^\pm\rangle = (1/\sqrt{2})\ (|00\rangle \pm |11\rangle)$ e $|\Psi^\pm\rangle = (1/\sqrt{2})\ (|01\rangle \pm |10\rangle)$ obtemos

$$\begin{aligned} |\Phi\rangle &= \frac{1}{2}\big\{|\Psi^-\rangle(-a|0\rangle - b|1\rangle) + |\Psi^+\rangle(-a|0\rangle + b|1\rangle) \\ &\quad + |\Phi^-\rangle(a|1\rangle + b|0\rangle) + |\Phi^+\rangle(a|1\rangle - b|0\rangle)\big\}. \end{aligned} \tag{1.7}$$

Alice agora realiza uma medida de Bell no qbit a ser teletransportado e no seu qbit do estado de Bell compartilhado com Bob. Ela obviamente não tem controle

sobre o resultado de sua medida. Alice tem 1/4 de chance de obter quaisquer dos quatro estados de Bell. Após esta medida de Bell, o estado que descreve o conjunto dos três qbits só pode ser uma das quatro possibilidade expostas na Tab. 1.2:

Tabela 1.2: Na primeira coluna temos o resultado da medida feita por Alice e na segunda o estado dos três qbits condicionados ao estado de Bell obtido por Alice.

Resultado de Alice	Estado dos três qbits
$\|\Psi^-\rangle$	$\|\Psi^-\rangle \otimes (-a\|0\rangle - b\|1\rangle)$
$\|\Psi^+\rangle$	$\|\Psi^+\rangle \otimes (-a\|0\rangle + b\|1\rangle)$
$\|\Phi^-\rangle$	$\|\Phi^-\rangle \otimes (a\|1\rangle + b\|0\rangle)$
$\|\Phi^+\rangle$	$\|\Phi^+\rangle \otimes (a\|1\rangle - b\|0\rangle)$

Alice, após a medida, comunica classicamente seu resultado a Bob. De posse desses dois bits de informação, Bob sabe em qual dos quatro estados expostos na Tab. 1.2 encontra-se sua partícula. Dessa forma, ele finaliza o protocolo aplicando apropriadamente uma operação unitária ao seu estado, obtendo finalmente $|\phi\rangle$. Qual operação Bob deve aplicar depende de qual resultado Alice obteve em sua medida de Bell. Veja a Tab. 1.3.

Tabela 1.3: As transformações unitárias que Bob deve realizar em seu qbit, condicionadas ao resultado da medida de Alice, para completar o protocolo de teletransporte. I é a matriz identidade e σ são as matrizes de Pauli.

Resultado de Alice	Operação de Bob	Qbit de Bob
$\|\Psi^-\rangle$	I	$I(-a\|0\rangle - b\|1\rangle) = -\|\phi\rangle$
$\|\Psi^+\rangle$	σ^z	$\sigma^z(-a\|0\rangle + b\|1\rangle) = -\|\phi\rangle$
$\|\Phi^-\rangle$	σ^x	$\sigma^x(a\|1\rangle + b\|0\rangle) = \|\phi\rangle$
$\|\Phi^+\rangle$	$\sigma^z\sigma^x$	$\sigma^z\sigma^x(a\|1\rangle - b\|0\rangle) = \|\phi\rangle$

A importância dos dois bits clássicos para finalizar com sucesso o protocolo pode ser vista da seguinte forma. Suponhamos que Bob não receba essa informação. Assim, ele não pode nada afirmar sobre qual foi o resultado da medida de Alice. Dessa forma, usando a Eq. (1.7), o estado dos três qbits, para Bob, pode ser escrito

como,

$$\begin{aligned}
\rho &= |\Phi\rangle\langle\Phi| \\
&= \frac{1}{4}\left[|\Psi^-\rangle\langle\Psi^-| \otimes (-a|0\rangle - b|1\rangle)\,(-a^*\langle 0| - b^*\langle 1|)\right. \\
&\quad +|\Psi^+\rangle\langle\Psi^+| \otimes (-a|0\rangle + b|1\rangle)\,(-a^*\langle 0| + b^*\langle 1|) \\
&\quad +|\Phi^-\rangle\langle\Phi^-| \otimes (a|1\rangle + b|0\rangle)\,(a^*\langle 1| + b^*\langle 0|) \\
&\quad \left.+|\Phi^+\rangle\langle\Phi^+| \otimes (a|1\rangle - b|0\rangle)\,(a^*\langle 1| - b^*\langle 0|)\right] \\
&\quad + \text{termos cruzados do tipo } |\Psi^-\rangle\langle\Psi^+|, |\Psi^-\rangle\langle\Phi^+|, ... \\
&= \frac{1}{4}\left[|\Psi^-\rangle\langle\Psi^-| \otimes \left(|a|^2|0\rangle\langle 0| + ab^*|0\rangle\langle 1| + a^*b|1\rangle\langle 0| + |b|^2|1\rangle\langle 1|\right)\right. \\
&\quad +|\Psi^+\rangle\langle\Psi^+| \otimes \left(|a|^2|0\rangle\langle 0| - ab^*|0\rangle\langle 1| - a^*b|1\rangle\langle 0| + |b|^2|1\rangle\langle 1|\right) \\
&\quad +|\Phi^-\rangle\langle\Phi^-| \otimes \left(|a|^2|1\rangle\langle 1| + ab^*|1\rangle\langle 0| + a^*b|0\rangle\langle 1| + |b|^2|0\rangle\langle 0|\right) \\
&\quad \left.+|\Phi^+\rangle\langle\Phi^+| \otimes \left(|a|^2|1\rangle\langle 1| - ab^*|1\rangle\langle 0| - a^*b|0\rangle\langle 1| + |b|^2|0\rangle\langle 0|\right)\right] \\
&\quad + \text{termos cruzados do tipo } |\Psi^-\rangle\langle\Psi^+|, |\Psi^-\rangle\langle\Phi^+|, ... \qquad (1.8)
\end{aligned}$$

Tomando o traço sobre os qbits de Alice na Eq. (1.8) obtemos o estado que descreve o qbit de Bob. Note que os termos cruzados não contribuem no cálculo deste traço.

$$\begin{aligned}
\rho^B &= \mathrm{Tr}_{1,2}[\rho] \\
&= \langle\Psi^-|\rho|\Psi^-\rangle + \langle\Psi^+|\rho|\Psi^+\rangle + \langle\Phi^-|\rho|\Phi^-\rangle + \langle\Phi^+|\rho|\Phi^+\rangle \\
&= \frac{1}{2}\left(|a|^2 + |b|^2\right)|0\rangle\langle 0| + \frac{1}{2}\left(|a|^2 + |b|^2\right)|1\rangle\langle 1| \\
&= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|, \qquad (1.9)
\end{aligned}$$

pois $|a|^2 + |b|^2 = 1$, dada a normalização do estado $|\phi\rangle$ a ser teletransportado.

Vemos claramente que o estado ρ^B do qbit de Bob é uma mistura estatística máxima. Agora, se Bob recebe os dois bits de informação de Alice, seu qbit é descrito por um dos quatro estados apresentados na Tab. 1.2. Neste caso, seu qbit é um estado puro e não está emaranhado com nenhum qbit de Alice, ilustrando que o canal quântico de comunicação é destruído após Alice realizar sua medida de Bell. Posto de outra forma, o resultado expresso pela Eq. (1.9) mostra a importância da transmissão dos dois bits informando Bob sobre o resultado da medida de Alice para que o teletransporte seja bem sucedido.

Para finalizar, vale a pena realçar que ao terminar o processo de teletransporte, o estado que descreve o qbit 1 (aquele originalmente com Alice e cujo estado foi transmitido a Bob) não mais é descrito pelo estado $|\phi\rangle$. Isto pode ser visto diretamente pelo fato de que após a medida de Bell ser feita por Alice, os dois qbits pertecentes a ela passam a ser descritos por um dos quatro estados de Bell, $\rho^A_{1,2} = |\Phi^\pm\rangle\langle\Phi^\pm|$ ou $\rho^A_{1,2} = |\Psi^\pm\rangle\langle\Psi^\pm|$. Calculando o traço com relação ao qbit 2 vemos que $\rho^A_1 =$

$\mathrm{Tr}_2[\rho^A_{1,2}] = (1/2)(|0\rangle\langle 0| + |1\rangle\langle 1|)$, e não $|\phi\rangle\langle\phi| = \big(|a|^2|0\rangle\langle 0| + ab^*|0\rangle\langle 1| + a^*b|1\rangle\langle 0| + |b|^2|1\rangle\langle 1|\big)$. Este resultado já era esperado pois se tanto o qbit 1 quanto o qbit 3 de Bob fossem descritos por $|\phi\rangle$, teríamos uma máquina de clonagem de estados quânticos, fato este proibido pelo teorema da não-clonagem [98]. Uma demonstração deste último teorema é apresentada no Apêndice B.

1.3.3 Criptografia quântica

Desde os primórdios da civilização o homem sempre se deparou com o problema de transmitir secretamente informações importantes. A ciência que estuda essa arte de se comunicar confidencialmente, tendo a certeza de que somente as partes interessadas terão acesso a informação, recebe o nome de criptografia.

Muitos dos modernos protocolos de criptografia anunciam publicamente o algoritmo utilizado para encriptar e decriptar a mensagem. A segurança desses protocolos se baseia apenas em uma longa sequência de números aleatórios que o emissor (Alice) e o receptor (Bob) da mensagem devem compartilhar em segredo. Ou seja, o sucesso desses protocolos depende exclusivamente da capacidade de os envolvidos na comunicação serem capazes de compartilhar essa sequência de números aleatórios, também conhecida como chave criptográfica ou apenas chave, certificando-se de que ninguém mais consiga ter acesso a ela.

Para compartilhar essa chave, Alice e Bob usam um canal clássico de comunicação. Por mais seguro que ele seja, em princípio ele pode ser monitorado por algum agente externo (Eva) sem que Alice e Bob percebam. Eva pode obter a chave, sem Alice e Bob notarem, pois qualquer informação clássica pode ser clonada. Eva pode, por exemplo, interceptar a chave enviada por Alice a Bob e, em seguida, reenviá-la para ele.

Agora, se Alice e Bob usarem um canal quântico de comunicação, eles terão certeza de que a transmissão da chave foi realizada com segurança total, ou de que ela foi interceptada por Eva. Essa segurança é baseada nas leis da Mecância Quântica e, desde que aceitemos que ela é uma teoria completa no sentido de EPR, não há meio de se burlar essa segurança.

O primeiro protocolo de criptografia quântica [10], ou mais corretamente, protocolo de distribuição de chaves quânticas, não se utilizou de estados emaranhados. Entretanto, Artur K. Ekert criou um protocolo [31] que faz uso do estado de Bell $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$ para transmitir chaves quânticas. Este protocolo, cuja segurança está baseada na violação da desigualdade de Clauser-Horne-Shimony-Holt (CHSH) [24], será apresentado em seguida.

Alice e Bob dispõem de um canal quântico que emite singletos. Alice recebe um dos constituintes do singleto enquanto Bob recebe o outro. Vamos supor, sem perder em generalidade, que as partículas viajam até Alice e Bob ao longo da direção z.

Ao receberem-nas, Alice e Bob medem o spin de suas partículas ao longo da direção $\mathbf{a}_i$ e $\mathbf{b}_j$, respectivamente. O vetor $\mathbf{a}_i$ ($\mathbf{b}_j$) é unitário e caracterizado pelos ângulos polar θ_i^a (θ_j^b) e azimutal φ_i^a (φ_j^b). Tanto Alice quanto Bob orientam, aleatoriamente para cada medida de spin, seus detectores ao longo de três vetores contidos no plano xy, i. e. $\theta_i^a = \theta_j^b = \pi/2$. Os ângulos azimutais que caracterizam estes vetores são: $\varphi_1^a = 0$, $\varphi_2^a = \pi/4$ e $\varphi_3^a = \pi/2$ para Alice, e $\varphi_1^b = \pi/4$, $\varphi_2^b = \pi/2$ e $\varphi_3^b = 3\pi/4$ para Bob.

A partir destes vetores, podemos definir o coeficiente de correlação de medidas de spin ao longo das direções $\mathbf{a}_i$ e $\mathbf{b}_j$ como sendo

$$E(\mathbf{a}_i, \mathbf{b}_j) = P_{00}(\mathbf{a}_i, \mathbf{b}_j) + P_{11}(\mathbf{a}_i, \mathbf{b}_j) - P_{01}(\mathbf{a}_i, \mathbf{b}_j) - P_{10}(\mathbf{a}_i, \mathbf{b}_j). \tag{1.10}$$

Aqui $P_{00}(\mathbf{a}_i, \mathbf{b}_j), P_{11}(\mathbf{a}_i, \mathbf{b}_j), P_{01}(\mathbf{a}_i, \mathbf{b}_j)$ e $P_{10}(\mathbf{a}_i, \mathbf{b}_j)$ representam a probabilidade de obtermos os resultados $(+1,+1), (-1,-1), (+1,-1)$ e $(-1,+1)$ ao longo das direções $\mathbf{a}_i$ e $\mathbf{b}_j$, respectivamente. Para um estado puro, a Eq. (1.10) pode ser posta da seguinte forma,

$$E(\mathbf{a}_i, \mathbf{b}_j) = \langle \Psi^- | \sigma_{\mathbf{a}_i}^A \otimes \sigma_{\mathbf{b}_j}^B | \Psi^- \rangle, \tag{1.11}$$

onde $\sigma_{\mathbf{a}_i}^A = \mathbf{a}_i \cdot \sigma^A$ e $\sigma_{\mathbf{b}_j}^B = \mathbf{b}_j \cdot \sigma^B$, $\sigma^A = (\sigma_x^A, \sigma_y^A, \sigma_z^A)$ e $\sigma^B = (\sigma_x^B, \sigma_y^B, \sigma_z^B)$ e o ponto representa o produto escalar. Para vermos isso basta lembrar que qualquer estado puro de dois qbits pode ser escrito como $|\Psi^-\rangle = a|0\rangle_{\mathbf{a}_i}|0\rangle_{\mathbf{b}_j} + b|0\rangle_{\mathbf{a}_i}|1\rangle_{\mathbf{b}_j} + c|1\rangle_{\mathbf{a}_i}|0\rangle_{\mathbf{b}_j} + d|1\rangle_{\mathbf{a}_i}|1\rangle_{\mathbf{b}_j}$, com a, b, c e d complexos, $|0(1)\rangle_{\mathbf{a}_i}$ autovetor de $\sigma_{\mathbf{a}_i}^A$ e $|0(1)\rangle_{\mathbf{b}_j}$ autovetor de $\sigma_{\mathbf{b}_j}^B$. Substituindo essa expansão de $|\Psi^-\rangle$ na Eq. (1.11) obtemos

$$E(\mathbf{a}_i, \mathbf{b}_j) = |a|^2 + |d|^2 - |b|^2 - |c|^2. \tag{1.12}$$

Agora, como $|a|^2 = P_{00}(\mathbf{a}_i, \mathbf{b}_j)$, $|d|^2 = P_{11}(\mathbf{a}_i, \mathbf{b}_j)$, $|b|^2 = P_{01}(\mathbf{a}_i, \mathbf{b}_j)$ e $|c|^2 = P_{10}(\mathbf{a}_i, \mathbf{b}_j)$, recuperamos a Eq. (1.10) a partir de (1.11).

Sendo as componentes cartesianas dos vetores $\mathbf{a}_i = (a_x, a_y, a_z)$ e $\mathbf{b}_j = (b_x, b_y, b_z)$ temos que

$$\begin{aligned} \sigma_{\mathbf{a}_i}^A \otimes \sigma_{\mathbf{b}_j}^B \;=\; & a_x b_x \sigma_x^A \sigma_x^B + a_x b_y \sigma_x^A \sigma_y^B + a_x b_z \sigma_x^A \sigma_z^B \\ & + a_y b_x \sigma_y^A \sigma_x^B + a_y b_y \sigma_y^A \sigma_y^B + a_y b_z \sigma_y^A \sigma_z^B \\ & + a_z b_x \sigma_z^A \sigma_x^B + a_z b_y \sigma_z^A \sigma_y^B + a_z b_z \sigma_z^A \sigma_z^B. \end{aligned} \tag{1.13}$$

Já que $\sigma_{\mathbf{a}_i}^A \otimes \sigma_{\mathbf{b}_j}^B$ é um observável (sua média tem que ser real) e $\sigma_y|0\rangle = \mathrm{i}|0\rangle$ e $\sigma_y|1\rangle = -\mathrm{i}|1\rangle$, somente termos com um número par de σ_y's na Eq. (1.13) são relevantes no cálculo de $E(\mathbf{a}_i, \mathbf{b}_j)$. Além disso, como a aplicação de σ_x e σ_y em $|0\rangle$ e $|1\rangle$ produzem estados ortogonais e a aplicação de σ_z produz apenas uma fase global no estado em que ele atua, termos que possuem um número ímpar de σ_z's se anulam. Dessa forma, os únicos termos da Eq. (1.13) contribuindo no cálculo de

$E(\mathbf{a}_i, \mathbf{b}_j)$ são

$$\begin{aligned} E(\mathbf{a}_i, \mathbf{b}_j) &= \langle \Psi^- | a_x b_x \sigma_x^A \sigma_x^B + a_y b_y \sigma_y^A \sigma_y^B + a_z b_z \sigma_z^A \sigma_z^B | \Psi^- \rangle \\ &= -\frac{a_x b_x}{2} \left(\langle 01 | \sigma_x^A \sigma_x^B | 10 \rangle + \langle 10 | \sigma_x^A \sigma_x^B | 01 \rangle \right) \\ &\quad -\frac{a_y b_y}{2} \left(\langle 01 | \sigma_y^A \sigma_y^B | 10 \rangle + \langle 10 | \sigma_y^A \sigma_y^B | 01 \rangle \right) \\ &\quad +\frac{a_z b_z}{2} \left(\langle 01 | \sigma_z^A \sigma_z^B | 01 \rangle + \langle 10 | \sigma_z^A \sigma_z^B | 10 \rangle \right) \\ &= -(a_x b_x + a_y b_y + a_z b_z) \\ &= -\mathbf{a}_i \cdot \mathbf{b}_j. \end{aligned} \tag{1.14}$$

Como era de se esperar, se Alice e Bob medem seus qbits na mesma direção, $\mathbf{a}_i = \mathbf{b}_j$, obtemos $E(\mathbf{a}_i, \mathbf{a}_i) = -1$. Isto expressa, para este caso em particular, o fato de que o novo estado descrevendo o par de qbits sempre será $|01\rangle_{\mathbf{a_i}}$ ou $|10\rangle_{\mathbf{a_i}}$, não importando a orientação do vetor $\mathbf{a}_i$.

Precisamos definir só mais uma quantidade [24] antes de apresentarmos o protocolo de transmissão de chave quântica [31]:

$$S \equiv E(\mathbf{a}_1, \mathbf{b}_1) - E(\mathbf{a}_1, \mathbf{b}_3) + E(\mathbf{a}_3, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_3). \tag{1.15}$$

Como o ângulo formado por todos os pares de vetores que aparecem acima vale $\pi/4$, exceto para o par $\mathbf{a}_1$ e $\mathbf{b}_3$, o qual é $3\pi/4$, temos que $E(\mathbf{a}_1, \mathbf{b}_1) = -E(\mathbf{a}_1, \mathbf{b}_3) = E(\mathbf{a}_3, \mathbf{b}_1) = E(\mathbf{a}_3, \mathbf{b}_3) = -\sqrt{2}/2$. Portanto,

$$S = -2\sqrt{2}. \tag{1.16}$$

Voltando ao protocolo, após Alice e Bob finalizarem as medidas nos vários pares de qbits oriundos de singletos, eles anunciam publicamente as orientações escolhidas para cada medida e se detectaram ou não seus qbits. Eles descartam todas as medidas em que pelo menos um deles não detectou nenhum qbit. Isso ocorre pois o detector não tem eficiência um. Em seguida eles separam todas as suas medidas em dois grupos: 1) grupo de todas as medidas nas quais Alice e Bob orientaram diferentemente seus detectores; 2) grupo onde ambos usaram a mesma orientação ($\{\mathbf{a}_2, \mathbf{b}_1\}$ e $\{\mathbf{a}_3, \mathbf{b}_2\}$). Feita essa triagem, Alice e Bob anunciam publicamente os resultados obtidos para todas as medidas do grupo 1. A partir destes dados eles calculam S, cujo resultado deve ser igual ao fornecido pela Eq. (1.16). Se esse resultado se verificar, eles podem utilizar os dados do grupo 2, os quais estão anti-correlacionados, como chave criptográfica. Caso o valor de S não seja aquele dado pela Eq. (1.16), Alice e Bob descartam todos os seus dados e recomeçam o protocolo.

A fim de provar a segurança desse protocolo, devemos calcular o valor de S supondo que um terceiro sujeito, diga-se Eva, interfira na transmissão dos qbits.

Suponhamos que Eva meça os qbits de Alice e Bob numa direção $\mathbf{n}_a$ e $\mathbf{n}_b$, respectivamente. Dessa forma, ao medir o singleto Eva obtém uma das quatro possibilidades abaixo representadas:

$$\begin{aligned}
|\Psi^-\rangle &\overset{\text{medida}}{\longrightarrow} |0\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}, \\
|\Psi^-\rangle &\overset{\text{medida}}{\longrightarrow} |0\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}, \\
|\Psi^-\rangle &\overset{\text{medida}}{\longrightarrow} |1\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}, \\
|\Psi^-\rangle &\overset{\text{medida}}{\longrightarrow} |1\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b},
\end{aligned} \tag{1.17}$$

onde $|\cdot\rangle_{\mathbf{n}_a}$ e $|\cdot\rangle_{\mathbf{n}_b}$ são os autoestados dos operadores $\sigma^A_{\mathbf{n}_a}$ e $\sigma^B_{\mathbf{n}_b}$.

Sejam $|\alpha(\mathbf{n}_a,\mathbf{n}_b)|^2, |\beta(\mathbf{n}_a,\mathbf{n}_b)|^2, |\gamma(\mathbf{n}_a,\mathbf{n}_b)|^2$ e $|\delta(\mathbf{n}_a,\mathbf{n}_b)|^2$ as probabilidades de detecção de cada uma das respectivas quatro possibilidades acima expostas. Explicitamos a depência das probabilidades em termos das orientações $\mathbf{n}_a$ e $\mathbf{n}_b$ para realçar que elas dependem da estratégia de medida utilizada por Eva. Sendo assim, o estado que chega a Alice e Bob após Eva realizar suas medidas é

$$\begin{aligned}
\zeta \;=\; & |\alpha(\mathbf{n}_a,\mathbf{n}_b)|^2 |0\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}\,{}_{\mathbf{n}_a}\langle 0|\,{}_{\mathbf{n}_b}\langle 0| + |\beta(\mathbf{n}_a,\mathbf{n}_b)|^2 |0\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}\,{}_{\mathbf{n}_a}\langle 0|\,{}_{\mathbf{n}_b}\langle 1| \\
& + |\gamma(\mathbf{n}_a,\mathbf{n}_b)|^2 |1\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}\,{}_{\mathbf{n}_a}\langle 1|\,{}_{\mathbf{n}_b}\langle 0| + |\delta(\mathbf{n}_a,\mathbf{n}_b)|^2 |1\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}\,{}_{\mathbf{n}_a}\langle 1|\,{}_{\mathbf{n}_b}\langle 1|.
\end{aligned} \tag{1.18}$$

Para um estado misto qualquer, a Eq. (1.10) pode-se ser escrita como

$$E(\mathbf{a}_i,\mathbf{b}_j) = \mathrm{Tr}\left[\zeta\left(\sigma^A_{\mathbf{a}_i}\otimes\sigma^B_{\mathbf{b}_j}\right)\right]. \tag{1.19}$$

Novamente podemos ver isso expandindo ζ na base $\{|n\rangle_{\mathbf{a}_i}|m\rangle_{\mathbf{b}_j}\,{}_{\mathbf{a}_i}\langle k|\,{}_{\mathbf{b}_j}\langle l|\}$, onde $n,m,k,l = 0,1$. Temos no total 16 vetores. No entanto, ao tomarmos o traço, restarão apenas os elementos da diagonal da matriz densidade. Estes, por sua vez, são dados por $P_{00}(\mathbf{a}_i,\mathbf{b}_j), P_{11}(\mathbf{a}_i,\mathbf{b}_j), -P_{01}(\mathbf{a}_i,\mathbf{b}_j), -P_{10}(\mathbf{a}_i,\mathbf{b}_j)$, mostrando que a Eq. (1.19) é equivalente a Eq. (1.10).

Para simplificar as contas, e sem perder em generalidade, podemos expandir o vetor $\mathbf{a}_i$ num sistema de referência $x'y'z'$, onde z' é paralelo a $\mathbf{n}_a$ e o vetor $\mathbf{b}_j$ num sistema $x''y''z''$ onde z'' é paralelo a $\mathbf{n}_b$. Fizemos esta escolha de tal forma que as relações abaixo sejam satisfeitas:

$$\sigma^A_{x'}|0(1)\rangle_{\mathbf{n}_a} = |1(0)\rangle_{\mathbf{n}_a}, \tag{1.20}$$
$$\sigma^B_{x''}|0(1)\rangle_{\mathbf{n}_b} = |1(0)\rangle_{\mathbf{n}_b}, \tag{1.21}$$
$$\sigma^A_{y'}|0(1)\rangle_{\mathbf{n}_a} = \mathrm{i}(-\mathrm{i})|1(0)\rangle_{\mathbf{n}_a}, \tag{1.22}$$
$$\sigma^B_{y''}|0(1)\rangle_{\mathbf{n}_b} = \mathrm{i}(-\mathrm{i})|1(0)\rangle_{\mathbf{n}_b}, \tag{1.23}$$
$$\sigma^A_{z'}|0(1)\rangle_{\mathbf{n}_a} = +(-)|0(1)\rangle_{\mathbf{n}_a}, \tag{1.24}$$
$$\sigma^B_{z''}|0(1)\rangle_{\mathbf{n}_b} = +(-)|0(1)\rangle_{\mathbf{n}_b}. \tag{1.25}$$

Nestes sistemas de coordenadas,

$$\begin{aligned}
\sigma^A &= \sigma^A_{x'}\mathbf{x}' + \sigma^A_{y'}\mathbf{y}' + \sigma^A_{z'}\mathbf{z}', && (1.26)\\
\sigma^B &= \sigma^B_{x''}\mathbf{x}'' + \sigma^B_{y''}\mathbf{y}'' + \sigma^B_{z''}\mathbf{z}'', && (1.27)\\
\mathbf{a}_i &= a'_x\mathbf{x}' + a'_y\mathbf{y}' + a'_z\mathbf{z}', && (1.28)\\
\mathbf{b}_j &= b''_x\mathbf{x}'' + b''_y\mathbf{y}'' + b''_z\mathbf{z}'', && (1.29)\\
\mathbf{n}_a &= \mathbf{z}', && (1.30)\\
\mathbf{n}_b &= \mathbf{z}'', && (1.31)
\end{aligned}$$

onde $\mathbf{x}', \mathbf{y}', \mathbf{z}'$ e $\mathbf{x}'', \mathbf{y}'', \mathbf{z}''$ são os versores que definem, respectivamente, os sistemas de referência $x'y'z'$ e $x''y''z''$.

Usando as expressões anteriores podemos escrever os operadores $\sigma^A_{\mathbf{a}_i}$ e $\sigma^B_{\mathbf{b}_j}$ da seguinte forma:

$$\sigma^A_{\mathbf{a}_i} = \mathbf{a}_i \cdot \sigma^A = a'_x\sigma^A_{x'} + a'_y\sigma^A_{y'} + a'_z\sigma^A_{z'}, \quad (1.32)$$

$$\sigma^B_{\mathbf{b}_j} = \mathbf{b}_i \cdot \sigma^B = b''_x\sigma^B_{x''} + b''_y\sigma^B_{y''} + b''_z\sigma^B_{z''}. \quad (1.33)$$

Por meio das Eqs. (1.32) e (1.33) vemos que

$$\begin{aligned}
\sigma^A_{\mathbf{a}_i} \otimes \sigma^B_{\mathbf{b}_j} &= a'_x b''_x \sigma^A_{x'}\sigma^B_{x''} + a'_x b''_y \sigma^A_{x'}\sigma^B_{y''} + a'_x b''_z \sigma^A_{x'}\sigma^B_{z''}\\
&\quad + a'_y b''_x \sigma^A_{y'}\sigma^B_{x''} + a'_y b''_y \sigma^A_{y'}\sigma^B_{y''} + a'_y b''_z \sigma^A_{y'}\sigma^B_{z''}\\
&\quad + a'_z b''_x \sigma^A_{z'}\sigma^B_{x''} + a'_z b''_y \sigma^A_{z'}\sigma^B_{y''} + a'_z b''_z \sigma^A_{z'}\sigma^B_{z''}. \quad (1.34)
\end{aligned}$$

Retornando ao cálculo do coeficiente de correlação, vemos que substituindo a Eq. (1.18) em (1.19) temos

$$\begin{aligned}
E(\mathbf{a}_i, \mathbf{b}_j) &= |\alpha(\mathbf{n}_a, \mathbf{n}_b)|^2 \, {}_{\mathbf{n}_a}\langle 0| \, {}_{\mathbf{n}_b}\langle 0|\sigma^A_{\mathbf{a}_i} \otimes \sigma^B_{\mathbf{b}_j}|0\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}\\
&\quad + |\beta(\mathbf{n}_a, \mathbf{n}_b)|^2 \, {}_{\mathbf{n}_a}\langle 0| \, {}_{\mathbf{n}_b}\langle 1|\sigma^A_{\mathbf{a}_i} \otimes \sigma^B_{\mathbf{b}_j}|0\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}\\
&\quad + |\gamma(\mathbf{n}_a, \mathbf{n}_b)|^2 \, {}_{\mathbf{n}_a}\langle 1| \, {}_{\mathbf{n}_b}\langle 0|\sigma^A_{\mathbf{a}_i} \otimes \sigma^B_{\mathbf{b}_j}|1\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}\\
&\quad + |\delta(\mathbf{n}_a, \mathbf{n}_b)|^2 \, {}_{\mathbf{n}_a}\langle 1| \, {}_{\mathbf{n}_b}\langle 1|\sigma^A_{\mathbf{a}_i} \otimes \sigma^B_{\mathbf{b}_j}|1\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}. \quad (1.35)
\end{aligned}$$

Observando as Eqs. (1.20-1.25), os únicos termos da Eq. (1.34) que contribuem no cálculo de $E(\mathbf{a}_i, \mathbf{b}_j)$ são

$$\begin{aligned}
E(\mathbf{a}_i, \mathbf{b}_j) &= |\alpha(\mathbf{n}_a, \mathbf{n}_b)|^2 \, {}_{\mathbf{n}_a}\langle 0| \, {}_{\mathbf{n}_b}\langle 0|a'_z b''_z \sigma^A_{z'}\sigma^B_{z''}|0\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}\\
&\quad + |\beta(\mathbf{n}_a, \mathbf{n}_b)|^2 \, {}_{\mathbf{n}_a}\langle 0| \, {}_{\mathbf{n}_b}\langle 1|a'_z b''_z \sigma^A_{z'}\sigma^B_{z''}|0\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}\\
&\quad + |\gamma(\mathbf{n}_a, \mathbf{n}_b)|^2 \, {}_{\mathbf{n}_a}\langle 1| \, {}_{\mathbf{n}_b}\langle 0|a'_z b''_z \sigma^A_{z'}\sigma^B_{z''}|1\rangle_{\mathbf{n}_a}|0\rangle_{\mathbf{n}_b}\\
&\quad + |\delta(\mathbf{n}_a, \mathbf{n}_b)|^2 \, {}_{\mathbf{n}_a}\langle 1| \, {}_{\mathbf{n}_b}\langle 1|a'_z b''_z \sigma^A_{z'}\sigma^B_{z''}|1\rangle_{\mathbf{n}_a}|1\rangle_{\mathbf{n}_b}\\
&= f(\mathbf{n}_a, \mathbf{n}_b) a'_z b''_z, \quad (1.36)
\end{aligned}$$

onde $f(\mathbf{n}_a, \mathbf{n}_b) = |\alpha(\mathbf{n}_a, \mathbf{n}_b)|^2 - |\beta(\mathbf{n}_a, \mathbf{n}_b)|^2 - |\gamma(\mathbf{n}_a, \mathbf{n}_b)|^2 + |\delta(\mathbf{n}_a, \mathbf{n}_b)|^2$. Como a soma do módulo quadrado dos coeficientes da expansão de ζ vale 1, então $|f(\mathbf{n}_a, \mathbf{n}_b)| \leq 1$.

Por meio das Eqs. (1.28-1.31) obtemos

$$a'_z = \mathbf{a}_i \cdot \mathbf{n}_a, \tag{1.37}$$
$$b''_z = \mathbf{b}_j \cdot \mathbf{n}_b. \tag{1.38}$$

Assim, a Eq. (1.36) é reescrita como

$$E(\mathbf{a}_i, \mathbf{b}_j) = |f(\mathbf{n}_a, \mathbf{n}_b)|(\mathbf{a}_i \cdot \mathbf{n}_a)(\mathbf{b}_j \cdot \mathbf{n}_b), \tag{1.39}$$

onde tomamos o módulo de $f(\mathbf{n}_a, \mathbf{n}_b)$ para enfatizar que sempre podemos tê-lo positivo, simplesmente redefinindo os eixos $\mathbf{n}_a$ e $\mathbf{n}_b$.

Além disso, Eva pode mudar sua estratégia de medida para cada par interceptado, bastando para isso alterar a orientação de $\mathbf{n}_a$ e $\mathbf{n}_b$. A função de correlação final se torna, pois,

$$E(\mathbf{a}_i, \mathbf{b}_j) = \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a, \mathbf{n}_b)(\mathbf{a}_i \cdot \mathbf{n}_a)(\mathbf{b}_j \cdot \mathbf{n}_b), \tag{1.40}$$

onde $\varrho(\mathbf{n}_a, \mathbf{n}_b)$ é a probabilidade normalizada de cada estratégia[9] utilizada por Eva, i. e., $\int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a, \mathbf{n}_b) = 1$.

Finalmente, usando a Eq. (1.40) a função S pode ser assim escrita:

$$\begin{aligned} S &= \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a, \mathbf{n}_b)[(\mathbf{a}_1 \cdot \mathbf{n}_a)(\mathbf{b}_1 \cdot \mathbf{n}_b) - (\mathbf{a}_1 \cdot \mathbf{n}_a)(\mathbf{b}_3 \cdot \mathbf{n}_b) \\ &\quad +(\mathbf{a}_3 \cdot \mathbf{n}_a)(\mathbf{b}_1 \cdot \mathbf{n}_b) + (\mathbf{a}_3 \cdot \mathbf{n}_a)(\mathbf{b}_3 \cdot \mathbf{n}_b)] \\ &= \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a, \mathbf{n}_b)\{(\mathbf{a}_1 \cdot \mathbf{n}_a)[\mathbf{b}_1 \cdot \mathbf{n}_b - \mathbf{b}_3 \cdot \mathbf{n}_b] + \\ &\quad +(\mathbf{a}_3 \cdot \mathbf{n}_a)[\mathbf{b}_1 \cdot \mathbf{n}_b + \mathbf{b}_3 \cdot \mathbf{n}_b]\}. \end{aligned} \tag{1.41}$$

Agora, como todos os vetores que aparecem na Eq. (1.41) são unitários, todos os produtos escalares têm módulo menor ou igual a 1. Assim,

$$\begin{aligned} |S| &\leq \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a, \mathbf{n}_b)\{|\mathbf{a}_1 \cdot \mathbf{n}_a||\mathbf{b}_1 \cdot \mathbf{n}_b - \mathbf{b}_3 \cdot \mathbf{n}_b| + \\ &\quad +|\mathbf{a}_3 \cdot \mathbf{n}_a||\mathbf{b}_1 \cdot \mathbf{n}_b + \mathbf{b}_3 \cdot \mathbf{n}_b|\}. \\ &\leq \int \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b \varrho(\mathbf{n}_a, \mathbf{n}_b)\{|\mathbf{b}_1 \cdot \mathbf{n}_b - \mathbf{b}_3 \cdot \mathbf{n}_b| + |\mathbf{b}_1 \cdot \mathbf{n}_b + \mathbf{b}_3 \cdot \mathbf{n}_b|\}. \end{aligned} \tag{1.42}$$

Analisando o termo entre chaves na Eq. (1.42) vemos que ele é da forma $|x - y| + |x + y|$, onde $x = \mathbf{b}_1 \cdot \mathbf{n}_b$ e $y = \mathbf{b}_3 \cdot \mathbf{n}_b$. Mas $|x - y| + |x + y| \leq |x| - |y| + |x| + |y| = 2|x|$, se $|x| > |y|$ ou $|x - y| + |x + y| \leq |y| - |x| + |x| + |y| = 2|y|$, se $|x| < |y|$. Portanto, $|x - y| + |x + y| \leq \max\{2|x|, 2|y|\}$. E como $|x| \leq 1$ e $|y| \leq 1$ então

[9] Se $\varrho(\mathbf{n}_a, \mathbf{n}_b) = |f(\mathbf{n}_a, \mathbf{n}_b)|\delta(\mathbf{n}_a - \mathbf{n'}_a)\delta(\mathbf{n}_b - \mathbf{n'}_b)$ recuperamos a Eq. (1.39). Ou seja, Eva fixou uma estratégia e a manteve para todas as medidas.

$|x-y|+|x+y| \leq 2$. Usando este último resultado na Eq. (1.42) e lembrando que $\varrho(\mathbf{n}_a, \mathbf{n}_b)$ está normalizada,

$$|S| \leq 2. \tag{1.43}$$

A Eq. (1.43) claramente mostra que qualquer interferência feita por Eva nos pares de qbits que se dirigem até Alice e Bob pode ser detectada por eles, pois nunca Eva conseguirá ao mesmo tempo extrair alguma informação e reproduzir o valor $S = -2\sqrt{2}$. Eva, no máximo,[10] fará com que os estados que cheguem a Alice e Bob alcancem $S = -2$, não importando a engenhosidade de sua estratégia. É neste sentido que devemos considerar como garantido pelas leis da física o segredo da chave criptográfica transmitida.

1.4 Visão geral da tese

Neste capítulo apresentamos uma visão geral de estados quânticos emaranhados. Mostramos a definição atual do que seria emaranhamento, tanto para estado puro quanto para estado misto. Em seguida apresentamos algumas das mais famosas aplicações de estados quânticos emaranhados: codificação superdensa [12], teletransporte quântico [11] e criptografia quântica [31].

No Cap. 2 estudamos os mais fortes critérios de separabilidade conhecidos. Por meio desses critérios, podemos saber facilmente se alguns tipos de estados quânticos estão ou não emaranhados. Começamos expondo a relação entre violação de desigualdade de Bell [9, 24] e emaranhamento [37]. Mostramos que todo estado puro bipartite emaranhado viola alguma desigualdade de Bell. Por outro lado, este resultado não se aplica a estados mistos [95], o que levou à criação de critérios mais fortes de separabilidade. Em seguida, apresentamos o critério de separabilidade de Peres-Horodecki [65, 47], válido para sistemas descritos por espaços de Hilbert de baixa dimensionalidade e o critério de Simon [88], aplicável a estados descritos por variáveis canônicas, simplesmente conhecidos como estados contínuos. Terminamos este capítulo apresentando o primeiro resultado original desta tese. Trata-se de um método para detectar se temos ou não emaranhamento em estados Gaussianos estudando-se a evolução temporal das dipersões da posição e do momento de apenas um dos constituintes do sistema.

O Cap. 3 é dedicado à quantificação do emaranhamento. Apresentamos três medidas de emaranhamento, válidas tanto para estados puros quanto para estados mistos. Em seguida estudamos em detalhes uma delas, o Emaranhamento de Formação (EoF). Mostramos, baseados na Ref. [99], uma dedução da expressão analítica para se calcular o EoF de um sistema formado por dois qbits. Deduzimos

[10] Se tivéssemos utilizado explicitamente as orientações de $\mathbf{a}_1, \mathbf{a}_3, \mathbf{b}_1$ e $\mathbf{b}_3$, teríamos obtido um limite superior ainda menor: $|S| \leq \sqrt{2}$

também, baseados no trabalho de Giedke *et al.* [36], a expressão analítica a partir da qual obtemos o EoF para estados Gaussianos simétricos. Munidos dessa expressão, apresentamos mais um resultado original desta tese: dois limitantes inferiores para o EoF de estados Gaussianos arbitrários [73]. Finalizamos o Cap. 3 estudando sistemas de mais de um qbit. Num outro resultado original, generalizamos [76] para N qbits o protocolo de teletransporte de Bennett *et al.* [11], i. e., mostramos como teleportar um cadeia de N qbits. A partir da eficiência que $2N$ qbits têm para teleportar N qbits, definimos uma nova medida de emaranhamento multipartite [76]. Esta medida, o Emaranhamento de Teletransporte (E_T), possui forte apelo físico e, dado um estado puro multipartite formado por um número par de constituintes, facilmente obtemos seu valor. Além disso, podemos interpretar o E_T como medindo a eficiência de codificação superdensa de um estado multipartite [75]. Mostramos, enfim, que o canal quântico necessário para teleportar N qbits, emaranhados ou não, nada mais é do que N estados de Bell trabalhando em paralelo [75].

No Cap. 4 propomos uma relação de incerteza mais geral [70, 71] do que a famosa relação de incerteza de Heisenberg [44]. Supondo que lidamos com partículas idênticas e emaranhadas, apresentamos uma nova desigualdade para as dispersões da posição e do momento das várias partículas de um sistema composto. Essa nova relação constitui uma possível explicação para o experimento envolvendo fótons emaranhados realizado por Kim e Shih [56]. Este experimento, no qual vemos uma aparente violação da desigualdade de Heisenberg, foi a maior motivação deste capítulo.

No Cap. 5 investigamos como o caos quântico, a localização e o emaranhamento se relacionam. Usando o modelo de Heisenberg e calculando o emaranhamento bipartite para primeiros, segundos e terceiros vizinhos, mostramos que [78], em geral, quanto maior a caoticidade do sistema menos emaranhamento bipartite obtemos. Este resultado é interessante pois mostramos, pela primeira vez, que nem sempre um ambiente caótico favorece o aparecimento de emaranhamento [7, 61]. A existência ou não de um alto grau de emaranhamento bipartite num ambiente caótico depende de qual modelo físico descreve nosso sistema. Mostramos, também, que a localização está fortemente entrelaçada com a caoticidade do sistema. Dependendo desse grau de caoticidade, ora o emaranhamento cresce e ora descresce com a localização [78].

Quando dois ou mais qbits, em equilíbrio térmico com um reservatório de temperatura T, estão emaranhados, lidamos com emaranhamento térmico. Este é o assunto do Cap. 6. Supondo que a interação entre dois qbits se dá por meio da Hamiltoniana de Heisenberg, estudamos detalhadamente o emaranhamento térmico para uma vasta gama de constantes de acoplamento [74]. Mostramos, pela primeira vez, que existem regiões de anisotropia da Hamiltoniana favorecendo o emaranhamento. Além disso, estas regiões aumentam a temperatura máxima na qual ainda encontramos emaranhamento [74]. Revisamos, também, os resultados anteriormente obtidos para modelagens mais simples e provamos que todos são casos particulares

da solução analítica que obtemos para o caso geral. Terminamos o Cap. 6 apresentando um resultado numérico que sugere fortemente a inexistência, para esse modelo, de um conjunto de constantes de acoplamento que propiciem um aumento no emaranhamento ao se aumentar a temperatura T do reservatório térmico.

Finalmente, no Cap. 7, expomos nossas considerações finais, relembramos os pontos relevantes dos capítulos anteriores e sugerimos possíveis assuntos a serem investigados futuramente.

Capítulo 2

Aspectos Qualitativos do Emaranhamento

2.1 Introdução

Já vimos que o emaranhamento é um recurso muito útil para a realização eficiente de tarefas até então impossíveis de serem executadas utilizando-se apenas as propriedades clássicas da Natureza. Dessa forma, torna-se natural perguntar quais estados quânticos estão emaranhados. Isto é, dada uma matriz densidade ρ, queremos saber se ela representa um estado quântico emaranhado. Este é um problema que ainda não tem solução geral de fácil implementação. Para sistemas bipartites (sistemas de duas partículas, por exemplo) temos condições necessárias e suficientes. Entretanto, somente para sistemas descritos por estados pertencentes a espaços de Hilbert de baixa dimensionalidade (2×2 e 2×3) temos um procedimento operacional para checar se a matriz densidade descrevendo o sistema é separável (não emaranhado). Para sistemas multipartites o problema é extremamente não trivial e praticamente não temos métodos operacionais. Neste capítulo, nos restringimos a sistemas bipartites.

Para estados puros, existe uma relação íntima entre emaranhamento e violação de desigualdade de Bell. Todo estado puro emaranhado viola alguma desigualdade de Bell. No entanto, isso deixa de ser verdade ao lidarmos com estados mistos. Existem estados mistos emaranhados cujas correlações podem ser explicadas por meio de uma teoria de variável oculta local [95]. Assim, estes estados satisfazem qualquer desigualdade de Bell que venhamos a construir. De alguma forma as correlações clássicas que existem nestes estados mascaram as correlações quânticas associadas ao emaranhamento. Essa foi a motivação para a busca de critérios de emaranhamento mais fortes do que violação de desigualdade de Bell.

A seguir apresentamos uma demonstração de que todo estado puro emaranhado viola alguma desigualdade de Bell. Depois discutimos o critério de separabilidade mais forte até hoje descoberto, o qual nos permite dizer se temos ou não emaranha-

mento em sistemas bipartites arbitrários (puros ou mistos). Analisamos detalhadamente este teste de separabilidade para sistemas bipartites, o qual é muito mais forte que violação de desigualdades de Bell. Este teste é conhecido como critério de Peres-Horodecki ou critério PPT (Transposição Parcial Positiva). Ele é válido tanto para sistemas puros ou mistos e tem a vantagem de ser uma condição necessária e suficiente de separabilidade de fácil implementação para estados pertencentes a espaços de Hilbert de dimensão 2×2 e 2×3. Apresentamos também o critério de separabilidade de Simon, o qual se aplica a sistemas descritos por variáveis canonicamente conjugadas, doravante estados contínuos. Esse critério se mostra uma condição necessária e suficiente de emaranhamento para uma certa classe importante de estados contínuos, os estados Gaussianos. Finalizamos este capítulo mostrando o primeiro resultado original desta tese: um método para determinar se um estado Gaussiano está emaranhado ou não, medindo-se apenas as dispersões na posição e no momento de uma das partículas constituintes do sistema.

2.2 Desigualdade de Bell e Emaranhamento

Usando uma notação semelhante àquela da Sec. 1.3.3, definimos a expressão

$$S = |P(a,b) - P(a,b')| + P(a',b) + P(a',b'), \tag{2.1}$$

onde $P(a,b) = \langle \mathbf{a}\cdot\sigma^{\mathbf{A}} \otimes \mathbf{b}\cdot\sigma^{\mathbf{B}} \rangle$. Aqui, A e B realçam quais são os observáveis de Alice e Bob e $\mathbf{a} = (a_x, a_y, a_z)$ e $\mathbf{b} = (b_x, b_y, b_z)$ são vetores unitários especificando as direções nas quais Alice e Bob medem os spins (± 1) de suas partículas.

A partir dos mesmos argumentos de localidade e realismo usados por Bell na demonstração de seu teorema [9], Clauser, Horne, Shimony, e Holt (CHSH) [24] demonstraram que qualquer teoria de variável oculta local implica em $S \leq 2$. Dessa forma, se um estado quântico fornece $S > 2$ dizemos que ele viola a desigualdade acima e possui características não-locais. Para uma demonstração deste teorema veja o Apêndice C. Nosso objetivo aqui é demonstrar a possibilidade de encontrar orientações $\mathbf{a}$, $\mathbf{a}'$, $\mathbf{b}$ e $\mathbf{b}'$ tais que qualquer estado puro emaranhado usado para calcular S forneça $S > 2$. Ou seja, todo estado emaranhado viola alguma desigualdade de Bell. A demonstração seguinte é fortemente baseada naquela feita originalmente por Gisin [37].

Usando a decomposição de Schmidt[1] podemos escrever qualquer estado emaranhado de dois qbits como

$$|\psi\rangle = c_1|01\rangle + c_2|10\rangle, \tag{2.2}$$

onde c_1 e c_2 são números *reais positivos*. Usando a Eq. (2.2) para calcular $P(a,b)$

[1] Veja o Apêndice D para uma demonstração da decomposição de Schmidt.

obtemos

$$\begin{aligned} P(a,b) &= c_1^2 \langle 01|\mathbf{a}\cdot\sigma^{\mathbf{A}}\otimes\mathbf{b}\cdot\sigma^{\mathbf{B}}|01\rangle + c_2^2 \langle 10|\mathbf{a}\cdot\sigma^{\mathbf{A}}\otimes\mathbf{b}\cdot\sigma^{\mathbf{B}}|10\rangle \\ &\quad +2\,c_1c_2\,\mathrm{Re}\left(\langle 01|\mathbf{a}\cdot\sigma^{\mathbf{A}}\otimes\mathbf{b}\cdot\sigma^{\mathbf{B}}|10\rangle\right). \end{aligned} \tag{2.3}$$

Mas

$$\langle 01|\mathbf{a}\cdot\sigma^{\mathbf{A}}\otimes\mathbf{b}\cdot\sigma^{\mathbf{B}}|01\rangle = -a_zb_z, \tag{2.4}$$

$$\langle 10|\mathbf{a}\cdot\sigma^{\mathbf{A}}\otimes\mathbf{b}\cdot\sigma^{\mathbf{B}}|10\rangle = -a_zb_z, \tag{2.5}$$

$$\mathrm{Re}\left(\langle 01|\mathbf{a}\cdot\sigma^{\mathbf{A}}\otimes\mathbf{b}\cdot\sigma^{\mathbf{B}}|10\rangle\right) = a_xb_x + a_yb_y. \tag{2.6}$$

Substituindo as Eqs. (2.4 - 2.6) na expressão para $P(a,b)$ temos

$$\begin{aligned} P(a,b) &= -c_1^2\,a_zb_z - c_2^2\,a_zb_z + 2\,c_1c_2(a_xb_x + a_yb_y) \\ &= -a_zb_z + 2\,c_1c_2(a_xb_x + a_yb_y). \end{aligned} \tag{2.7}$$

Para obtermos a última igualdade usamos o fato de que $|\psi\rangle$ está normalizado, i. e., $c_1^2 + c_2^2 = 1$. Expressões semelhantes são obtidas para $P(a',b)$, $P(a,b')$ e $P(a',b')$.

Supondo os seguintes valores para os vetores $\mathbf{a}(\mathbf{a}')$ e $\mathbf{b}(\mathbf{b}')$:

$$a_x(a'_x) = \sin\alpha(\sin\alpha'), \quad a_y(a'_y) = 0(0), \quad a_z(a'_z) = \cos\alpha(\cos\alpha'), \tag{2.8}$$

$$b_x(b'_x) = \sin\beta(\sin\beta'), \quad b_y(b'_y) = 0(0), \quad b_z(b'_z) = \cos\beta(\cos\beta'), \tag{2.9}$$

obtemos

$$P(a,b) = -\cos\alpha\cos\beta + 2\,c_1c_2\sin\alpha\sin\beta. \tag{2.10}$$

Expressões idênticas valem para $P(a',b)$, $P(a,b')$ e $P(a',b')$, bastando colocar as 'linhas' apropriadas. Fixando $\alpha = 0$ e $\alpha' = \pi/2$ temos

$$P(a,b) = -\cos\beta, \quad P(a',b) = 2\,c_1c_2\sin\beta, \tag{2.11}$$

$$P(a,b') = -\cos\beta', \quad P(a',b') = 2\,c_1c_2\sin\beta'. \tag{2.12}$$

Assim, a Eq. (2.1) fica reescrita como

$$S = |\cos\beta - \cos\beta'| + 2\,c_1c_2(\sin\beta + \sin\beta'). \tag{2.13}$$

Escolhendo β e β' tais que $\cos\beta = -\cos\beta' > 0$ e $\sin\beta = \sin\beta' > 0$ temos

$$S = 2\cos\beta + 4\,c_1c_2\sin\beta. \tag{2.14}$$

Calculando o máximo da função anterior

$$\frac{\mathrm{d}S}{\mathrm{d}\beta} = 0 \longrightarrow \tan\beta = 2\,c_1c_2. \tag{2.15}$$

A partir do valor de $\tan\beta$ podemos calcular $\cos\beta$ e $\sin\beta$:

$$\cos\beta = \frac{1}{\sqrt{1+\tan^2\beta}} = \frac{1}{\sqrt{1+4\,c_1^2c_2^2}}, \tag{2.16}$$

$$\sin\beta = \sqrt{1-\cos^2\beta} = \frac{2\,c_1c_2}{\sqrt{1+4\,c_1^2c_2^2}}. \tag{2.17}$$

Substituindo as duas últimas expressões na Eq. (2.14) obtemos

$$S = 2\sqrt{1+4\,c_1^2c_2^2} > 2. \qquad \square \tag{2.18}$$

A desigualdade se deve ao fato do termo dentro da raiz quadrada ser sempre maior do que 1.

A demonstração anterior, feita para sistemas bipartites 2×2, pode ser generalizada [66] para um sistema bipartite de dimensão arbitrária $M\times N$. Dessa forma, todo sistema bipartite emaranhado viola alguma desigualdade de Bell.

2.3 Critério de Separabilidade de Peres-Horodecki

O teorema anterior pode ser encarado como um critério de separabilidade: um estado está emaranhado se ele viola alguma desigualdade de Bell. Entretanto, ele só é válido para estados puros. Na verdade, ele falha para a maioria dos estados mistos. Faz-se necessário, então, a criação de critérios mais fortes e de fácil implementação válidos também para estados que não sejam puros. É neste contexto que surge o critério de separabilidade de Peres-Horodecki.

2.3.1 Condição Necessária de Asher Peres

Relembrando a definição de separabilidade, uma matriz densidade ρ é separável se, e somente se, ela pode ser escrita, para algum k, como uma soma de produtos diretos da seguinte forma:

$$\rho = \sum_{i=0}^{k} p_i\rho_i^A\otimes\rho_i^B, \tag{2.19}$$

onde $p_i>0$, $\sum_{i=0}^{k}p_i=1$, e ρ_i^A e ρ_i^B são matrizes densidade dos subsistemas A e B.

O estado acima é o estado mais geral que pode ser preparado por dois observadores separados e que recebem instruções de uma fonte comum. No jargão de Teoria Quântica da Informação, podemos dizer que a matriz ρ acima é a mais geral que pode ser construída via LOCC (Operações Locais e Comunicação Clássica).

Partindo dessa definição, Asher Peres [65] demonstra o seguinte teorema:

Teorema 1 *Se ρ é uma matriz densidade separável, então o operador obtido pela transposição parcial de ρ é positivo semidefinido.*[2]

Antes de provar o teorema acima precisamos de algumas definições e lemas que serão úteis ao longo da demonstração.

Definição 3 *Um operador é positivo semidefinido se seus autovalores são não negativos. A notação usada para indicar que um operador $\mathcal{O}$ é positivo semidefinido é: $\mathcal{O} \geq 0$.*

Definição 4 *Se $\mathcal{T}$ é o operador transposição e $\mathcal{O}_{ij}$ é um elemento de matriz do operador $\mathcal{O}$ numa base qualquer, então, $\mathcal{T}\mathcal{O}_{ij} = \mathcal{O}_{ji}$. Usamos também a seguinte notação para indicar transposição: $\mathcal{O}^T$.*

Lema 1 *$\mathcal{T}(\mathcal{AB}) = \mathcal{T}(\mathcal{B})\mathcal{T}(\mathcal{A})$, onde $\mathcal{A}$ e $\mathcal{B}$ são operadores.*

Prova:
Seja $(\mathcal{AB})_{ij}$ um elemento de matriz do operador$\mathcal{AB}$. Então:

$$\begin{aligned}\mathcal{T}(\mathcal{AB})_{ij} = (\mathcal{AB})_{ji} &= \sum_k \mathcal{A}_{jk}\mathcal{B}_{ki} = \sum_k \mathcal{B}_{ki}\mathcal{A}_{jk} \\ &= \sum_k \mathcal{T}\mathcal{B}_{ik}\mathcal{T}\mathcal{A}_{kj} = (\mathcal{T}(\mathcal{B})\mathcal{T}(\mathcal{A}))_{ij}\end{aligned}$$

Portanto, $\mathcal{T}(\mathcal{AB}) = \mathcal{T}(\mathcal{B})\mathcal{T}(\mathcal{A})$. □

Lema 2 *Se $\mathcal{O}$ é um operador hermitiano e positivo semidefinido e $\mathcal{T}$ é o operador transposição então $\mathcal{TO}$ é positivo semidefinido, isto é, $\mathcal{T}$ é um mapa positivo.*

Prova:
Seja $\mathcal{U}$ a transformação unitária que diagonaliza $\mathcal{O}$. Sendo $\tilde{\mathcal{O}}$ o operador diagonal então $\tilde{\mathcal{O}} = \mathcal{UOU}^\dagger$. Como por definição $\mathcal{O}$ é positivo seimidefinido então $\tilde{\mathcal{O}} \geq 0$. Como $\tilde{\mathcal{O}} \geq 0$ é diagonal então $\mathcal{T}\tilde{\mathcal{O}} \geq 0$. Usando o lema 1 vemos que $\mathcal{T}\tilde{\mathcal{O}} = \mathcal{T}(\mathcal{UOU}^\dagger) = \mathcal{T}(\mathcal{U}^\dagger)\mathcal{TOT}(\mathcal{U}) \geq 0$. Definindo $\mathcal{V} = \mathcal{T}(\mathcal{U}^\dagger)$ e $\mathcal{V}^\dagger = \mathcal{T}(\mathcal{U})$ vemos que $\mathcal{VTOV}^\dagger \geq 0$. Mas $\mathcal{VV}^\dagger = \mathcal{T}(\mathcal{U}^\dagger)\mathcal{T}(\mathcal{U}) = \mathcal{T}(\mathcal{UU}^\dagger) = \mathcal{I}$, onde $\mathcal{I}$ é a matriz identidade. Assim $\mathcal{V}$ também é transformação unitária. Mas uma transformação unitária não altera os autovalores de um operador. Assim, $\mathcal{VTOV}^\dagger \geq 0$ implica em $\mathcal{TO} \geq 0$. Ou seja, $\mathcal{T}$ é mapa positivo. □

[2] Muitos autores também usam a notação operador *positivo* ao invés de *positivo semidefinido*. Rigorosamente, operador *positivo* deveria ser aquele cujos autovalores são positivos (excluindo o zero).

Prova do teorema 1:
Como temos matriz densidade separável, ela pode ser escrita conforme a Eq. (2.19). Um elemento de matriz desse estado pode ser escrito da seguinte forma:

$$\rho_{m\mu,n\nu} = \sum_{i=1}^{k} p_i (\rho_i^A)_{mn} (\rho_i^B)_{\mu\nu}. \tag{2.20}$$

Índices latinos (gregos) referem-se ao sistema A (B). Vamos definir a seguinte matriz σ, que nada mais é do que a transposição parcial em relação ao sistema A.

$$\sigma_{m\mu,n\nu} = \rho_{n\mu,m\nu}. \tag{2.21}$$

Usando a Eq. (2.19), a Eq. (2.21) pode ser escrita da seguinte forma:

$$\sigma = \sum_{i=1}^{k} p_i (\rho_i^A)^T \otimes \rho_i^B. \tag{2.22}$$

Usando o lema 2 sabemos que $(\rho_i^A)^T \geq 0$. Além disso, como a transposição não altera os elementos diagonais de ρ_i^A temos que $Tr\left\{(\rho_i^A)^T\right\} = 1$. Ou seja, como $(\rho_i^A)^T$ é operador positivo semidefinido e possui traço unitário, ele é uma matriz densidade. Dessa forma, o operador σ é matriz densidade, pois ele é uma soma convexa de matrizes densidade. Mas o fato de σ ser matriz densidade implica em $\sigma \geq 0$, isto é, o operador obtido pela transposição parcial de ρ é positivo semidefinido. □

Vale a pena ressaltar que os autovalores de σ são invariantes por transformações unitárias locais feitas em ρ. Isto pode ser facilmente visto se aplicarmos a seguinte transformação unitária em ρ:

$$\rho \to \left(\mathcal{U}^A \otimes \mathcal{U}^B\right) \rho \left(\mathcal{U}^A \otimes \mathcal{U}^B\right)^\dagger. \tag{2.23}$$

Usando a Eq. (2.19) temos que:

$$\rho \to \sum_{i=0}^{k} p_i \mathcal{U}^A \rho_i^A \left(\mathcal{U}^A\right)^\dagger \otimes \mathcal{U}^B \rho_i^B \left(\mathcal{U}^B\right)^\dagger. \tag{2.24}$$

Dessa forma,

$$\sigma \to \sum_{i=0}^{k} p_i \left(\mathcal{U}^A \rho_i^A \left(\mathcal{U}^A\right)^\dagger\right)^T \otimes \mathcal{U}^B \rho_i^B \left(\mathcal{U}^B\right)^\dagger. \tag{2.25}$$

Usando o lema 1:

$$\sigma \to \sum_{i=0}^{k} p_i \left(\left(\mathcal{U}^A\right)^\dagger\right)^T \left(\rho_i^A\right)^T \left(\mathcal{U}^A\right)^T \otimes \mathcal{U}^B \rho_i^B \left(\mathcal{U}^B\right)^\dagger. \tag{2.26}$$

Usando o fato de que $\mathcal{U}^\dagger = \left(\mathcal{U}^T\right)^*$ temos:

$$\sigma \to \sum_{i=0}^{k} p_i \left(\mathcal{U}^A\right)^* \left(\rho_i^A\right)^T \left(\left(\mathcal{U}^A\right)^*\right)^\dagger \otimes \mathcal{U}^B \rho_i^B \left(\mathcal{U}^B\right)^\dagger. \tag{2.27}$$

Definindo $\mathcal{U}^* = \mathcal{V}$ temos:

$$\sigma \to \left(\mathcal{V}^A \otimes \mathcal{U}^B\right) \sigma \left(\mathcal{V}^A \otimes \mathcal{U}^B\right)^\dagger . \tag{2.28}$$

Como $\mathcal{U}$ e $\mathcal{V}$ são transformações unitárias, então σ também sofre uma transformação unitária local dado que ρ sofra uma transformação unitária local. Dessa forma, os autovalores de σ são invariantes por transformações unitárias locais em ρ. Esse fato é muito importante, pois nos permite aplicar o critério da transposição parcial em qualquer representação da matriz densidade ρ. Não importa em qual base ρ está escrita. Basta tomarmos o transposição parcial e checar os autovalores de σ para testar se temos emaranhamento. É por isso que este critério é operacional e de fácil implementação.

2.3.2 Condição Suficiente da Família Horodecki

Ao escrever seu trabalho, Asher Peres conjecturou que o critério da positividade da matriz parcialmente transposta (PPT) poderia ser, além de condição necessária de separabilidade, uma condição suficiente. Talvez tal conjectura se deveu ao fato de o critério PPT ser, para alguns casos, muito mais forte que violações de desigualdade de Bell.

Concomitantemente à publicação do artigo de Asher Peres, a família Horodecki demonstrou um critério necessário e suficiente de separabilidade baseado na teoria de mapas positivos. Esse critério, para sistemas de baixa dimensionalidade (2×2 e 2×3), mostrou-se equivalente ao critério PPT. A família Horodecki [47] também esboçou uma prova de que o critério PPT não seria condição suficiente para sistemas de alta dimensionalidade. Pouco tempo depois desse esboço de prova, Paweł Horodecki, em outro artigo [48], forneceu contra-exemplos para sistemas 2×4 e 3×3, mostrando inequivocamente a ineficácia do critério PPT para sistemas de alta dimensionalidade.

Pretendemos retomar a demonstração feita pela família Horodecki de seu critério de separabilidade baseado na teoria de mapas positivos, bem como sua equivalência ao critério PPT.

Antes de iniciar a demonstração dos três teoremas do trabalho da família Horodecki precisamos de algumas definições e lemas. Vamos também mudar um pouco nossa notação: operadores serão representados por letras maiúsculas latinas e não mais por letras caligráficas maiúsculas, pois agora precisamos das letras caligráficas para representar os espaços de Hilbert. Devemos estar atentos também para não confundir a partição do sistema em A(Alice) e B(Bob) com alguns operadores representados por essas duas letras.

Definição 5 *Seja $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ o espaço de Hilbert de dimensão finita que descreve o nosso sistema bipartido. Por $\mathcal{A}_A$ e $\mathcal{A}_B$ entendemos o conjunto de operadores que*

atuam em $\mathcal{H}_A$ e $\mathcal{H}_B$, respectivamente. $\mathcal{A}_A$ e $\mathcal{A}_B$ são espaços de Hilbert-Schmidt, com produto escalar $\langle A, B\rangle = Tr\left\{B^\dagger A\right\}$, onde A, $B \in \mathcal{A}_i$, $i = A, B$.

Definição 6 *Um operador A é positivo semidefinido se $Tr\{AP\} \geq 0$, onde P é um projetor qualquer.*

A definição anterior é equivalente à não negatividade dos autovalores de A (definição 3). Isso pode ser visto da seguinte maneira. Seja U a transformação unitária que diagonaliza A, isto é, $\tilde{A} = UAU^\dagger$. Então, $Tr\{AP\} = Tr\{U^\dagger UAU^\dagger UP\} = Tr\{UAU^\dagger UPU^\dagger\} = Tr\{\tilde{A}Q\}$, onde $Q = UPU^\dagger$. Dessa forma, $Tr\{\tilde{A}Q\} = Tr\{AP\} \geq 0$. Mas Q também é projetor: $Q^2 = UPU^\dagger\ UPU^\dagger = UP^2U^\dagger = UPU^\dagger = Q$. Como Q pode ser qualquer projetor, bastando para isso escolhermos P apropriadamente, tomamos Q como sendo aqueles que projetam $\tilde{A}$ em seus autoestados. Assim, todos os autovalores de $\tilde{A}$ são não negativos. Usando o fato de que uma transformação unitária não altera os autovalores de um operador e que A e $\tilde{A}$ estão conectados por uma transformação unitária, temos que todos os autovalores de A são não negativos.

Definição 7 (Mapa positivo) *Seja $\mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ o espaço dos mapas lineares de $\mathcal{A}_A$ para $\mathcal{A}_B$. Um mapa $\Lambda \in \mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ é positivo se ele mapeia operadores positivos[3] pertencentes a $\mathcal{A}_A$ no conjunto dos operadores positivos pertencentes a $\mathcal{A}_B$. Isto é, se $A \geq 0$ então $\Lambda(A) \geq 0$.*

Definição 8 (Mapa Completamente Positivo (CP)) *Um mapa $\Lambda \in \mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ é CP se o mapa induzido*

$$\Lambda_n = \Lambda \otimes I : \mathcal{A}_A \otimes \mathcal{M}_n \to \mathcal{A}_B \otimes \mathcal{M}_n$$

é positivo para todo n, onde $\mathcal{M}_n$ é o conjunto de matrizes complexas $n \times n$ e I é o mapa identidade.

Pela definição acima vemos que um mapa CP também é um mapa positivo e que o produto tensorial de um mapa CP pela identidade mapeia operadores positivos em operadores positivos.

Lema 3 *Para qualquer estado inseparável $\tilde{\rho} \in \mathcal{A}_A \otimes \mathcal{A}_B$ existe um operador Hermitiano $\tilde{A}$ tal que $Tr\{\tilde{A}\tilde{\rho}\} < 0$ e $Tr\{\tilde{A}\sigma\} \geq 0$ para qualquer estado σ separável.*

Prova:
Para demonstrar o lema acima, a família Horodecki usa o seguinte teorema, que

[3]Por economia de espaço, ao nos referirmos a operadores positivos estamos nos referindo a operadores positivos semidefinidos.

é uma consequência do teorema de Hahn-Banach [29]: Se W_1 e W_2 são conjuntos convexos fechados em um espaço real de Banach[4] e um destes conjuntos é também conjunto compacto,[5] então existe um funcional f e um $\alpha \in R$ (reais) tais que para todos os pares de elementos $w_1 \in W_1, w_2 \in W_2$ temos

$$f(w_1) < \alpha \leq f(w_2). \tag{2.29}$$

O teorema acima mostra que um conjunto convexo num espaço de Banach é completamente descrito por desigualdades envolvendo funcionais contínuos. Por construção $\tilde{\rho}$ e σ são conjuntos convexos fechados. Além disso, $\tilde{\rho}$, por ser um conjunto unitário, é compacto. (Pois qualquer sequência construída a partir de um conjunto unitário S que tem s como elemento só pode conter o próprio elemento. Dessa forma, qualquer subsequência extraída daí convergirá para s, que obviamente pertence a S.) Dessa forma, pelo teorema de Hahn-Banach, existem uma função f e um α real tais que

$$f(\tilde{\rho}) < \alpha \leq f(\sigma), \tag{2.30}$$

para qualquer σ separável. Agora, um funcional contínuo agindo sobre um espaço de Hilbert pode ser representado por um vetor desse espaço [47]. Como f age sobre um espaço de Hilbert ($\tilde{\rho}, \sigma \in \mathcal{A}_A \otimes \mathcal{A}_B$), podemos representá-lo por meio de um elemento pertencente a esse espaço. Seja $A = A^\dagger$ esse elemento, tal que $f(\bullet) = Tr\{\bullet A\}$. Escolhemos A hermitiano para garantir que o traço seja um número real. Assim, a Eq. (2.30) fica:

$$Tr\{A\tilde{\rho}\} < \alpha \leq Tr\{A\sigma\}. \tag{2.31}$$

Seja $A = \tilde{A} + \alpha I$, onde I é a identidade. Substituindo na Eq. (2.31) temos:

$$\begin{aligned} Tr\{(\tilde{A}+\alpha I)\tilde{\rho}\} < \quad & \alpha \quad \leq Tr\{(\tilde{A}+\alpha I)\sigma\} \\ Tr\{\tilde{A}\tilde{\rho}\} + \alpha \underbrace{Tr\{\tilde{\rho}\}}_{1} < \quad & \alpha \quad \leq Tr\{\tilde{A}\sigma\} + \alpha \underbrace{Tr\{\sigma\}}_{1} \\ Tr\{\tilde{A}\tilde{\rho}\} \quad & < 0 \quad \leq Tr\{\tilde{A}\sigma\}. \qquad \square \end{aligned} \tag{2.32}$$

Usando o lema acima a família Horodecki demonstrou o seguinte critério de separabilidade.

Teorema 2 *Um estado $\rho \in \mathcal{A}_A \otimes \mathcal{A}_B$ é separável se, e somente se, $Tr\{A\rho\} \geq 0$ para qualquer operador A que satisfaça $Tr\{A(P \otimes Q)\} \geq 0$, onde P e Q são projetores que atuam em $\mathcal{H}_A$ e $\mathcal{H}_B$, respectivamente.*

[4] Um espaço de Banach é um espaço vetorial completo com norma $\|v\|$. Se a norma deste espaço for dada por um produto escalar temos um espaço de Hilbert. Isto é, espaço de Banach é mais geral que o espaço de Hilbert, pois aquele, numa colocação não tão rigorosa, não exige um produto escalar.

[5] Um conjunto S é compacto se, para qualquer sequência de elementos $s_1, s_2, \ldots$ de S, uma subsequência pode sempre ser extraída tal que esta subsequência tenda para algum elemento $s \in S$.

Prova:
Se ρ é separável, então ele é dado pela Eq. (2.19). Assim,

$$Tr\{A\rho\} = \sum_{i=0}^{k} p_i Tr\left\{A\left(\rho_i^A \otimes \rho_i^B\right)\right\}.$$

Sendo U_i^A e U_i^B as transformações unitárias que diagonalizam ρ_i^A e ρ_i^B, temos:

$$\begin{aligned} Tr\{A\rho\} &= \sum_{i=0}^{k} p_i Tr\left\{A\left(U_i^{A\dagger}U_i^A\rho_i^A U_i^{A\dagger}U_i^A \otimes U_i^{B\dagger}U_i^B\rho_i^B U_i^{B\dagger}U_i^B\right)\right\} \\ &= \sum_{i=0}^{k} p_i Tr\left\{\underbrace{\left(U_i^A \otimes U_i^B\right)A\left(U_i^A \otimes U_i^B\right)^\dagger}_{A'}\underbrace{U_i^A\rho_i^A U_i^{A\dagger}}_{\rho_i^{A'}} \otimes \underbrace{U_i^B\rho_i^B U_i^{B\dagger}}_{\rho_i^{B'}}\right\} \\ &= \sum_{i=0}^{k} p_i Tr\left\{A'\left(\rho_i^{A'} \otimes \rho_i^{B'}\right)\right\}, \end{aligned} \tag{2.33}$$

onde $\rho_i^{A'}$ e $\rho_i^{B'}$ são diagonais. Sabemos que uma transformação unitária não altera os autovalores de um operador. Então, como por hipótese $Tr\{A(P\otimes Q)\} \geq 0$, isto é, A é um operador positivo, temos que $Tr\{A'(P\otimes Q)\} \geq 0$, pois A e A' estão conectados por uma transformação unitária. Agora, como $\rho_i^{A'}$ e $\rho_i^{B'}$ são diagonais, eles podem ser escritos como uma soma de projetores, onde os pesos para cada projetor são seus autovalores positivos, $\lambda_j^{A_i}$ para $\rho_i^{A'}$ e $\lambda_j^{B_i}$ para $\rho_i^{B'}$:

$$\rho_i^{A'} = \sum_{j=1}^{dim\,\mathcal{H}_{A_i}} \lambda_j^{A_i} P_j^i, \tag{2.34}$$

$$\rho_i^{B'} = \sum_{j=1}^{dim\,\mathcal{H}_{B_i}} \lambda_j^{B_i} Q_j^i, \tag{2.35}$$

onde $dim\,\mathcal{H}_{A_i}$ e $dim\,\mathcal{H}_{B_i}$ são as dimensões dos espaços de Hilbert em que $\rho_i^{A'}$ e $\rho_i^{B'}$ atuam, respectivamente. Logo, substituindo as Eqs. (2.34) e (2.35) na Eq. (2.33) temos:

$$Tr\{A\rho\} = \sum_{i=0}^{k} \sum_{j=1}^{dim\,\mathcal{H}_{A_i}} \sum_{j'=1}^{dim\,\mathcal{H}_{B_i}} p_i \lambda_j^{A_i} \lambda_{j'}^{B_i} Tr\left\{A'\left(P_j^i \otimes Q_{j'}^i\right)\right\}. \tag{2.36}$$

Como $Tr\{A'(P\otimes Q)\} \geq 0$, para qualquer P e Q, então $Tr\left\{A'\left(P_j^i \otimes Q_{j'}^i\right)\right\} \geq 0$. Além disso, $\lambda_j^{A_i}$, $\lambda_{j'}^{B_i}$ e p_i são maiores ou iguais a zero. Portanto, o lado direito da Eq. (2.36) é maior ou igual a zero. Ou seja, $Tr\{A\rho\} \geq 0$.
Agora, para provar que se $Tr\{A\rho\} \geq 0$ então ρ é separável vamos supor o contrário e

mostrar que chegamos numa contradição. Isto é, vamos supor que $Tr\{A\rho\} \geq 0$, para qualquer A que satisfaça $Tr\{A(P \otimes Q)\} \geq 0$, e que ρ seja inseparável. Usando o lema 3 vemos que podemos encontrar um operador Hermitiano A tal que $Tr\{A\rho\} < 0$ e ao mesmo tempo $Tr\{A\sigma\} \geq 0$ para *qualquer estado separável* σ. Então este A também satisfaz $Tr\{A(P \otimes Q)\} \geq 0$, pois $P \otimes Q$ pode ser considerado estado separável (a menos de uma constante de normalização). Ou seja, encontramos um A que também satisfaz $Tr\{A(P \otimes Q)\} \geq 0$ e ao mesmo tempo $Tr\{A\rho\} < 0$. Mas isso contradiz a hipótese, pois supomos inicialmente um estado inseparável tal que $Tr\{A\rho\} \geq 0$, para *qualquer* A satisfazendo $Tr\{A(P \otimes Q)\} \geq 0$. Logo, ρ só pode ser separável. □

A originalidade da familía Horodecki ocorreu na demonstração do próximo teorema, onde eles traduziram o teorema anterior para a linguagem de mapas positivos.

Teorema 3 *Seja ρ uma matriz densidade que atua sobre o espaço de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_B$. Então ρ é separável se, e somente se, para qualquer mapa positivo $\Lambda : \mathcal{A}_B \to \mathcal{A}_A$ o operador $I \otimes \Lambda\rho$ é positivo.*

Prova:
Existe um isomorfismo entre mapas positivos e operadores positivos que é construído da seguinte forma. Dada uma base arbitrária ortonormal E_i de $\mathcal{A}_A$, definimos um mapa isomórfico $\mathcal{S}$ que mapeia o conjunto de mapas lineares $\Lambda : \mathcal{A}_A \to \mathcal{A}_B$ em operadores que atuam sobre $\mathcal{H}_A \otimes \mathcal{H}_B$ da seguinte forma,

$$\begin{aligned} \mathcal{L}(\mathcal{A}_A, \mathcal{A}_B) \ni \Lambda \quad \to \quad & \mathcal{S}(\Lambda) = \sum_i E_i^\dagger \otimes \Lambda(E_i) \in \mathcal{A}_A \otimes \mathcal{A}_B \\ & \mathcal{S}(\Lambda) = (I \otimes \Lambda) \sum_i E_i^\dagger \otimes E_i \in \mathcal{A}_A \otimes \mathcal{A}_B. \end{aligned} \tag{2.37}$$

Para o isomorfismo acima construído, usando o resultado deduzido por Jamiołkowski [53], o mapa $\Lambda \in \mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ é positivo se, e somente se, $\mathcal{S}(\Lambda)$ é operador[6] hermitiano e $Tr\{\mathcal{S}(\Lambda)P \otimes Q\} \geq 0$ para quaisquer projetores $P \in \mathcal{A}_A$ e $Q \in \mathcal{A}_B$. Aqui vemos que $\mathcal{S}(\Lambda)$ equivale ao operador A do teorema 2.

Seja $\{P_{ij} = |i\rangle\langle j|\}_{i,j=1}^{dim\mathcal{H}_A}$ nossa base em $\mathcal{A}_A$, onde $\{|i\rangle\}$ é uma base em $\mathcal{H}_A$.

[6]Subentende-se, daqui em diante, que $\mathcal{S}(P \otimes Q) = \mathcal{S}P \otimes Q$.

Usando essa base e a Eq. (2.37), o teorema 2 pode ser escrito da seguinte forma:

$$Tr\left\{\left((I\otimes\Lambda)\sum_{ij}P_{ji}\otimes P_{ij}\right)\rho\right\} \geq 0, \tag{2.38}$$

$$Tr\left\{\left((I\otimes\Lambda T)\sum_{ij}P_{ji}\otimes TP_{ij}\right)\rho\right\} \geq 0, \tag{2.39}$$

$$Tr\left\{\left((I\otimes\Lambda T)\sum_{ij}P_{ji}\otimes P_{ji}\right)\rho\right\} \geq 0, \tag{2.40}$$

onde T é o operador transposição (veja definição 4). Além disso, lembrando que T é mapa positivo (lema 2), o mapa ΛT também é mapa positivo. Dessa forma, como Λ representa o conjunto de todos os mapas positivos, podemos fazer a seguinte substituição sem perder em generalidade: $\Lambda T \to \Lambda$. Assim, a Eq. (2.40) fica:

$$Tr\left\{\left((I\otimes\Lambda)\sum_{ij}P_{ji}\otimes P_{ji}\right)\rho\right\} \geq 0. \tag{2.41}$$

Vamos definir o seguinte projetor,

$$P_0 = \frac{1}{d}\sum_{ij}P_{ji}\otimes P_{ji}, \tag{2.42}$$

onde $d = dim\mathcal{H}_A$. Substituindo a Eq. (2.42) na Eq. (2.41) temos:

$$Tr\left\{(I\otimes\Lambda)\,dP_0\rho\right\} \geq 0, \tag{2.43}$$

$$Tr\left\{(I\otimes\Lambda)\,P_0\rho\right\} \geq 0, \tag{2.44}$$

pois $d > 0$. Agora, usando o produto escalar do espaço de Hilbert $\mathcal{A}_A\otimes\mathcal{A}_B$ (definição 5) na Eq. (2.44) temos:

$$\left\langle\rho,(I\otimes\Lambda P_0)^\dagger\right\rangle \geq 0, \tag{2.45}$$

$$\langle\rho, I\otimes\Lambda P_0\rangle \geq 0. \tag{2.46}$$

Para chegarmos a última equação usamos o fato de que P_0 é hermitiano e de que mapas positivos preservam a hermiticidade de um operador. Escrevendo a equação adjunta da Eq. (2.46) temos:

$$\langle I\otimes\Lambda\rho, P_0\rangle \geq 0, \tag{2.47}$$

$$Tr\{P_0^\dagger\,(I\otimes\Lambda\rho)\} \geq 0, \tag{2.48}$$

$$Tr\{P_0\,(I\otimes\Lambda\rho)\} \geq 0, \tag{2.49}$$

onde usamos novamente a definição do produto escalar e agora $\Lambda : \mathcal{A}_B \to \mathcal{A}_A$ pois trabalhamos com o mapa adjunto [47]. Como P_0 é um projetor qualquer então a

Eq. (2.49) implica que $I \otimes \Lambda\rho$ é operador positivo para qualquer Λ. Mas a Eq. (2.49) nada mais é do que o teorema 2 escrito de outra maneira, isto é, a Eq. (2.49) é safisfeita se, e somente se, ρ é separável. Logo, pela definição 6, ρ é separável se, e somente se, $I \otimes \Lambda\rho$ é operador positivo. □

Usando o teorema anterior, a família Horodecki conseguiu provar a seguinte condição (operacional), necessária e suficiente, de separabilidade para sistemas 2×2 e 2×3.

Teorema 4 *Um estado ρ agindo sobre espaços $C^2 \otimes C^2$ ou $C^2 \otimes C^3$ é separável se, e somente se, sua transposição parcial é um operador positivo.*

Prova:
O fato de que se ρ é separável então sua transposição parcial é um operador positivo já foi demonstrado. (É o trabalho de Asher Peres anteriormente analisado.) Agora, para provar que se a transposição parcial de ρ é um operador positivo então ρ é separável, a família Horodecki usou o seguinte resultado obtido por Strømer [89] e Woronowicz [100]: "Qualquer mapa positivo $\Lambda : \mathcal{A}_B \to \mathcal{A}_A$, onde $\mathcal{H}_A = \mathcal{H}_B = C^2$ ou $\mathcal{H}_A = C^3$ e $\mathcal{H}_B = C^2$, pode ser escrito da seguinte forma:

$$\Lambda = \Lambda_1^{CP} + \Lambda_2^{CP} T, \tag{2.50}$$

onde Λ_i^{CP} são mapas CP." Como Λ_i^{CP} são mapas CP, então os mapas $\Lambda_i = I \otimes \Lambda_i^{CP}$ são mapas positivos (veja definição 8). Seja ρ^{T_B} a transposição parcial de ρ em relação ao subsistema B, isto é, $\rho^{T_B} = (I \otimes T)\rho$, onde T é o operador transposição. Por hipótese $\rho^{T_B} \geq 0$. Então:

$$\Lambda_1\rho + \Lambda_2\rho^{T_B} \geq 0, \tag{2.51}$$

$$\Lambda_1\rho + \Lambda_2(I \otimes T)\rho \geq 0. \tag{2.52}$$

Usando a definição de Λ_i temos:

$$(I \otimes \Lambda_1^{CP})\rho + (I \otimes \Lambda_2^{CP})(I \otimes T)\rho \geq 0, \tag{2.53}$$

$$(I \otimes \Lambda_1^{CP})\rho + (I \otimes \Lambda_2^{CP} T)\rho \geq 0, \tag{2.54}$$

$$I \otimes (\Lambda_1^{CP} + \Lambda_2^{CP} T)\rho \geq 0. \tag{2.55}$$

Mas como qualquer mapa positivo pode ser escrito conforme a Eq. (2.50), a Eq. (2.55) vale:

$$I \otimes \Lambda\rho \geq 0. \tag{2.56}$$

Assim, pelo teorema 3, o estado ρ é separável. □

Vale ressaltar que toda a dedução desse teorema poderia ser refeita usando a transposição parcial em relação ao subsistema A, isto é, usando ρ^{T_A}. Isso mostra que o critério acima pode ser aplicado tomando a transposição parcial em relação ao subsistema A ou ao subsistema B.

2.3.3 Exemplos

Vamos agora apresentar alguns exemplos de aplicação do critério de separabilidade por transposição parcial. Estes exemplos realçam a operacionalidade do critério e mostram como ele é muito mais forte do que violação de desigualdade de Bell.

A operacionalidade desse teste pode ser vista facilmente ao escrevermos a matriz que representa um estado $\rho \in C^M \otimes C^N$. Essa matriz pode ser escrita da seguinte forma:

$$\rho = \begin{pmatrix} A_{11} & \dots & A_{1M} \\ \vdots & & \vdots \\ A_{M1} & \dots & A_{MM} \end{pmatrix}, \tag{2.57}$$

onde A_{mn} são matrizes $N \times N$ agindo no espaço C^N. Essas matrizes são facilmente construídas se lembrarmos da notação introduzida na Sec. 2.3.1 (veja Eq. (2.20)). Os elementos de matriz de A_{mn} são dados por: $\{A_{mn}\}_{\mu\nu} = \rho_{m\mu,n\nu}$. Com essa notação, a transposição parcial em relação ao sistema B é obtida transpondo-se as matrizes A_{mn}:

$$\rho^{T_B} = \begin{pmatrix} A_{11}^T & \dots & A_{1M}^T \\ \vdots & & \vdots \\ A_{M1}^T & \dots & A_{MM}^T \end{pmatrix}. \tag{2.58}$$

Ou seja, dada uma matriz densidade ρ em qualquer representação, para implementarmos o critério de separabilidade de Peres-Horodecki, basta transpor as matrizes A_{mn} acima definidas, calcular os autovalores dessa nova matriz e checar sua positividade. Se tivermos autovalores negativos, temos estados inseparáveis. Caso contrário, lidamos com estados separáveis. (Esta última conclusão é válida apenas para sistemas 2×2 e 2×3.)

Estado de Werner

Vamos começar analisando o estado de Werner abaixo definido:

$$\rho_W = x \left|\psi^-\right\rangle \left\langle\psi^-\right| + \frac{1-x}{4} I, \tag{2.59}$$

onde $|\psi^-\rangle = (1/\sqrt{2})\,(|01\rangle - |10\rangle)$ e I é a matriz identidade. O estado acima pode ser visto como uma mistura estatística composta de uma fração x de singleto e uma fração $(1-x)$ de proporções iguais de singleto e dos três componentes do tripleto. Representando matricialmente o estado acima na base computacional ($|00\rangle$,$|01\rangle$, $|10\rangle$,$|11\rangle$):

$$\rho_W = \begin{pmatrix} \frac{1-x}{4} & 0 & 0 & 0 \\ 0 & \frac{1+x}{4} & \frac{-x}{2} & 0 \\ 0 & \frac{-x}{2} & \frac{1+x}{4} & 0 \\ 0 & 0 & 0 & \frac{1-x}{4} \end{pmatrix}. \tag{2.60}$$

Calculando o transposição parcial $\sigma_W = \rho_W^{T_B}$ temos:

$$\sigma_W = \begin{pmatrix} \frac{1-x}{4} & 0 & 0 & \frac{-x}{2} \\ 0 & \frac{1+x}{4} & 0 & 0 \\ 0 & 0 & \frac{1+x}{4} & 0 \\ \frac{-x}{2} & 0 & 0 & \frac{1-x}{4} \end{pmatrix}. \tag{2.61}$$

Diagonalizando a matriz acima obtemos três autovalores iguais a $(1+x)/4$ e um igual a $(1-3x)/4$. Aplicando o critério PPT vemos que se $x < 1/3 \approx 0,333$ temos todos os autovalores positivos. Assim, para $x < 1/3$ temos estado separável. Usando critérios de separabilidade baseados em violação de desigualdades de Bell pode-se mostrar [65] que para $x < 1/\sqrt{2} \approx 0,707$ o estado ρ_W satisfaz o critério de localidade de Bell. Ou seja, existem valores de x para os quais o estado ρ_W não viola a desigualdade de Bell mas, mesmo assim, está emaranhado. Isso mostra claramente que o critério PPT é muito mais forte do que violações de desigualdades de Bell.

Estado de Gisin

Um outro exemplo interessante é o estado formado por uma fração x do estado puro $a\,|01\rangle + b\,|10\rangle$, onde $a, b \in R$ e $a^2 + b^2 = 1$ e frações $(1-x)/2$ dos estados puros $|00\rangle$ e $|11\rangle$. Representando matricialmente esse estado temos:

$$\rho_G = \begin{pmatrix} \frac{1-x}{2} & 0 & 0 & 0 \\ 0 & xa^2 & xab & 0 \\ 0 & xab & xb^2 & 0 \\ 0 & 0 & 0 & \frac{1-x}{2} \end{pmatrix}. \tag{2.62}$$

A matriz parcialmente transposta é:

$$\sigma_G = \begin{pmatrix} \frac{1-x}{2} & 0 & 0 & xab \\ 0 & xa^2 & 0 & 0 \\ 0 & 0 & xb^2 & 0 \\ xab & 0 & 0 & \frac{1-x}{2} \end{pmatrix}. \tag{2.63}$$

Calculando seu determinante, vemos que para $x > (1 + 2|ab|)^{-1}$ ele é negativo (fato este que implica pelo menos um autovalor negativo). Dessa forma, para $x >$

$(1+2|ab|)^{-1}$ temos estado quântico emaranhado. Entretanto, esse mesmo estado viola a desigualdade de Bell [38] apenas quando $x > [1+2|ab|(\sqrt{2}-1)]^{-1}$. Novamente temos valores de x para os quais encontramos estados emaranhados que não violam a desigualdade de Bell.

Estado de Peres-Horodecki

Este exemplo é o mais fantástico de todos. Seja ρ_{PH} o estado onde misturamos uma fração x de singleto mais uma fração $(1-x)$ do estado maximamente polarizado $|00\rangle$:

$$\rho_{PH} = x \left|\psi^-\right\rangle \left\langle\psi^-\right| + (1-x) |00\rangle \langle 00| . \tag{2.64}$$

A partir da representação matricial deste estado,

$$\rho_{PH} = \begin{pmatrix} 1-x & 0 & 0 & 0 \\ 0 & \frac{x}{2} & \frac{-x}{2} & 0 \\ 0 & \frac{-x}{2} & \frac{x}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{2.65}$$

obtemos a matriz parcialmente transposta

$$\sigma_{PH} = \begin{pmatrix} 1-x & 0 & 0 & \frac{-x}{2} \\ 0 & \frac{x}{2} & 0 & 0 \\ 0 & 0 & \frac{x}{2} & 0 \\ \frac{-x}{2} & 0 & 0 & 0 \end{pmatrix}. \tag{2.66}$$

Seu determinante vale $-x^4/16$. Este resultado mostra que para todo $x \in (0,1]$ temos emaranhamento. Apenas para um único valor de x, $x = 0$, temos estado separável. No entanto, para $x \leq 0,8$ esse estado não viola [46] a desigualdade de Bell. Aqui vemos realmente que o critério PPT é muito mais forte que violação de desigualdade de Bell.

Podemos entender porque o critério PPT é mais forte do que violação de desigualdade de Bell [65] notando que o teste PPT é estrutural, isto é, ele se utiliza da estrutura matemática da matriz densidade. Nos testes de violação de desigualdade de Bell usamos a matriz densidade apenas para calcular probabilidades. Não analisamos a matriz densidade propriamente dita, mas apenas suas previsões estatísticas.

Gostaríamos de ressaltar, também, que até hoje não há nenhuma interpretação física do critério PPT ou do critério de mapas positivos. Os resultados anteriores foram praticamente traduções de teoremas da análise funcional e da teoria de mapas positivos para a física. Acreditamos que um entendimento maior do que sejam estados quânticos emaranhados deve necessariamente passar por uma interpretação física desses critérios de separabilidade[3].

[3]Podemos dizer que hoje "entendemos" fisicamente a violação da desigualdade de Bell. Uma

2.4 Critério de Separabilidade de Simon

O critério PPT proposto por Peres e pela família Horodecki se limitava a sistemas bipartites descritos por um espaço de Hilbert discreto. Este critério, conforme vimos acima, é suficiente apenas para sistemas 2×2 e 2×3. Isso levou Duan *et al.* [26] a suspeitar que o critério PPT não produziria resultados muito promissores para sistemas descritos por espaços de Hilbert de dimensão infinita. Dessa forma, esses autores usaram uma outra estratégia para deduzir seu critério de separabilidade. Surpreendentemente, no entanto, Simon [88] provou que o critério PPT é muito útil na identificação de estados contínuos bipartidos emaranhados. Além disso, ao nos restringirmos a estados Gaussianos, a positividade da matriz densidade parcialmente transposta torna-se uma condição necessária e suficiente de separabilidade.

2.4.1 Condição Necessária e Suficiente de Simon

O principal resultado de Simon foi mostrar que no espaço de fases podemos interpretar a transposição parcial como uma reflexão especular da variável canônica momento. A partir disso, Simon obtém relações de incertezas mais fortes do que aquelas decorrentes do princípio de incerteza de Heisenberg, as quais devem ser satisfeitas por todos os estados separáveis. E o mais interessante, para sistemas Gaussianos a não violação dessas novas relações de incerteza transforma-se em condição necessária e suficiente de separabilidade. Para entender esse resultado, precisamos de alguns conceitos que serão apresentados abaixo.

Seja um sistema bipartido de dois modos, descrito pelos operadores de aniquilação $\hat{a}_j = (\hat{q}_j + i\hat{p}_j)/\sqrt{2}$, $j = 1, 2$. (Supomos sempre $\hbar = 1$). O modo 1 corresponde ao sistema A (Alice) e o modo 2 corresponde ao sistema B (Bob). As relações de comutação entre $\hat{q}_j$ e $\hat{p}_j$ podem ser expressas de uma forma compacta se definimos o seguinte vetor coluna:

$$\hat{\xi} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2)^T. \tag{2.67}$$

As relações de comutação são:

$$[\hat{\xi}_\alpha, \hat{\xi}_\beta] = i\Omega_{\alpha\beta}, \quad \alpha, \beta = 1, 2, 3, 4. \tag{2.68}$$

A matriz Ω é uma matriz 4×4 dada por:

$$\Omega = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.69}$$

Ao trabalhar no espaço de fases, vamos precisar do seguinte vetor coluna:

$$\xi = (q_1, p_1, q_2, p_2)^T. \tag{2.70}$$

violação dessa desigualdade, posto que aceitemos a hipótese de realismo local de Bell, indica que não é possível construir uma teoria de variáveis ocultas locais que expliquem as correlações observadas em determinadas medidas feitas por dois observadores separados por uma distância tipo espaço.

Na expressão anterior não temos mais os 'chapéus', pois agora lidamos com variáveis canônicas e não operadores. Usando a notação anterior, a distribuição de Wigner para uma matriz densidade ρ que descreve um sistema bipartido é:

$$W(q,p) = \frac{1}{\pi^2}\int \mathrm{d}^2q' \left\langle q-q'\right| \rho \left|q+q'\right\rangle \mathrm{e}^{2\mathrm{i}q'\cdot p}, \tag{2.71}$$

onde $q=(q_1,q_2)$ e $p=(p_1,p_2)$. Agora podemos demonstrar o seguinte teorema:

Teorema 5 *Se ρ é separável e tomamos a sua transposição parcial em relação a Bob, obtemos uma nova matriz densidade σ cuja distribuição de Wigner é obtida da distribuição de Wigner de ρ por uma reflexão especular da variável canônica p_2, isto é, $\rho\to\sigma : W(\xi)\to W(\Lambda\xi)$, onde $\Lambda = diag(1,1,1,-1)$ é uma matriz 4×4 diagonal.*

Prova:
Reescrevendo a Eq. (2.71) temos:

$$\begin{aligned} W(q,p) &= \frac{1}{\pi^2}\int \mathrm{d}q_1'\mathrm{d}q_2' \left\langle q_1-q_1', q_2-q_2'\right| \rho \left|q_1+q_1', q_2+q_2'\right\rangle \\ &\quad \times \exp\left[2\mathrm{i}(q_1'p_1+q_2'p_2)\right]. \end{aligned} \tag{2.72}$$

Como ρ é separável, podemos substituí-lo pela Eq. (2.19):

$$\begin{aligned} W(q,p) &= \frac{1}{\pi^2}\sum_j \tilde{p}_j \int \mathrm{d}q_1'\mathrm{d}q_2' \left\langle q_1-q_1', q_2-q_2'\right| \rho_j^A\otimes\rho_j^B \left|q_1+q_1', q_2+q_2'\right\rangle \\ &\quad \times \exp\left[2\mathrm{i}(q_1'p_1+q_2'p_2)\right], \\ &= \frac{1}{\pi^2}\sum_j \tilde{p}_j \int \mathrm{d}q_1'\mathrm{d}q_2' \left\langle q_1-q_1'\right| \rho_j^A \left|q_1+q_1'\right\rangle \left\langle q_2-q_2'\right| \rho_j^B \left|q_2+q_2'\right\rangle \\ &\quad \times \exp\left[2\mathrm{i}(q_1'p_1+q_2'p_2)\right], \\ &= \frac{1}{\pi^2}\sum_j \tilde{p}_j \int \mathrm{d}q_1'\mathrm{d}q_2' \rho_j^A(q_1-q_1', q_1+q_1')\rho_j^B(q_2-q_2', q_2+q_2') \\ &\quad \times \exp\left[2\mathrm{i}(q_1'p_1+q_2'p_2)\right]. \end{aligned} \tag{2.73}$$

Tomando a transposição parcial com relação a Bob:

$$\begin{aligned} W^{T_B}(q,p) &= \frac{1}{\pi^2}\sum_j \tilde{p}_j \int \mathrm{d}q_1'\mathrm{d}q_2' \rho_j^A(q_1-q_1', q_1+q_1')\rho_j^B(q_2+q_2', q_2-q_2') \\ &\quad \times \exp\left[2\mathrm{i}(q_1'p_1+q_2'p_2)\right]. \end{aligned} \tag{2.74}$$

Fazendo a mudança de variável $q_2'\to -q_2'$ temos:

$$\begin{aligned} W^{T_B}(q,p) &= \frac{1}{\pi^2}\sum_j \tilde{p}_j \int \mathrm{d}q_1'\mathrm{d}q_2' \rho_j^A(q_1-q_1', q_1+q_1')\rho_j^B(q_2-q_2', q_2+q_2') \\ &\quad \times \exp\left\{2\mathrm{i}[q_1'p_1+q_2'(-p_2)]\right\}. \end{aligned} \tag{2.75}$$

Comparando as Eqs. (2.73) e (2.75) vemos que:

$$W^{T_B}(q_1, q_2, p_1, p_2) = W(q_1, q_2, p_1, -p_2). \tag{2.76}$$

Ou seja, $\rho \to \sigma = \rho^{T_B} : W(\xi) \to W(\Lambda\xi)$. □

O teorema anterior mostra que no espaço de fases uma transposição é equivalente a uma reflexão especular na variável momento. O próximo passo é entender como essa reflexão especular no momento influencia as relações de incerteza que um estado separável deve satisfazer.

Seja $\Delta\hat{\xi} = \hat{\xi} - \langle\hat{\xi}\rangle$, onde $\langle\hat{\xi}_\alpha\rangle = Tr\{\hat{\xi}_\alpha\rho\}$. Definimos as mesmas grandezas para as variáveis canônicas: $\Delta\xi_\alpha = \xi_\alpha - \langle\xi_\alpha\rangle$, onde agora $\langle\xi_\alpha\rangle = \int \mathrm{d}^4\xi\ \xi_\alpha W(\xi)$. Como a distribuição de Wigner fornece as mesmas previsões estatísticas que ρ então $\langle\hat{\xi}_\alpha\rangle = \langle\xi_\alpha\rangle$. Um elemento da matriz de variância V, ou matriz de correlação, é definido da seguinte forma:

$$\begin{aligned} V_{\alpha\beta} = \frac{1}{2}\left\langle\left\{\Delta\hat{\xi}_\alpha, \Delta\hat{\xi}_\beta\right\}\right\rangle &= \frac{1}{2}Tr\left\{\left\{\Delta\hat{\xi}_\alpha, \Delta\hat{\xi}_\beta\right\}\rho\right\} \\ &= \int \mathrm{d}^4\xi\ \Delta\xi_\alpha\Delta\xi_\beta W(\xi), \end{aligned} \tag{2.77}$$

onde $\{A, B\} = AB + BA$ é a operação de anticomutação. A matriz de variância V de um estado ρ qualquer satisfaz a seguinte desigualdade, que é uma consequência do princípio de incerteza de Heisenberg [87]:

Teorema 6 *Se ρ é um estado contínuo bipartido qualquer então,*

$$V + \frac{\mathrm{i}}{2}\Omega \geq 0. \tag{2.78}$$

Prova:
Para demonstrar o resultado acima invocamos o teorema de Williamson [96], que para um sistema bipartido pode ser assim enunciado: "Para qualquer matriz $V_{4\times4}$ real ($V = V^*$), simétrica ($V = V^T$) e positiva definida ($V \geq 0$), existe uma transformação simplética $S \in S_p(4, R)$[7] tal que $SVS^T = V'$, onde V' possui a forma diagonal $V' = diag(k_1, k_1, k_2, k_2)$." Esse teorema diz que sempre podemos encontrar uma transformação simplética que desacopla os modos 1 e 2. Usando o teorema anterior vemos que a matriz de variância V pode ser escrita da seguinte forma:

$$V' = \begin{pmatrix} k_1 & 0 & 0 & 0 \\ 0 & k_1 & 0 & 0 \\ 0 & 0 & k_2 & 0 \\ 0 & 0 & 0 & k_2 \end{pmatrix} = \begin{pmatrix} \Delta^2 x_1' & 0 & 0 & 0 \\ 0 & \Delta^2 p_1' & 0 & 0 \\ 0 & 0 & \Delta^2 x_2' & 0 \\ 0 & 0 & 0 & \Delta^2 p_2' \end{pmatrix},$$

[7] $S_p(4, R)$ é o grupo das matrizes simpléticas reais e de dimensão 4

onde usamos a definição da matriz de variância na representação onde ela é diagonal. Como implementamos uma transformação simplética, x_1', p_1', x_2' e p_2' possuem as mesmas relações de comutação que x_1, p_1, x_2 e p_2. Dessa forma, as relações de incerteza de Heisenberg são:

$$\Delta^2 x_1' \Delta^2 p_1' \geq \frac{1}{4} \implies k_1 k_1 \geq \frac{1}{4} \Longrightarrow k_1 \geq \frac{1}{2}, \tag{2.79}$$

$$\Delta^2 x_2' \Delta^2 p_2' \geq \frac{1}{4} \implies k_2 k_2 \geq \frac{1}{4} \Longrightarrow k_2 \geq \frac{1}{2}. \tag{2.80}$$

E como uma transformação simplética não altera as relações de comutação das variáveis canônicas temos que $\Omega = \Omega'$ e, portanto,

$$V' + \frac{\mathrm{i}}{2}\Omega' = \begin{pmatrix} k_1 & \frac{\mathrm{i}}{2} & 0 & 0 \\ -\frac{\mathrm{i}}{2} & k_1 & 0 & 0 \\ 0 & 0 & k_2 & \frac{\mathrm{i}}{2} \\ 0 & 0 & -\frac{\mathrm{i}}{2} & k_2 \end{pmatrix}. \tag{2.81}$$

Diagonalizando a matriz anterior obtemos os seguintes autovalores:

$$\begin{aligned} \lambda_1 = k_1 - \frac{1}{2},\ \lambda_2 = k_1 + \frac{1}{2}, \\ \lambda_3 = k_2 - \frac{1}{2},\ \lambda_4 = k_2 + \frac{1}{2}. \end{aligned} \tag{2.82}$$

Mas como $k_j \geq 1/2$ então $\lambda_j \geq 0$. Portanto, $V' + \frac{\mathrm{i}}{2}\Omega' \geq 0$. Mas uma transformação simplética, apesar de não preservar o espectro de autovalores (não temos uma transformação de similaridade), é uma transformação que não altera a positividade de uma matriz [87]. Logo, como $V' + \frac{\mathrm{i}}{2}\Omega' = S\left(V + \frac{\mathrm{i}}{2}\Omega\right)S^T$ temos que $V + \frac{\mathrm{i}}{2}\Omega \geq 0$. □

Vamos deduzir, agora, uma outra relação de incerteza, a qual apenas estados ρ separáveis devem satisfazer. Supomos, daqui em diante, que estamos trabalhando com estados contínuos onde os momentos de primeira ordem $\langle \hat{\xi}_j \rangle$ são nulos. (Isso não altera as características dos estados que estamos estudando e nem perdemos em generalidade. Tudo se passa como se tivéssemos redefinido as origens dos eixos x e p. Uma maneira de se implementar isso consiste na mudança de variável $\xi \to \xi - \langle \xi \rangle$).

Se fizermos o produto matricial $\Lambda\Omega\Lambda$ obtemos o seguinte resultado:

$$\tilde{\Omega} = \Lambda\Omega\Lambda = \begin{pmatrix} J & 0 \\ 0 & -J \end{pmatrix}. \tag{2.83}$$

Observe que $\tilde{\Omega}$ difere de Ω por um sinal negativo em J. Agora, usando a Eq. (2.77) podemos descobrir o que acontece com V quando tomamos a transposição parcial de um estado separável ρ. Como supomos $\langle \hat{\xi}_\alpha \rangle = 0$ então:

$$V_{\alpha\beta} = \int \mathrm{d}^4\xi\, \xi_\alpha \xi_\beta W(\xi). \tag{2.84}$$

A transposição parcial na representação de Wigner é equivalente a reflexão especular $W(\xi) \to W(\Lambda\xi)$. Sendo $\tilde{V}$ a matriz de variância calculada com a distribuição de Wigner $W(\Lambda\xi)$ temos:

$$\begin{aligned}\tilde{V}_{\alpha\beta} &= \int \mathrm{d}^4\xi\, \xi_\alpha\xi_\beta W(\Lambda\xi) \\ &= \int \mathrm{d}\xi_1\mathrm{d}\xi_2\mathrm{d}\xi_3\mathrm{d}\xi_4\, \xi_\alpha\xi_\beta W(\xi_1,\xi_2,\xi_3,-\xi_4). \end{aligned} \tag{2.85}$$

Fazendo a mudança de variável $-\xi_4 \to \xi_4$ obtemos:

$$\begin{aligned}\tilde{V}_{\alpha\beta} &= \int \mathrm{d}\xi_1\mathrm{d}\xi_2\mathrm{d}\xi_3\mathrm{d}\xi_4 \sum_\mu \Lambda_{\alpha\mu}\xi_\mu \sum_\nu \Lambda_{\beta\nu}\xi_\nu W(\xi_1,\xi_2,\xi_3,\xi_4) \\ &= \sum_\mu \Lambda_{\alpha\mu} \int \mathrm{d}^4\xi\, \xi_\mu\xi_\nu W(\xi) \sum_\nu \Lambda_{\nu\beta} \\ &= \sum_\mu \sum_\nu \Lambda_{\alpha\mu} V_{\mu\nu} \Lambda_{\nu\beta}. \end{aligned} \tag{2.86}$$

Observando a Eq. (2.86) temos que:

$$\tilde{V} = \Lambda V \Lambda. \tag{2.87}$$

E usando o fato de que $\Lambda^2 = I$ temos:

$$V = \Lambda \tilde{V} \Lambda. \tag{2.88}$$

Supondo que ρ é um estado separável, então $W(\Lambda\xi)$ é uma distribuição de Wigner legítima, pois $\rho^{T_B} \Longleftrightarrow W(\Lambda\xi)$ é também matriz densidade se ρ for separável. Dessa forma, a matriz de variância calculada via $W(\Lambda\xi)$ também deve satisfazer a relação de incerteza dada pela Eq. (2.78):

$$\tilde{V} + \frac{\mathrm{i}}{2}\Omega \geq 0. \tag{2.89}$$

Usando as Eqs. (2.83) e (2.88), a Eq. (2.89) pode ser escrita da seguinte forma:

$$V + \frac{\mathrm{i}}{2}\tilde{\Omega} \geq 0. \tag{2.90}$$

A Eq. (2.90) é uma condição necessária para separabilidade. Ela também é uma condição operacional pois, dado ρ, basta calcularmos sua matriz de variância V, somar $\frac{\mathrm{i}}{2}\tilde{\Omega}$ e diagonalizar essa nova matriz. Se algum de seus autovalores for menor que zero, temos estado inseparável. Entretanto, vamos mostrar que as desigualdades dadas pelas Eqs. (2.78) e (2.90) podem ser escritas de um modo invariante por transformações unitárias locais de ρ. Nessa nova forma de escrever as Eqs. (2.78) e (2.90), obtemos ainda mais operacionalidade na aplicação do critério de separabilidade. (Não vamos precisar mais diagonalizar matrizes, por exemplo.)

Simon e Sudarshan [86] mostraram a seguinte equivalência, onde U é a transformação unitária que ρ sofre quando aplicamos a transformação simplética S em ξ:

$$\hat{\xi} \to S\hat{\xi} : \rho \to U\rho U^{\dagger} \Longleftrightarrow W(\xi) \to W(S^{-1}\xi). \tag{2.91}$$

Isto é, se ρ sofre uma transformação unitária U, sua distribuição de Wigner transforma-se em $W(S^{-1}\xi)$. Usando esse resultado podemos provar o seguinte lema, que nos será útil mais à frente:

Lema 4 *Se* $W(\xi) \to W(S^{-1}\xi)$ *então* $V \to V' = SVS^T$.

Prova:
Sabemos que (Eq. (2.84)):

$$V_{\alpha\beta} = \int \mathrm{d}^4\xi \, \xi_\alpha \xi_\beta W(\xi). \tag{2.92}$$

Então,

$$V'_{\alpha\beta} = \int \mathrm{d}^4\xi \, \xi_\alpha \xi_\beta W(S^{-1}\xi). \tag{2.93}$$

Fazendo a mudança de variável $\xi = S\xi'$ obtemos:

$$V'_{\alpha\beta} = \sum_{\mu\nu} \int \mathrm{d}^4\xi' \, |J(\xi,\xi')| S_{\alpha\mu}\xi'_\mu S_{\beta\nu}\xi'_\nu W(\xi'). \tag{2.94}$$

Aqui $|J(\xi,\xi')|$ representa o módulo da matriz Jacobiana. Mas

$$J(\xi,\xi')_{\alpha\beta} = \frac{\partial \xi_\alpha}{\partial \xi'_\beta} = \sum_\gamma S_{\alpha\gamma} \frac{\partial \xi'_\gamma}{\partial \xi'_\beta} = \sum_\gamma S_{\alpha\gamma}\delta_{\gamma\beta} = S_{\alpha\beta}.$$

Ou seja, $J(\xi,\xi') = S$. Dessa forma, como o determinante de S é igual a unidade, o módulo do determinante da matriz Jacobiana é 1.

$$\begin{aligned} V'_{\alpha\beta} &= \sum_{\mu\nu} \int \mathrm{d}^4\xi' \, S_{\alpha\mu}\xi'_\mu S_{\beta\nu}\xi'_\nu W(\xi') \\ &= \sum_{\mu\nu} S_{\alpha\mu} \int \mathrm{d}^4\xi' \, \xi'_\mu \xi'_\nu W(\xi') S_{\beta\nu} \\ &= \sum_{\mu\nu} S_{\alpha\mu} V_{\mu\nu} S^T_{\nu\beta}. \end{aligned}$$

Isto é,

$$V' = SVS^T. \qquad \square \tag{2.95}$$

A relação de incerteza dada pela Eq. (2.78) possui forma invariante por transformações simpléticas $S \in S_p(4,R)$ pois, por definição de transformação simplética, $S\Omega S^T = \Omega$. Contudo, conforme demonstramos anteriormente, estados separáveis

devem satisfazer também a Eq. (2.90). Esta última condição é invariante por transformações simpléticas locais: $S_{local} \in S_p(2,R) \otimes S_p(2,R) \subset S_p(4,R)$. Para ver isso, basta lembrarmos da representação matricial de S_{local}:

$$S_{local} = \begin{pmatrix} S_1 & 0 \\ 0 & S_2 \end{pmatrix}. \tag{2.96}$$

Como S_1, S_2 são locais, então, usando a definição de matriz simplética:

$$S_1 J S_1^T = J = S_2 J S_2^T. \tag{2.97}$$

Usando a Eq. (2.97) vemos que a Eq. (2.90) adquire forma invariante:

$$S_{local} : V + \frac{i}{2}\tilde{\Omega} \geq 0 \rightarrow V' + \frac{i}{2}\tilde{\Omega} \geq 0, \tag{2.98}$$

onde $V' = S_{local} V S_{local}^T$.

Vamos, agora, escrever a Eq. (2.78) numa forma manifestamente invariante por transformações locais $S_{local} \in S_p(2,R) \otimes S_p(2,R)$. Para chegar nesta forma invariante representamos V da seguinte maneira:

$$V = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{2.99}$$

onde A, B, e C são matrizes 2×2. Usando a Eq. (2.95) vemos que os blocos de V se transformam da seguinte forma por S_{local}:

$$A \rightarrow S_1 A S_1^T, \quad B \rightarrow S_2 B S_2^T, \quad C \rightarrow S_1 C S_2^T. \tag{2.100}$$

Usando a identidade $\det(MN) = \det M \, \det N$ e o fato de que $\det S_1 = \det S_2 = 1$ vemos que $I_1 = \det A$, $I_2 = \det B$ e $I_3 = \det C$ são invariantes por transformações simpléticas locais. Temos mais um outro invariante, $I_4 = Tr\{AJCJBJC^T J\}$. Podemos ver isso se usarmos a propriedade cíclica do traço e lembrarmos de que se S é transformação simplética então S^T também o é:

$$\begin{aligned} Tr\{AJCJBJC^T J\} &\rightarrow Tr\{(S_1 A S_1^T) J (S_1 C S_2^T) J (S_2 B S_2^T) J (S_2 C^T S_1^T) J\} \\ &\rightarrow Tr\{S_1 A (S_1^T J S_1) C (S_2^T J S_2) B (S_2^T J S_2) C^T S_1^T J\} \\ &\rightarrow Tr\{S_1 A J C J B J C^T S_1^T J\} \\ &\rightarrow Tr\{A J C J B J C^T S_1^T J S_1\} \\ &\rightarrow Tr\{A J C J B J C^T J\}. \end{aligned} \tag{2.101}$$

Usando esses invariantes podemos demonstrar que o princípio de incerteza dado pela Eq. (2.78) é equivalente à seguinte expressão invariante por transformações do grupo

$S_p(2,R) \otimes S_p(2,R)$:

$$\det A \det B + \left(\frac{1}{4} - \det C\right)^2 - Tr\{AJCJBJC^TJ\} - \frac{1}{4}(\det A + \det B) \geq 0. \quad (2.102)$$

Para demonstrar essa equivalência precisamos do seguinte lema:

Lema 5 *Qualquer matriz de variância V pode, via transformações simpléticas locais, ser posta na seguinte forma:*

$$V_0 = \begin{pmatrix} a & 0 & c_1 & 0 \\ 0 & a & 0 & c_2 \\ c_1 & 0 & b & 0 \\ 0 & c_2 & 0 & b \end{pmatrix}. \quad (2.103)$$

Prova:
Para chegar em V_0 precisamos efetuar duas transformações simpléticas locais em V, $S = S_1 \otimes S_2$ e $R = R_1 \otimes R_2$. Vamos implementar a primeira transformação simplética S:

$$V \to V' = \begin{pmatrix} A' & C' \\ C'^T & B' \end{pmatrix} = \begin{pmatrix} S_1 A S_1^T & S_1 C S_2^T \\ S_2 C^T S_1^T & S_2 B S_2^T \end{pmatrix}. \quad (2.104)$$

Pelo teorema de Williamson, podemos escolher S_1 e S_2 de tal forma que A' e B' sejam diagonais:

$$V \to V' = \begin{pmatrix} a & 0 & c'_{11} & c'_{12} \\ 0 & a & c'_{21} & c'_{22} \\ c'_{11} & c'_{21} & b & 0 \\ c'_{12} & c'_{22} & 0 & b \end{pmatrix}. \quad (2.105)$$

Agora escolhemos R_1 e R_2 da seguinte forma:

$$R_1 = \begin{pmatrix} \sin\alpha & -\cos\alpha \\ \cos\alpha & \sin\alpha \end{pmatrix}, \quad R_2 = \begin{pmatrix} \sin\beta & -\cos\beta \\ \cos\beta & \sin\beta \end{pmatrix}. \quad (2.106)$$

Além de serem matrizes simpléticas, R_1 e R_2 são matrizes ortogonais, i. e., $R_1 R_1^T = R_2 R_2^T = I$. Essa propriedade implica a invariância das matrizes A' e B' ao efetuarmos a transformação $R = R_1 \otimes R_2$ em V'. Por exemplo, $R_1 A' R_1^T = a R_1 I R_1^T = a R_1 R_1^T = aI = A'$. Por outro lado, C' se transforma em

$$C' \to C'' = R_1 C' R_2^T. \quad (2.107)$$

Os termos não diagonais de C'' são

$$\begin{aligned} c''_{12} &= (c'_{11}\cos\beta + c'_{12}\sin\beta)\sin\alpha - (c'_{21}\cos\beta + c'_{22}\sin\beta)\cos\alpha, \\ c''_{21} &= (c'_{21}\sin\beta - c'_{22}\cos\beta)\sin\alpha - (c'_{12}\cos\beta - c'_{11}\sin\beta)\cos\alpha. \end{aligned}$$

Como queremos deixar C'' diagonal, devemos impor $c''_{12} = c''_{21} = 0$. Isto implica

$$\tan\alpha = \frac{c'_{21}\cos\beta + c'_{22}\sin\beta}{c'_{11}\cos\beta + c'_{12}\sin\beta} = \frac{c'_{12}\cos\beta - c'_{11}\sin\beta}{c'_{21}\sin\beta - c'_{22}\cos\beta}. \tag{2.108}$$

Sempre podemos satisfazer a condição acima escolhendo

$$\tan(2\beta) = \frac{2\left(c'_{11}c'_{12} + c'_{21}c'_{22}\right)}{(c'_{11})^2 - (c'_{22})^2 + (c'_{21})^2 - (c'_{12})^2}\,. \tag{2.109}$$

Assim, podemos deixar C'' diagonal e, conseqüentemente, V pode sempre ser posta na forma padrão V_0 via transformações simpléticas locais. □

Agora podemos provar a equivalência entre as Eqs. (2.78) e (2.102) procedendo do seguinte modo. Tomemos a matriz V_0 e calculemos os invariantes I_1, I_2, I_3 e I_4:

$$I_1 = \det A = a^2, \tag{2.110}$$

$$I_2 = \det B = b^2, \tag{2.111}$$

$$I_3 = \det C = c_1 c_2, \tag{2.112}$$

$$i_4 = Tr\left\{AJCJBJC^TJ\right\} = ab(c_1^2 + c_2^2). \tag{2.113}$$

Sustituindo esses invariantes na Eq. (2.102) obtemos:

$$a^2b^2 + \left(\frac{1}{4} - c_1c_2\right)^2 - ab(c_1^2 + c_2^2) - \frac{1}{4}\left(a^2 + b^2\right) \geq 0. \tag{2.114}$$

Aplicando o princípio de incerteza, dado pela Eq. (2.78), obtemos:

$$M = V_0 + \frac{i}{2}\Omega = \begin{pmatrix} a & \frac{i}{2} & c_1 & 0 \\ -\frac{i}{2} & a & 0 & c_2 \\ c_1 & 0 & b & \frac{i}{2} \\ 0 & c_2 & -\frac{i}{2} & b \end{pmatrix} \geq 0. \tag{2.115}$$

Como a expressão acima é positiva definida, isto é, seus autovalores não são negativos, e o determinante de uma matriz é invariante por transformações unitárias, então seu determinante é maior ou igual a zero. Calculando este determinante:

$$\det M = a^2b^2 + \left(\frac{1}{4} - c_1c_2\right)^2 - ab(c_1^2 + c_2^2) - \frac{1}{4}\left(a^2 + b^2\right) \geq 0. \tag{2.116}$$

Comparando as Eqs. (2.114) e (2.116) vemos que elas são idênticas. Dessa forma, pelo menos para a matriz V_0, o princípio de incerteza, Eq. (2.78), e a desigualdade invariante por S_{local}, Eq. (2.102), são equivalentes. Mas usando o lema 5 vemos que qualquer matriz V pode ser escrita como V_0 por transformações simpléticas locais. Portanto, como a relação dada pela Eq. (2.102) é também invariante por transformações simpléticas locais, ela é válida para qualquer matriz de variância V. Esse resultado que acabamos de derivar é a prova do seguinte teorema:

Teorema 7 *Qualquer estado bipartido de variáveis contínuas ρ deve satisfazer a seguinte desigualdade, a qual é uma consequência do princípio de incerteza de Heisenberg:*

$$detAdetB + \left(\frac{1}{4} - detC\right)^2 - Tr\{AJCJBJC^TJ\} - \frac{1}{4}(detA + detB) \geq 0,$$

onde a matriz de variância V do estado ρ é:

$$V = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}.$$

Só nos resta escrever a condição necessária de separabilidade numa forma manifestamente invariante por transformações simpléticas locais. Isso pode ser facilmente feito se lembrarmos que aplicando o critério de transposição parcial obtemos a seguinte transformação para a matriz de variância: $V \to \tilde{V} = \Lambda V \Lambda$, isto é:

$$\begin{aligned} \tilde{V} &= \begin{pmatrix} I & 0 \\ 0 & \sigma_z \end{pmatrix} \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & \sigma_z \end{pmatrix} \\ &= \begin{pmatrix} A & C\sigma_z \\ \sigma_z C^T & \sigma_z B \sigma_z \end{pmatrix} = \begin{pmatrix} \tilde{A} & \tilde{C} \\ \tilde{C}^T & \tilde{B} \end{pmatrix}, \end{aligned} \tag{2.117}$$

onde $\sigma_z = \mathrm{diag}(1, -1)$ é a matriz de Pauli. Usando o mesmo procedimento que nos levou ao teorema 7, podemos mostrar que a condição necessária de separabilidade, Eq. (2.89), é equivalente a:

$$\det\tilde{A}\det\tilde{B} + \left(\frac{1}{4} - \det\tilde{C}\right)^2 - Tr\{\tilde{A}J\tilde{C}J\tilde{B}J\tilde{C}^TJ\} - \frac{1}{4}(\det\tilde{A} + \det\tilde{B}) \geq 0. \tag{2.118}$$

Mas,

$$\det\tilde{A} = \det A, \tag{2.119}$$

$$\det\tilde{B} = \det(\sigma_z B \sigma_z) = \underbrace{\det\sigma_z}_{-1} \det B \underbrace{\det\sigma_z}_{-1} = \det B, \tag{2.120}$$

$$\det\tilde{C} = \det(C\sigma_z) = \underbrace{\det\sigma_z}_{-1} \det C = -\det C, \tag{2.121}$$

$$\begin{aligned} Tr\{\tilde{A}J\tilde{C}J\tilde{B}J\tilde{C}^TJ\} &= Tr\left\{AJ(C\sigma_z)J(\sigma_z B\sigma_z)J(\sigma_z C^T)J\right\} \\ &= Tr\left\{AJC\underbrace{\sigma_z J\sigma_z}_{J}B\underbrace{\sigma_z J\sigma_z}_{J}C^TJ\right\} \\ &= Tr\{AJCJBJC^TJ\}. \end{aligned} \tag{2.122}$$

Dessa forma, substituindo as últimas quatro equações na Eq. (2.118) temos:

$$\det A\det B + \left(\frac{1}{4} + \det C\right)^2 - Tr\{AJCJBJC^TJ\} - \frac{1}{4}(\det A + \det B) \geq 0. \tag{2.123}$$

Esta é a condição de separabilidade escrita numa forma invariante por transformações simpléticas locais. Ela difere da Eq. (2.102) pelo sinal positivo que antecede o termo det$C$. Combinando a Eq. (2.123) com a Eq. (2.102) chegamos ao seguinte importante teorema:

Teorema 8 *Se ρ representa um estado bipartido separável de variáveis contínuas então ρ deve satisfazer a seguinte desigualdade, a qual é uma consequência do princípio de incerteza de Heisenberg e da relação entre transposição parcial de ρ e reflexões especulares do momento no espaço de fases de sua distribuição de Wigner:*

$$detAdetB + \left(\frac{1}{4} - |detC|\right)^2 - Tr\{AJCJBJC^TJ\} - \frac{1}{4}(detA + detB) \geq 0,$$

onde a matriz de variância V do estado ρ é:

$$V = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}.$$

Vamos nos preocupar agora com estados Gaussianos, os quais são completamente especificados caso se conheça sua matriz de variância V. Simon, usando propriedades que estados Gaussianos separáveis devem satisfazer, demonstrou a seguinte condição necessária e suficiente de separabilidade:

Teorema 9 *Um sistema Gaussiano bipartido é separável se, e somente se, sua matriz de variância satisfaz a desigualdade abaixo,*

$$detAdetB + \left(\frac{1}{4} - |detC|\right)^2 - Tr\{AJCJBJC^TJ\} - \frac{1}{4}(detA + detB) \geq 0, \quad (2.124)$$

onde V é dado por:

$$V = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}.$$

Prova:
A demonstração da necessidade já foi feita anteriormente para qualquer estado ρ separável. Só precisamos provar a suficiência do critério para estados Gaussianos. Para isso, precisamos do seguinte lema:

Lema 6 *Se ρ é um estado Gaussiano e det$C \geq 0$, então ele é separável.*

Prova:
Temos dois casos a considerar, det$C > 0$ e det$C = 0$. Comecemos por det$C > 0$, o que nos permite escrever a matriz V_0, dada pela Eq. (2.103), de tal forma que $a \geq b$, $c_1 \geq c_2 > 0$. Em seguida implementamos a transformação simplética

$S_{local} = \mathrm{diag}(x, x^{-1}, x^{-1}, x)$ e $S'_{local} = \mathrm{diag}(y, y^{-1}, y, y^{-1})$. Obtemos a seguinte matriz $V'_0 = S'_{local} S_{local} V_0 S_{local} S'_{local}$:

$$V_0 \to V'_0 = \begin{pmatrix} y^2x^2a & 0 & y^2c_1 & 0 \\ 0 & y^{-2}x^{-2}a & 0 & y^{-2}c_2 \\ y^2c_1 & 0 & y^2x^{-2}b & 0 \\ 0 & y^{-2}c_2 & 0 & y^{-2}x^2b \end{pmatrix}. \tag{2.125}$$

Seja a U a transformação de similaridade ($UU^T = I$) abaixo:

$$U = \begin{pmatrix} \cos\theta & 0 & \sin\theta & 0 \\ 0 & \cos\theta & 0 & \sin\theta \\ -\sin\theta & 0 & \cos\theta & 0 \\ 0 & -\sin\theta & 0 & \cos\theta \end{pmatrix}. \tag{2.126}$$

Essa transformação pode ser interpretada como rotações por um mesmo ângulo θ nos planos q_1, q_2 e p_1, p_2. Mas rotações idênticas nos eixos da posição e do momento são também transformações simpléticas ($U\Omega U^T = \Omega$), veja:

$$U\Omega U^T = \begin{pmatrix} 0 & u^2+v^2 & 0 & 0 \\ -u^2-v^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & u^2+v^2 \\ 0 & 0 & -u^2-v^2 & 0 \end{pmatrix}, \tag{2.127}$$

onde $u = \cos\theta$ e $v = \sin\theta$. Dessa forma,

$$U\Omega U^T = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} = \Omega. \tag{2.128}$$

Apliquemos a transformação U na matriz V'_0:

$$V''_0 = UV'_0U^T = \begin{pmatrix} v''_{11} & 0 & v''_{13} & 0 \\ 0 & v''_{22} & 0 & v''_{24} \\ v''_{13} & 0 & v''_{33} & 0 \\ 0 & v''_{24} & 0 & v''_{44} \end{pmatrix}, \tag{2.129}$$

onde v''_{jk} são:

$$v''_{11} = \frac{y^2\left(a\,x^4\,\cos^2\theta + c_1\,x^2\,\sin(2\,\theta) + b\,\sin^2\theta\right)}{x^2}, \tag{2.130}$$

$$v''_{22} = \frac{a\,\cos^2\theta + c_2\,x^2\,\sin(2\,\theta) + b\,x^4\,\sin^2\theta}{x^2\,y^2}, \tag{2.131}$$

$$v''_{33} = \frac{y^2\left(b\,\cos^2\theta - c_1\,x^2\,\sin(2\,\theta) + a\,x^4\,\sin^2\theta\right)}{x^2}, \tag{2.132}$$

$$v''_{44} = \frac{b\,x^4\,\cos^2\theta - c_2\,x^2\,\sin(2\,\theta) + a\,\sin^2\theta}{x^2\,y^2}, \tag{2.133}$$

$$v''_{13} = \frac{y^2\left(2\,c_1\,x^2\,\cos(2\,\theta) + \left(b - a\,x^4\right)\,\sin(2\,\theta)\right)}{2\,x^2}, \tag{2.134}$$

$$v''_{24} = \frac{2\,c_2\,x^2\,\cos(2\,\theta) + \left(b\,x^4 - a\right)\,\sin(2\,\theta)}{2\,x^2\,y^2}. \tag{2.135}$$

Queremos que V''_0 fique diagonal. Devemos, pois, impor $v''_{13} = v''_{24} = 0$. Isso nos leva a um sistema linear em $\cos 2\theta$ e $\sin 2\theta$:

$$2\,c_1\,x^2\,\cos(2\,\theta) + \left(b - a\,x^4\right)\,\sin(2\,\theta) = 0 \tag{2.136}$$

$$2\,c_2\,x^2\,\cos(2\,\theta) + \left(b\,x^4 - a\right)\,\sin(2\,\theta) = 0. \tag{2.137}$$

Para que o sistema acima tenha solução, o determinante abaixo deve ser nulo:

$$\begin{vmatrix} 2\,c_1\,x^2 & b - a\,x^4 \\ 2\,c_2\,x^2 & b\,x^4 - a \end{vmatrix} = 0. \tag{2.138}$$

Para que o determinante acima seja nulo, basta tomarmos x dado por:

$$x = \left(\frac{bc_2 + ac_1}{bc_1 + ac_2}\right)^{\frac{1}{4}}. \tag{2.139}$$

Sempre podemos escolher x dessa forma pois supomos $c_1 \geq c_2 > 0$. (a e b também são positivos pois, por definição, os elementos diagonais da matriz V correspondem as dispersões na posição e momento, as quais, por sua vez, são grandezas sempre não negativas.) Calculando explicitamente os autovalores de V''_0 obtemos a seguinte matriz diagonal:

$$V''_0 = \mathrm{diag}(v''_{11} = \lambda_+, v''_{22} = \lambda'_+, v''_{33} = \lambda_-, v''_{44} = \lambda'_-), \tag{2.140}$$

onde os autovalores são dados por:

$$\lambda_\pm = \frac{y^2}{2}\left[ax^2 + \frac{b}{x^2} \pm \sqrt{\left(ax^2 - \frac{b}{x^2}\right)^2 + 4c_1^2}\right], \tag{2.141}$$

$$\lambda'_\pm = \frac{1}{2y^2}\left[\frac{a}{x^2} + bx^2 \pm \sqrt{\left(\frac{a}{x^2} - bx^2\right)^2 + 4c_2^2}\right]. \tag{2.142}$$

Como U é transformação simplética, V_0'' obedece as relações de incerteza de Heisenberg dadas pela Eq. (2.78). Dessa forma, $\lambda_-\lambda'_- \geq 1/4$. Escolhendo y de tal forma que $\lambda_- = \lambda'_-$ obtemos $\lambda_+, \lambda'_+ \geq \lambda_- = \lambda'_- \geq 1/2$. Portanto, todos os autovalores de V_0'' são maiores ou iguais a $1/2$, isto é,

$$V_0'' - \frac{1}{2}I \geq 0. \tag{2.143}$$

Mas a Eq. (2.143) implica um estado Gaussiano P-representável (separável) [32]. Como V_0' e V_0'' estão relacionadas por uma transformação unitária, $V_0' \geq 1/2$, isto é, V_0' representa um estado separável. Mas V_0 e V_0', por sua vez, estão relacionadas por transformações simpléticas locais. Logo, V_0 corresponde a um estado separável.

Tomemos, agora, $\det C = 0$. Supomos, sem perda de generalidade, que $c_1 \geq c_2 = 0$. Implementando, em V_0, a seguinte transformação simplética local, $S_{local} = \mathrm{diag}(\sqrt{2a}, 1/\sqrt{2a}, \sqrt{2b}, 1/\sqrt{2b})$, temos:

$$V_0' = \begin{pmatrix} 2a^2 & 0 & 2c_1\sqrt{ab} & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 2c_1\sqrt{ab} & 0 & 2b^2 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}. \tag{2.144}$$

Diagonalizando a matriz V_0' obtemos os seguintes autovalores:

$$\kappa_1 = \kappa_2 = \frac{1}{2}, \tag{2.145}$$

$$\kappa_\pm = a^2 + b^2 \pm \sqrt{(a^2 - b^2)^2 + 4abc_1^2}. \tag{2.146}$$

Como V_0' é obtida de V_0 via transformação simplética local, ela satizfaz a Eq. (2.78):

$$M' = V_0' + \frac{i}{2}\Omega \geq 0. \tag{2.147}$$

Um dos autovalores de M' é:

$$\kappa = \frac{1}{4}\left(1 + 2\kappa_- - \sqrt{5 - 4\kappa_- + 4\kappa_-^2}\right). \tag{2.148}$$

Como $M' \geq 0$ então $\kappa \geq 0$. Resolvendo para κ_- encontramos que $\kappa_- \geq 1/2$. Mas κ_- é menor que κ_+. Dessa forma, $V_0' - I/2 \geq 0$. Como V_0 relaciona-se com V_0' por transformação local, então V_0 é separável.

Acabamos de mostrar que se $\det C \geq 0$ então V_0 é separável. Mas, de acordo com o lema 5, qualquer matriz de variância V pode ser posta na forma de V_0 via transformações simpléticas locais. Logo, como $\det C$ é um invariante por trasformações simpléticas locais, podemos aplicar o critério diretamente em V. □

Podemos, agora, finalizar a demonstração do teorema. Há dois casos distintos a considerar em nossa análise:

(1) A matriz V satizfaz a Eq. (2.124) e $\det C \geq 0$;

(2) A matriz V satizfaz a Eq. (2.124) e $\det C < 0$.

No caso 1, como $\det C \geq 0$, o lema 6 garante que V representa um estado ρ separável. No caso 2, $\det C < 0$, podemos tomar a transposição parcial de ρ. Isso nos gera um novo estado $\tilde{\rho}$, cuja matriz de variância é $\tilde{V}$. Em virtude da Eq. (2.121) obtemos $\det \tilde{C} = -\det C > 0$. Então, por força do lema 6, esse estado é separável. Mas se $\tilde{\rho}$ é separável, então o estado ρ também o é, pois a transposição parcial de um estado separável também é separável. Ou seja, se ρ satisfaz a Eq. (2.124) então ρ é separável. □

2.5 Detecção Local de Emaranhamento

Os critérios de emaranhamento apresentados nas últimas seções só podem ser implementados se conhecemos o estado ρ que descreve nosso sistema composto. Através da matriz densidade podemos dizer se lidamos com sistemas emaranhados ou com sistemas separáveis. Mas uma pergunta naturalmente surge neste contexto. Podemos afirmar se temos emaranhamento entre dois subsistemas se não conhecemos completamente ρ?

Para estados puros ($\mathrm{Tr}(\rho^2) = 1$) é facil ver que se conhecemos uma das matrizes reduzidas do sistema podemos decidir se temos emaranhamento. Caso a matriz reduzida seja pura ($\mathrm{Tr}(\rho_1^2) = 1$) o sistema é separável, estando emaranhado quando ρ_1 é não pura ($\mathrm{Tr}(\rho_1^2) < 1$). Isto é, se temos alguma informação *prévia* do sistema em questão (lidamos com estado puro), podemos decidir sobre seu emaranhamento sem conhecermos seu estado global.

No entanto, para testar a pureza da matriz reduzida, precisamos conhecê-la completamente. Podemos novamente nos indagar se é possível discernir se um sistema puro está emaranhado conhecendo-se apenas *parcialmente* sua matriz densidade reduzida. Lidando com estados contínuos respondemos afirmativamente a questão anterior. Conhecendo-se apenas os elementos diagonais da matriz reduzida de um dos subsistemas, podemos decidir se temos ou não emaranhamento [72].

Para mostrar isso explicitamente, construímos uma função de onda descrevendo duas partículas Gaussianas não-emaranhadas e uma função de onda descrevendo duas partículas Gaussianas emaranhadas. Deixando ambos os sistemas evoluírem livremente no tempo, mostramos que estudando uma única partícula de cada sistema, obtemos resultados diferentes na evolução temporal da dispersão da posição para essas partículas. Como será exposto abaixo, esse fato nos permite mostrar se estamos trabalhando com um sistema emaranhado ou não emaranhado, e que, no caso de sistema emaranhado, podemos também extrair, dessa evolução temporal, seu grau de emaranhamento.

2.5.1 Sistema Bipartite Não Emaranhado

Considere um sistema unidimensional de duas partículas Gaussianas não-emaranhadas. Sem perder em generalidade, supomos que as partículas possuem a mesma massa m e podem, em princípio, ser distinguidas. A função de onda que descreve esse sistema é:

$$\psi(x_1, x_2, t) = \psi_1(x_1, t) \otimes \psi_2(x_2, t), \tag{2.149}$$

onde

$$\psi_1(x_1, t) = \int f(k_1) e^{\mathrm{i}[k_1 x_1 - \omega(k_1)t]} \mathrm{d}k_1, \tag{2.150}$$

$$\psi_2(x_2, t) = \int f(-k_2) e^{\mathrm{i}[k_2 x_2 - \omega(k_2)t]} \mathrm{d}k_2. \tag{2.151}$$

Aqui $\omega(k) = \frac{\hbar k^2}{2m}$ é a relação de dispersão para partícula livre e $f(k_1)$ e $f(-k_2)$ representam o fato de que temos partículas Gaussianas movendo-se em direções opostas [25]:

$$f(k) = \frac{\sqrt{a}}{(2\pi)^{3/4}} e^{-\frac{a^2}{4}(k-k_c)^2}. \tag{2.152}$$

Na Eq. (2.152), a^{-1} representa a dispersão do pacote gaussiano centrado em k_c e o fator que multiplica a exponencial é a constante de normalização.

Integrando nas variáveis k_1 e k_2, multiplicando o resultado pelo seu complexo conjugado e integrando em x_2 obtemos a densidade de probabilidade da partícula 1 para um dado tempo t:

$$|\varphi(x_1, t)|^2 = \sqrt{\frac{2}{\pi a^2}} \frac{1}{\sqrt{1 + F(t)}} \exp\left[-\frac{2}{a^2} \frac{(x_1 - v_c t)^2}{1 + F(t)}\right], \tag{2.153}$$

onde $F(t)$ e v_c são dados por:

$$F(t) = \frac{4\hbar^2 t^2}{m^2 a^4}, \qquad v_c = \frac{\hbar k_c}{m}. \tag{2.154}$$

Usando a Eq. (2.153), a dispersão $\Delta x_1 = \sqrt{\langle x_1^2 \rangle - \langle x_1 \rangle^2}$ da posição da partícula 1 é

$$\Delta x_1(t) = \frac{a}{2}\sqrt{1 + F(t)}. \tag{2.155}$$

Tomando a transformada de Fourier da Eq. (2.149), multiplicando o resultado pelo seu complexo conjugado e integrando em k_2 obtemos:

$$|\tilde{\varphi}(k_1, t)|^2 = \sqrt{\frac{a^2}{2\pi}} \exp\left[-\frac{a^2}{2}(k_1 - k_c)^2\right]. \tag{2.156}$$

Usando a Eq. (2.156) e o fato de que $p_1 = \hbar k_1$ facilmente obtemos a dispersão do momento:

$$\Delta p_1(t) = \frac{\hbar}{a}. \tag{2.157}$$

Como esperado para uma partícula livre, sua dispersão do momento é constante no tempo.

2.5.2 Sistema Bipartite Emaranhado

Agora vamos construir um sistema bipartite Gaussiano emaranhado. Novamente ambas as partículas são distinguíveis e possuem a mesma massa m.

$$\Psi(x_1, x_2, t = 0) = \int \mathrm{d}k_1 \mathrm{d}k_2 f(k_1, k_2) \psi_1(x_1, 0) \otimes \psi_2(x_2, 0). \tag{2.158}$$

Aqui $\psi_1(x_1, 0)$ e $\psi_2(x_2, 0)$ são dados por:

$$\psi_1(x_1, 0) = \mathrm{e}^{\mathrm{i}k_1 x_1} \mathrm{e}^{\frac{-x_1^2}{a^2}}, \tag{2.159}$$

$$\psi_2(x_2, 0) = \mathrm{e}^{\mathrm{i}k_2 x_2} \mathrm{e}^{\frac{-x_2^2}{a^2}}. \tag{2.160}$$

A Eq. (2.158) é uma superposição de pacotes Gaussianos bipartites centrados em k_1 e k_2, onde $f(k_1, k_2) = g(k_1, k_2)\ \delta(k_1 + k_2)$ são os coeficientes de expansão e $\delta(k_1 + k_2)$ é uma restrição que emaranha o sistema. Essa função delta faz com que o momento seja conservado. No referencial de centro de massa, podemos entender a função de onda acima como uma superposição de pacotes Gaussianos movendo-se em direções opostas com o mesmo momento. E mais, as Eqs. (2.159) e (2.160) são proporcionas às Eqs. (2.150) e (2.151). Para ver isso, basta integrá-las em $t = 0$ e substituir k_c por k_1 e k_2, respectivamente.

Usando a função delta, a Eq. (2.158) pode ser reescrita como:

$$\Psi(x_1, x_2, 0) = \int \mathrm{d}k_1 g(k_1) \left(\mathrm{e}^{\mathrm{i}k_1 x_1} \mathrm{e}^{\frac{-x_1^2}{a^2}}\right) \left(\mathrm{e}^{-\mathrm{i}k_1 x_2} \mathrm{e}^{\frac{-x_2^2}{a^2}}\right). \tag{2.161}$$

A Eq. (2.161) claramente mostra que $\delta(k_1 + k_2)$ emaranha o sistema, pois $\Psi(x_1, x_2, 0)$ não pode ser escrita como um simples produto tensorial de funções de onda pertencentes às partículas 1 e 2, i. e., lidamos agora com funções de onda inseparáveis. Apenas se $g(k_1)$ for outra função delta, o sistema será separável e recuperamos a Eq. (2.149). Na Eq. (2.161), escolhemos $g(k_1)$ como sendo uma distribuição Gaussiana centrada em k_c:

$$g(k_1) = \sqrt{\frac{2}{\pi a^2}} f_2^{\frac{1}{4}} \frac{(b/2)}{\sqrt{\pi}} \exp\left[-(b/2)^2 (k_1 - k_c)^2\right], \tag{2.162}$$

onde b é um novo parâmetro que mede o grau de emaranhamento como explicado mais à frente e $f_n = 1 + n\frac{a^2}{b^2}$, $n = 1, 2$. Quando $b \to \infty$ a função $\frac{(b/2)}{\sqrt{\pi}} \exp\left[-(b/2)^2 (k_1 - k_c)^2\right] \to \delta(k_1 - k_c)$ [2] e $f_2 \to 1$, mostrando que não temos mais emaranhamento. Podemos ver isso por meio do seguinte cálculo. Usando as Eqs. (2.162) e (2.161),

$$\lim_{b \to \infty} \Psi(x_1, x_2, 0) = \left[\left(\frac{2}{\pi a^2}\right)^{1/4} \mathrm{e}^{\mathrm{i}k_c x_1} \mathrm{e}^{\frac{-x_1^2}{a^2}}\right] \otimes \left[\left(\frac{2}{\pi a^2}\right)^{1/4} \mathrm{e}^{-\mathrm{i}k_c x_2} \mathrm{e}^{\frac{-x_2^2}{a^2}}\right]. \tag{2.163}$$

A Eq. (2.163) é idêntica à Eq. (2.149), se calculamos as integrais nas Eqs. (2.150) e (2.151). Além disso, pode-se mostrar que se $b \to 0$ e $a \to \infty$, a Eq. (2.161) é exatamente o estado EPR com $x_0 = 0$ [32]. Como dito na Ref. [32], a Eq. (2.161) pode ser interpretada como uma generalização da função de onda de EPR. Este dois fatos sugerem que b pode ser considerado como uma medida do grau de emaranhamento, na qual $b \to \infty$ representa estado separável e $b \to 0$ representa um estado de máximo emaranhamento.

Integrando a Eq. (2.161) obtemos o estado bipartite Gaussiano normalizado para $t = 0$:

$$\Psi(x_1, x_2, 0) = \sqrt{\frac{2}{\pi a^2}} f_2^{\frac{1}{4}} \exp[\mathrm{i}k_c(x_1 - x_2)] \exp\left[-\frac{f_1}{a^2}(x_1^2 + x_2^2) + \frac{2}{b^2}x_1 x_2\right]. \quad (2.164)$$

É interessante notar que a Eq. (2.164) representa um estado inseparável devido ao termo $\exp\left[\frac{2}{b^2}x_1 x_2\right]$. Se $b \to \infty$ este termo tende a 1 e obtemos a Eq. (2.149) como caso limite da Eq. (2.164). Em outras palavras, quando $b \to \infty$ obtemos a Eq. (2.149), um estado separável, não emaranhado. Para qualquer outro valor de b temos a Eq. (2.164), um estado inseparável, emaranhado.

Para provarmos que b nos dá o grau de emaranhamento do estado descrito pela Eq. (2.164) e que somente quando $b \to \infty$ temos estado não emaranhado, calculamos sua matriz de correlação (MC) e aplicamos, em seguida, o critério de separabilidade de Simon [88] discutido anteriormente. Este critério nos diz que lidamos com estado Gaussiano separável se, e somente se, $b \to \infty$. Em seguida, realizando uma transformação simplética local na MC para deixá-la na forma padrão [88, 26], calculamos o Emaranhamento de Formação (EoF) [36], o qual é uma função monotonicamente decrescente do parâmetro b, provando que quanto maior b menos emaranhado está nosso sistema. No Cap. 3 discutiremos em detalhes essa medida.

Um estado Gaussiano de dois modos é completamente especificado por sua MC. Ela é uma matriz 4×4, possuindo os seguintes elementos [88, 26]:

$$\gamma_{ij} = \mathrm{Tr}\left[(R_i R_j + R_j R_i)\rho\right] - 2\mathrm{Tr}[R_i\rho]\mathrm{Tr}[R_j\rho], \quad (2.165)$$

onde $R = (X_1, P_1, X_2, P_2)^T$ e R_j são os operadores de posição e momento das duas partículas. Assim,

$$\gamma = \begin{pmatrix} A & C \\ C^T & A \end{pmatrix}, \quad (2.166)$$

onde

$$A = \begin{pmatrix} \frac{a^2 f_1}{2 f_2} & 0 \\ 0 & \frac{2\hbar^2 f_1}{a^2} \end{pmatrix}, \quad C = \begin{pmatrix} \frac{a^4}{2b^2 f_2} & 0 \\ 0 & -\frac{2\hbar^2}{b^2} \end{pmatrix}. \quad (2.167)$$

Como mostramos nas seções anteriores, o critério de separabilidade de Simon garante

que a MC representa um sistema separável se, e somente se,[8]

$$I = \det A \det B + \left(\hbar^2 - |\det C|\right)^2 - \mathrm{Tr}\{AJCJBJC^T J\} - \hbar^2(\det A + \det B) \geq 0, \quad (2.168)$$

onde

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Mas um cálculo simples mostra que

$$I = -4\hbar^4 \frac{a^4}{b^4}\frac{1}{f_2}. \quad (2.169)$$

Logo, $I < 0$ exceto quando $b \to \infty$, provando que para qualquer outro valor de b temos emaranhamento.

Implementando, agora, a transformação simplética $S = \mathrm{diag}\ (s,\ s^{-1},\ s,\ s^{-1})$, onde $s = \left(4\hbar^2 f_2/a^4\right)^{1/4}$, deixamos γ em sua forma padrão $\gamma_0 = S\gamma S^T$:

$$\gamma_0 = \begin{pmatrix} n & 0 & k_x & 0 \\ 0 & n & 0 & -k_p \\ k_x & 0 & n & 0 \\ 0 & -k_p & 0 & n \end{pmatrix}, \quad (2.170)$$

onde $n = \hbar f_1/\sqrt{f_2}$ e $k_x = k_p = \hbar a^2/(b^2\sqrt{f_2})$. Esta é uma MC de um estado Gaussiano simétrico e conforme mostraremos no Cap. 3 seu EoF vale

$$EoF(\Psi) = f\left[\sqrt{(n-k_x)(n-k_p)}\right], \quad (2.171)$$

onde,

$$f(\delta) = c_+(\delta)\ \log_2[c_+(\delta)] - c_-(\delta)\ \log_2[c_-(\delta)]. \quad (2.172)$$

Aqui $c_\pm(\delta) = (\delta^{-1/2} \pm \delta^{1/2})^2/4$. Analisando o comportamento do EoF dado pela Eq. (2.171) vemos claramente que ele é função decrescente do parâmetro b (Figs. 2.1 e 2.2).

Agora que temos $\Psi(x_1, x_2, 0)$ podemos expandi-lo nos autoestados de momento e calcular a função de onda para qualquer t:

$$\Psi(x_1, x_2, t) = \int \mathrm{d}k_1 \mathrm{d}k_2 c(k_1, k_2) \mathrm{e}^{\mathrm{i}[k_1 x_1 + k_2 x_2 - \omega(k_1)t - \omega(k_2)t]}, \quad (2.173)$$

onde os coeficientes de expansão são

$$c(k_1, k_2) = \frac{1}{(2\pi)^2}\int \Psi(x_1, x_2, 0) e^{-\mathrm{i}k_1 x_1} e^{-\mathrm{i}k_2 x_2} \mathrm{d}x_1 \mathrm{d}x_2. \quad (2.174)$$

[8]Para recuperar o critério de Simon conforme mostramos na seção anterior, devemos trocar $\hbar^2$ na Eq. (2.168) por $\hbar^2/4$. Esta diferença se deve ao fato de que Simon usou uma definição de matriz de correlação como sendo metade da adotada aqui. Usamos a notação de Duan *et al.* [26], pois no Cap. 3, ela nos será útil.

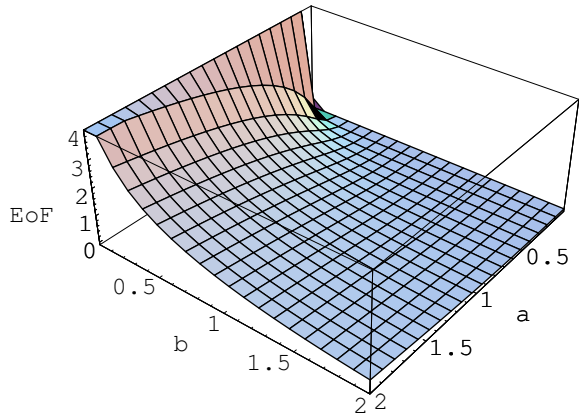


Figura 2.1: Emaranhamento de formação, Eq. (2.171), para o estado Gaussiano simétrico descrito pela Eq. (2.164), como função dos parâmetros a e b. Aqui, $\hbar = 1$. O EoF aumenta quando $b \to 0$ e diminui quando $a \to 0$.

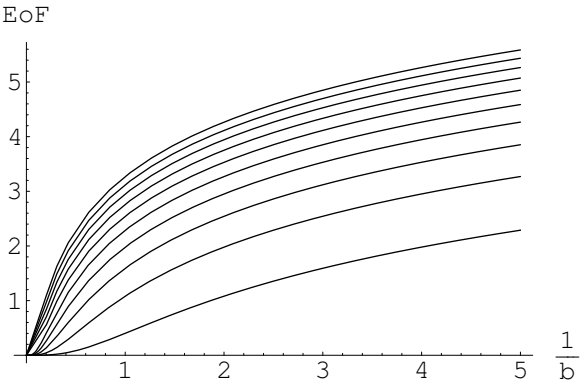


Figura 2.2: Emaranhamento de formação, Eq. (2.171), como função de $1/b$ para 10 valores de a. De baixo para cima, a varia de 1 a 10 em incrementos de uma unidade. Novamente, $\hbar = 1$. Vemos que o EoF aumenta se b diminui e, para um dado b, quanto maior a, maior o EoF.

Calculando as duas integrais na Eq. (2.174) temos

$$c(k_1,k_2) = \frac{a\mathrm{e}^{-\frac{a^2k_c^2}{2f_2}}}{\sqrt{8\pi^3}f_2^{1/4}} \exp\left[-\frac{a^2f_1(k_1^2+k_2^2)}{4f_2} + \frac{a^2k_c(k_1-k_2)}{2f_2} - \frac{a^4k_1k_2}{2b^2f_2}\right]. \quad (2.175)$$

Usando as Eqs. (2.175) e (2.173), integrando em k_1 e k_2, e multiplicando o resultado

pelo seu complexo conjugado temos

$$\begin{aligned}|\Psi(x_1,x_2,t)|^2 &= \mathcal{A}(t)\exp\{-\mathcal{B}(t)\left[f_1(1+f_2F(t))(x_1^2+x_2^2)\right.\\ &\quad -a^2f_2(1+F(t))\sqrt{F(t)}k_c(x_1-x_2)\\ &\quad \left.-(2a^2/b^2)(1-f_2F(t))x_1x_2\right]\},\end{aligned} \tag{2.176}$$

onde $\mathcal{A}(t)$ e $\mathcal{B}(t)$ são:

$$\mathcal{A}(t)=\frac{2}{\pi a^2}\sqrt{\frac{f_2}{(1+F(t))(1+f_2^2F(t))}}\,\mathrm{e}^{-\frac{a^2k_c^2f_2F(t)}{1+f_2^2F(t)}}, \tag{2.177}$$

$$\mathcal{B}(t)=\frac{2}{a^2(1+F(t))(1+f_2^2F(t))}. \tag{2.178}$$

Finalmente, integrando a Eq. (2.176) em x_2 obtemos a densidade de probabilidade da partícula 1 no tempo t:

$$|\Phi(x_1,t)|^2=\sqrt{\frac{2f_2}{\pi a^2f_1}}\frac{1}{\sqrt{1+f_2F(t)}}\exp\left[-\frac{2f_2}{a^2f_1}\frac{(x_1-v_ct)^2}{1+f_2F(t)}\right]. \tag{2.179}$$

Usando a Eq. (2.179) para calcular a dispersão na posição da partícula 1 obtemos

$$\Delta x_1(t)=\frac{a}{2}\sqrt{\frac{f_1}{f_2}[1+f_2F(t)]}. \tag{2.180}$$

A partir da transformada de Fourier da Eq. (2.173) obtemos a função de onda na representação de momentos:

$$\tilde{\Psi}(k_1,k_2,t)=2\pi c(k_1,k_2)\mathrm{e}^{-\mathrm{i}[\omega(k_1)+\omega(k_2)]t}. \tag{2.181}$$

Multiplicando a Eq. (2.181) pelo seu complexo conjugado e integrando em k_2 temos

$$|\tilde{\Phi}(k_1,t)|^2=\sqrt{\frac{a^2}{2\pi f_1}}\exp\left[-\frac{a^2}{2f_1}(k_1-k_c)^2\right]. \tag{2.182}$$

Lembrando que $p_1=\hbar k_1$ e usando a Eq. (2.182) facilmente calculamos a dispersão do momento da partícula 1:

$$\Delta p_1(t)=\frac{\hbar}{a}\sqrt{f_1}. \tag{2.183}$$

De novo, devido a evolução livre da partícula 1, a dispersão do momento é constante no tempo.

2.5.3 O Protocolo de Medida

Agora que já temos todas as ferramentas (dispersões do momento e da posição para os casos emaranhado e não emaranhado) apresentamos um procedimento de medida, o qual, usado num ensemble de pares de partículas Gaussianas, nos permite detectar localmente se o par está emaranhado bem como seu grau de emaranhamento. Lembramos que, por simplicidade, $\hbar = m = 1$.

Seja Bob nosso físico, o qual recebe uma das partículas do par produzido por Alice. Bob sabe, pois Alice lhe disse, que todas as partículas por ele recebidas são ou pacotes gaussianos emaranhados ou não emaranhados, de acordo com os dois modelos descritos acima. Não há outra possibilidade. Alice produz muitos pares de uma vez. E continua a produzir muitos pares de uma vez para vários instantes de tempo. Bob, claro, não sabe quais os valores dos parâmetros a e b usados por Alice. No entanto, Bob é curioso o suficiente e deseja saber se suas partículas estão emaranhadas ou não. Bob não pode se utilizar de nenhuma comunicação clássica, ele só pode atuar localmente em suas partículas e, para piorar sua situação mais um pouco, ele só dispõe de aparatos de medidas para detectar as dispersões na posição e no momento de suas partículas. Para saciar sua curiosidade, ele procede da seguinte maneira.

Primeiro ele mede, usando um subensemble, a dispersão dos momentos de seu pacote de onda. Ele mede $\Delta p_1 = u$. Ele ainda não sabe se é a Eq. (2.157) ou a Eq. (2.183) que representa sua medida. Mas ele tem certeza que só pode ser uma das duas possibilidades acima, o que implica somente dois tipos de evolução temporal para a dispersão da posição de suas partículas.

Se suas partículas não estão emaranhadas e Bob usa na Eq. (2.155) o fato de que $\Delta p_1(t) = u = \frac{1}{a}$ temos:

$$\Delta x_1(t) = \frac{1}{2u}\sqrt{1 + 4u^4 t^2}. \tag{2.184}$$

Todavia, se as partículas de Bob estão emaranhadas e agora ele usa o fato de que $\Delta p_1(t) = u = \frac{\sqrt{f_1}}{a}$, a Eq. (2.180) torna-se:

$$\Delta x_1(t) = \frac{1}{2u}\sqrt{\frac{u^4 b^4}{u^4 b^4 - 1} + 4u^4 t^2}. \tag{2.185}$$

Olhando para as Eqs. (2.184) e (2.185) vemos que se Bob sabe quando Alice produziu os pares ele é capaz de descobrir, com apenas uma medida de Δx_1, se suas partículas estão emaranhadas ou não. E a razão é simples: Suponhamos, sem perder em generalidade, que Alice inicia a produzir os pares em $t = 0$. Medindo a dispersão da posição para um dado tempo t Bob obtém $\Delta x_1(t)$. Lembrando que Bob também conhece o valor de u, ele pode, usando a Eq. (2.184), calcular o valor de $\Delta x_1(t)$. Se esse valor calculado para a dispersão é o mesmo do que aquele medido, as partículas

de Bob não estão emaranhadas com as de Alice. Se $\Delta x_1(t)$ difere do valor medido, temos emaranhamento. Neste último caso, usando a Eq. (2.185), Bob pode obter o valor de b. Para qualquer t Bob pode usar esse procedimento. Na verdade, Bob vê duas curvas distintas para a evolução temporal de $\Delta x_1(t)$, dependendo se suas partículas estão ou não emaranhadas. Veja a Fig. 2.3.

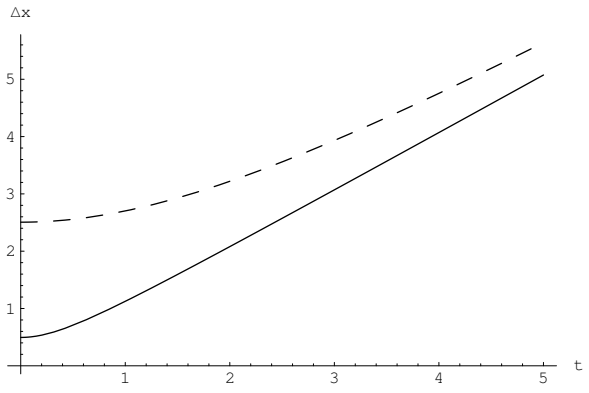


Figura 2.3: A curva tracejada é a evolução temporal da dispersão da posição para um pacote de onda gaussiano emaranhado enquanto a curva sólida representa o caso não emaranhado. Escolhemos $b = 1$ e $u = 1.01$.

Analisando a Eq. (2.185) vemos que para ela ser válida para todo tempo $t \geq 0$ devemos impor:

$$ub > 1. \tag{2.186}$$

Vale a pena notar que assintoticamente as Eqs. (2.184) e (2.185) são idênticas. Por conseguinte, a fim de que Bob consiga corretamente distinguir entre os dois casos, ele deve realizar suas medidas para tempos menores que um tempo crítico t_c, o qual é definido como sendo o tempo onde o termo independente de t dentro da raiz quadrada da Eq. (2.185) é da ordem do termo t^2:

$$t_c \approx \frac{b^2}{2\sqrt{u^4 b^4 - 1}}. \tag{2.187}$$

Podemos aumentar t_c fazendo $ub \to 1$. Isso pode parecer uma limitação desse procedimento, mas como Alice envia uma mensagem clássica a Bob definindo a origem do tempo, Bob pode começar as medidas tão cedo quanto possível.

Vamos, agora, complicar ainda mais a vida de Bob. Supomos, daqui para frente, que Bob não sabe quando Alice começou a produzir os pares. Isso significa que Bob não pode usar o protocolo anterior a fim de descobrir se suas partículas estão emaranhadas com as de Alice. O procedimento anterior falha porque Bob não sabe qual tempo t deve usar para calcular $\Delta x(t)$.

Primeiramente provamos porque uma única medida no tempo t não é suficiente para Bob dizer se suas partículas estão ou não emaranhadas, supondo que ele não

saiba quando Alice começou a produzir os pares de partículas. A idéia da prova reside em mostrar que os elementos diagonais da matriz densidade reduzida dos estados não emaranhados podem sempre ser confundidos com os elementos diagonais da matriz reduzida dos estados emaranhados no tempo $t = 0$. O mesmo raciocínio se aplica para qualquer t, mas para $t = 0$ a demonstração é mais simples e não perdemos, com essa escolha, em generalidade.

Na representação dos momentos e para $t = 0$, os elementos diagonais da matriz reduzida que descreve uma das partículas do par emaranhado são dados pela Eq. (2.182):

$$\varrho_1(k_1) = \int \langle k_1, k_2|\, \Psi \,\rangle\langle\, \Psi \,|k_1, k_2\rangle \, \mathrm{d}k_2 = \sqrt{\frac{a^2}{2\pi f_1}} \exp\left[-\frac{a^2}{2f_1}(k_1 - k_c)^2\right]. \qquad (2.188)$$

De acordo com a Eq. (2.156), para qualquer t, os elementos diagonais, na representação dos momentos, da matriz reduzida de um dos membros do par não emaranhado é

$$\rho_1(k_1, t) = \int \langle k_1, k_2|\, \psi \,\rangle\langle\, \psi \,|k_1, k_2\rangle \, \mathrm{d}k_2 = \sqrt{\frac{a'^2}{2\pi}} \exp\left[-\frac{a'^2}{2}(k_1 - k_c)^2\right]. \qquad (2.189)$$

Se queremos elementos diagonais idênticos para a matriz reduzida devemos impor

$$a' = \frac{a}{\sqrt{f_1}} = \frac{1}{u}. \qquad (2.190)$$

De acordo com a Eq. (2.179), os elementos diagonais da matriz reduzida de um dos membros do par emaranhado, na representação de posição, para $t = 0$ é

$$\varrho_1(x_1) = \int \langle x_1, x_2|\, \Psi \,\rangle\langle\, \Psi \,|x_1, x_2\rangle \, \mathrm{d}x_2 = \sqrt{\frac{2f_2}{\pi a^2 f_1}} \exp\left[-\frac{2f_2}{a^2 f_1} x_1^2\right]. \qquad (2.191)$$

E finalmente, como pode ser visto na Eq. (2.153), para uma partícula do par não emaranhado, seus elementos diagonais na representação de posição para qualquer t são

$$\begin{aligned} \rho_1(x_1) &= \int \langle x_1, x_2|\, \psi \,\rangle\langle\, \psi \,|x_1, x_2\rangle \, \mathrm{d}x_2 \\ &= \sqrt{\frac{2}{\pi a'^2(1 + F(t, a'))}} \exp\left[-\frac{2}{a'^2}\frac{(x_1 - v_c t)^2}{1 + F(t, a')}\right]. \end{aligned} \qquad (2.192)$$

Se desejamos as Eqs. (2.191) e (2.192) fornecendo as mesmas predições estatísticas devemos ter

$$\frac{2f_2}{a^2 f_1} = \frac{2}{a'^2}\frac{1}{1 + F(t, a')}. \qquad (2.193)$$

A Eq. (2.193) garante que as duas matrizes densidade possuam a mesma dispersão na posição. (Não precisamos nos preocupar com os momentos de ordem um dessas

funçoes Gaussianas pois uma translação do eixo x_1 faz com que eles sejam zero.) Por meio das Eqs. (2.190) e (2.193) e lembrando que $f_n = 1 + n\frac{a^2}{b^2}$ obtemos para o tempo t:

$$t = \frac{1}{2u^2}\frac{1}{\sqrt{u^4b^4 - 1}}. \tag{2.194}$$

A Eq. (2.194) diz que para um único, e somente um único, tempo t, os elementos diagonais das matrizes densidade reduzidas, uma descrevendo um membro do par emaranhado e a outra uma partícula do par não emaranhado, fornecem as mesmas predições estatísticas. Isto implica a impossibilidade de discernimos se temos ou não um sistema emaranhado por meio de uma única medida da dispersão do momento e da posição da partícula 1. (A menos que, claro, Bob saiba quando Alice começou a produzir seus pares.) Veja Fig. 2.4.

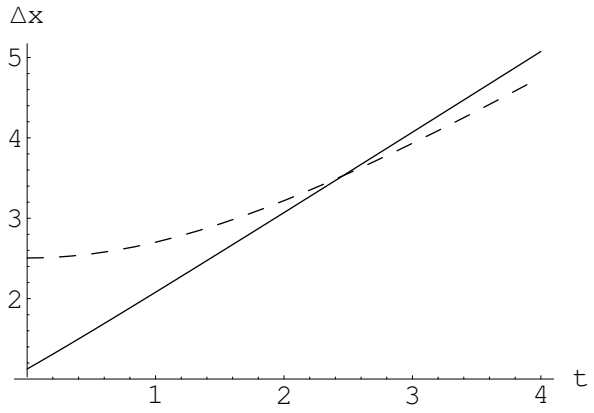


Figura 2.4: A curva tracejada é a evolução temporal da dispersão da posição para um pacote Gaussiano emaranhado produzido 1 unidade de tempo depois da produção de um pacote não emaranhado, o qual está representado por uma curva sólida. As curvas se interceptam quando $t \approx 2.46$. Se Bob mede Δx_1 para este tempo, ele é incapaz de distinguir entre as duas possíveis maneiras que Alice pode produzir os pares de partículas. Para qualquer outro ponto sobre a curva tracejada, podemos encontrar uma curva sólida que a intercepta. Assim, Bob não pode distinguir como suas partículas foram produzidas medindo-se apenas uma única vez Δx_1. Aqui, $b = 1$ e $u = 1.01$.

Para contornar essa limitação, Bob aplica o seguinte protocolo, o qual usa explicitamente a diferença na evolução temporal dos dois sistemas.

Bob inicialmente mede a dispersão do momento de suas partículas ($\Delta p_1 = u$). Como ele não sabe quando nem onde Alice começou a produzir os pares de partículas, a evolução temporal da dispersão da posição é dada por uma destas duas possibilidades,

$$\Delta x_1(t) = \frac{1}{2u}\sqrt{1 + 4u^4(t + t_0)^2}. \tag{2.195}$$

$$\Delta x_1(t) = \frac{1}{2u}\sqrt{\frac{u^4b^4}{u^4b^4-1} + 4u^4(t+t_0)^2}. \tag{2.196}$$

Aqui t_0 é o tempo decorrido desde a produção do primeiro conjunto de pares por Alice até o primeiro conjunto de medidas feitas por Bob. Bob agora faz muitas medidas da dispersão da posição para diferentes instantes de tempo t. A partir dessas medidas ele obtém o seguinte conjunto de pontos: $\{(\Delta x_1(0), 0), (\Delta x_1(t_1), t_1), \ldots, (\Delta x_1(t_n), t_n)\}$. Ele faz o maior número possível de medidas. Com esses n pares de pontos ele fita a seguinte curva, onde α e β são os parâmetros livres e u já é conhecido:

$$\Delta x_1(t) = \frac{1}{2u}\sqrt{\alpha + 4u^4(t+\beta)^2}. \tag{2.197}$$

Observando as Eqs. (2.197), (2.195), e (2.196) vemos que se $\alpha = 1$, Bob lida com pacotes Gaussianos não emaranhados. Mas se $\alpha \neq 1$, então ele lida com partículas emaranhadas. E usando α Bob pode calcular o grau de emaranhamento b. Só por completeza, vale a pena mencionar que β nos dá t_0. E como dissemos para o protocolo anterior, Bob deve começar suas medidas o mais cedo possível, pois assintoticamente no tempo as Eqs. (2.195) e (2.196) são idênticas.

2.5.4 Consistência do Modelo

O modelo acima descrito poderia levar alguém a suspeitar que o fato de termos dois modos de evolução temporal para a dispersão da posição de uma partícula abriria a possibilidade de transmissão de informação com velocidade maior que a da luz (rigorosamente isso não é possível, conforme mostraremos abaixo). A maneira pela qual isso talvez pudesse ser feito basear-se-ia no seguinte protocolo: Alice produziria um ensemble de pares de partículas emaranhadas e enviaria a Bob um membro de cada par. Alice poderia então medir, por exemplo, o momento de suas partículas, fato que destruiria o emaranhamento entre os pares de partículas compartilhadas. Isso acarretaria numa evolução temporal da dispersão da posição dada pela Eq. (2.184). Caso Alice não fizesse nenhuma medida em suas partículas então teríamos uma evolução temporal dada pela Eq. (2.185). Dessa forma, alguém poderia imaginar que se Alice e Bob estiverem separados por uma distância tipo espaço, Bob poderia, medindo a dispersão da posição de suas partículas, descobrir se Alice mediu ou não o momento de suas partículas. Se isso fosse possível, teríamos um protocolo de transmissão de informação superluminal, onde uma evolução dada pela Eq. (2.184) representaria, por exemplo, o bit 1, e uma evolução dada pela Eq. (2.185) o bit 0.

O ponto falho no raciocínio acima reside no fato de que Alice não tem controle sobre qual momento ela mede. Para um dado momento medido k_0, a evolucão temporal da dispersão da posição é dada pela Eq. (2.184). Mas como Alice não tem controle sobre qual momento ela mede devemos somar sobre todas as possibilidades a fim de corretamente descrever o que Bob observa. Esse fato faz com que a dispersão

da posição vista por Bob seja dada pela Eq. (2.185). Ou seja, tudo se passa como se Alice não tivesse medido o momento de suas partículas e não há como transmitir informação alguma usando o fato de Alice ter ou não medido o momento de suas partículas. Vamos agora mostrar explicitamente que as dispersões do momento e da posição medidas por Bob independem do fato de Alice medir ou não o momento de suas partículas.

Podemos reescrever a Eq. (2.173), que representa um par de pacotes gaussianos emaranhados, da seguinte forma:

$$|\Psi(t)\rangle = \int 2\pi c(k_1,k_2)\mathrm{e}^{-\mathrm{i}[\omega(k_1)+\omega(k_2)]t}\,|k_1\rangle_B\,|k_2\rangle_A\,\mathrm{d}k_1\mathrm{d}k_2, \tag{2.198}$$

onde $\langle x|k\rangle = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{ikx}$. Os símbolos A e B são usados só para nos lembrar com quem estamos lidando, Alice e Bob respectivamente.

Se Alice não mede o momento de suas partículas, então, a partir da Eq. (2.198) podemos obter as dipersões da posição e do momento medidos por Bob (já calculamos isso anteriormente):

$$\Delta x_1(t) = \frac{a}{2}\sqrt{\frac{f_1}{f_2}[1+f_2F(t)]}, \tag{2.199}$$

$$\Delta p_1(t) = \frac{\hbar}{a}\sqrt{f_1}. \tag{2.200}$$

Vamos supor agora que Alice mede os momentos de todas as suas partículas. Podemos representar essa medida pelo seguinte operador:

$$P_{k_0} = \mathcal{I}_1 \otimes |k_0\rangle_{A\,A}\langle k_0|\,, \tag{2.201}$$

onde $\mathcal{I}_1$ é o operador identidade da partícula 1 e k_0 é o momento medido.

Aplicando esse projetor na Eq. (2.198) obtemos:

$$\begin{aligned} |\Psi'(t)\rangle &= P_{k_0}\,|\Psi(t)\rangle \\ &= \int 2\pi c(k_1,k_2)\mathrm{e}^{-\mathrm{i}[\omega(k_1)+\omega(k_2)]t}\,|k_1\rangle_B\,|k_0\rangle_{A\,A}\langle k_0\,|k_2\rangle_A\,\mathrm{d}k_1\mathrm{d}k_2. \end{aligned} \tag{2.202}$$

Mas sabemos que ${}_A\langle k_0\,|k_2\rangle_A = \delta(k_2-k_0)$. Então, usando essa função delta para eliminar a integração em k_2:

$$|\Psi'(t)\rangle = \int 2\pi c(k_1,k_0)\mathrm{e}^{-\mathrm{i}\omega(k_1)t}\,|k_1\rangle_B\,\mathrm{d}k_1 \otimes \mathrm{e}^{-\mathrm{i}\omega(k_0)t}\,|k_0\rangle_A\,. \tag{2.203}$$

Observando a Eq. (2.203) vemos claramente que Alice medindo o momento de suas partículas quebra a correlação quântica do sistema ('desemaranha' o sistema). O novo estado, para uma dada medida de momento k_0, pode ser descrito por um

produto tensorial de uma onda plana com momento k_0 para a partícula 2 (partícula com Alice) e um estado gaussiano para a partícula 1 (partícula com Bob). Então, para um dado momento k_0 medido por Alice, o estado normalizado da partícula com Bob é:

$$\left|\Phi'(t)\right\rangle_B = \frac{\int \mathrm{d}k_1 2\pi c(k_1,k_0)\mathrm{e}^{-\mathrm{i}\omega(k_1)t}\left|k_1\right\rangle_B}{\sqrt{\int \mathrm{d}k_1' \left|2\pi c(k_1',k_0)\right|^2}}. \tag{2.204}$$

Realizando a integração do denominador temos:

$$\left|\Phi'(t)\right\rangle_B = \frac{\sqrt{\alpha}}{(2\pi)^{\frac{1}{4}}}\int \mathrm{e}^{-\frac{\alpha^2}{4}(k_1-\beta)^2}\mathrm{e}^{-\mathrm{i}\omega(k_1)t}\left|k_1\right\rangle_B \mathrm{d}k_1, \tag{2.205}$$

onde α e β são:

$$\alpha = a\sqrt{\frac{f_1}{f_2}}, \qquad \beta = \left(k_c - \frac{a^2}{b^2}k_0\right)\frac{1}{f_1}. \tag{2.206}$$

Entretanto, como Bob não tem como saber qual momento Alice mediu sem ela lhe transmitir um sinal clássico, o ensemble de partículas com Bob tem que ser descrito por uma mistura estatística de todas as possibilidades de medida de momento por Alice:

$$\rho_B(t) = \frac{\int \mathrm{d}k_0 \left|\langle\Psi(t)|k_0\rangle_A\right|^2 \left|\Phi'(t)\right\rangle_{B\,B}\left\langle\Phi'(t)\right|}{\int \mathrm{d}k_0' \left|\langle\Psi(t)|k_0'\rangle_A\right|^2}, \tag{2.207}$$

onde,

$$\left|\langle\Psi(t)|k_0\rangle_A\right|^2 = \int \mathrm{d}k_1 \left|2\pi c(k_1,k_0)\right|^2, \tag{2.208}$$

é a probabilidade de Alice medir k_0.

Substituindo a Eq. (2.208) na Eq. (2.207) e lembrando que o denominador da Eq. (2.207) vale 1 temos:

$$\rho_B(t) = \int \mathrm{d}k_0\mathrm{d}k_1 \left|2\pi c(k_1,k_0)\right|^2 \left|\Phi'(t)\right\rangle_{B\,B}\left\langle\Phi'(t)\right|. \tag{2.209}$$

Podemos simplificar mais ainda a Eq. (2.209) usando a Eq. (2.204):

$$\rho_B(t) = \int \mathrm{d}k_0\mathrm{d}k_1\mathrm{d}k_1' 4\pi^2 c(k_1,k_0)c^*(k_1',k_0)\mathrm{e}^{-\mathrm{i}[\omega(k_1)-\omega(k_1')]t}\left|k_1\right\rangle_{B\,B}\left\langle k_1'\right|. \tag{2.210}$$

Realizando a integração em k_0 temos:

$$\rho_B(t) = \int \mathrm{d}k_1\mathrm{d}k_1' G(k_1,k_1')\mathrm{e}^{-\mathrm{i}[\omega(k_1)-\omega(k_1')]t}\left|k_1\right\rangle_{B\,B}\left\langle k_1'\right|, \tag{2.211}$$

onde,

$$G(k_1,k_1') = \sqrt{\frac{a^2}{2\pi f_1}}\mathrm{e}^{-\frac{a^2k_c^2}{2f_1}}\exp\left\{-\frac{a^2f_1}{4f_2}\left[\frac{1}{2}\left(1+\frac{f_2}{f_1^2}\right)\left(k_1^2+k_1'^2\right)\right.\right.$$
$$\left.\left.-2k_c\frac{f_2}{f_1^2}\left(k_1+k_1'\right)-\frac{a^4}{b^4f_1^2}k_1k_1'\right]\right\}. \quad (2.212)$$

Então, usando a matriz densidade dada pela Eq. (2.211) podemos calular as dispersões da posição e do momento para o ensemble de partículas com Bob:

$$\Delta x_1(t) = \sqrt{Tr\left\{X_1^2\rho_B(t)\right\}-\left(Tr\left\{X_1\rho_B(t)\right\}\right)^2}, \quad (2.213)$$

$$\Delta p_1(t) = \sqrt{Tr\left\{P_1^2\rho_B(t)\right\}-\left(Tr\left\{P_1\rho_B(t)\right\}\right)^2}. \quad (2.214)$$

Aqui, X_1 e $P_1=\hbar K_1$ são os operadores posição e momento da partícula 1.

Calculando os traços acima obtemos:

$$\Delta x_1(t) = \frac{a}{2}\sqrt{\frac{f_1}{f_2}[1+f_2F(t)]}, \quad (2.215)$$

$$\Delta p_1(t) = \frac{\hbar}{a}\sqrt{f_1}. \quad (2.216)$$

Observando essas dispersões vemos que elas são idênticas às que teríamos caso Alice não tivesse medido o momento de suas partículas (veja Eqs. (2.199) e (2.215) e Eqs. (2.200) e (2.216)). Dessa forma, a maneira proposta de transmissão de sinal superluminal no início dessa subseção não funciona.

Prova da Regra do Traço Parcial

Vamos, agora, mostrar um resultado bem geral, o qual garante que qualquer medida feita por Alice não afeta os resultados das medidas feitas por Bob. Na verdade, esse resultado nada mais é do que a prova da regra do traço parcial. Esta regra, muitas vezes impunemente usada, diz: quando lidamos com um sistema composto descrito pelo estado ρ e temos acesso apenas ao subsistema B, o estado que descreve B é obtido 'traçando-se' os subsistemas a que não temos acesso. Conforme veremos abaixo, essa regra é consequência de aspectos probabilísticos da Mecância Quântica.

Observemos a Eq. (2.210), que pode ser reescrita da seguinte forma:

$$\rho_B(t) = \int \mathrm{d}k_0\mathrm{d}k_1\mathrm{d}k_1'\mathrm{d}k_2\mathrm{d}k_2'4\pi^2c(k_1,k_2)c^*(k_1',k_2')\mathrm{e}^{-\mathrm{i}[\omega(k_1)-\omega(k_1')]t}$$
$$\times\mathrm{e}^{-\mathrm{i}[\omega(k_2)-\omega(k_2')]t}\left|k_1\right\rangle_B{}_B\left\langle k_1'\right|\delta(k_0-k_2)\delta(k_0-k_2'). \quad (2.217)$$

Usando o fato de que ${}_A\langle k_0|k_2\rangle_A=\delta(k_0-k_2)$ e ${}_A\langle k_2'|k_0\rangle_A=\delta(k_0-k_2')$ podemos reescrever a Eq. (2.217):

$$\rho_B(t) = \int \mathrm{d}k_0 \, {}_A\langle k_0| \left[\int \mathrm{d}k_1 \mathrm{d}k_1' \mathrm{d}k_2 \mathrm{d}k_2' 4\pi^2 c(k_1,k_2) c^*(k_1',k_2') \mathrm{e}^{-\mathrm{i}[\omega(k_1)-\omega(k_1')]t} \right.$$
$$\left. \times \, \mathrm{e}^{-\mathrm{i}[\omega(k_2)-\omega(k_2')]t} \, |k_1\rangle_{B\,B} \langle k_1'| \otimes |k_2\rangle_{A\,A} \langle k_2'| \right] |k_0\rangle_A \,. \quad (2.218)$$

Mas sabemos que:

$$\rho_{AB}(t) = \int \mathrm{d}k_1 \mathrm{d}k_1' \mathrm{d}k_2 \mathrm{d}k_2' 4\pi^2 c(k_1,k_2) c^*(k_1',k_2') \mathrm{e}^{-\mathrm{i}[\omega(k_1)-\omega(k_1')]t}$$
$$\times \mathrm{e}^{-\mathrm{i}[\omega(k_2)-\omega(k_2')]t} \, |k_1\rangle_{B\,B} \langle k_1'| \otimes |k_2\rangle_{A\,A} \langle k_2'| \,. \quad (2.219)$$

Então, a Eq. (2.217) pode ser escrita do seguinte modo:

$$\rho_B(t) = Tr_A\{\rho_{AB}(t)\}, \quad (2.220)$$

onde $Tr_A\{\ \} = \int \mathrm{d}k_0 \, {}_A\langle k_0| \ |k_0\rangle_A$ é o traço parcial sobre os estados de Alice (nesse caso, sobre os estados da partícula 2, que está com Alice).

A Eq. (2.220) foi deduzida supondo que Alice mediu os momentos de suas partículas. Isto é, tomamos o traço parcial usando como base os auto-estados do observável momento medido por Alice. Mas como o traço independe da base que usamos para calculá-lo, então, para qualquer observável local, $\mathcal{O}_A = \mathcal{I}_1 \otimes \mathcal{O}_2$, medido por Alice, a matriz densidade vista por Bob será sempre a mesma. Isto é, não importa qual observável Alice meça, sempre teremos $\rho_B(t)$ como a matriz densidade vista por Bob. Isso garante que o valor médio de qualquer observável que Bob venha a medir será independente do que Alice escolheu para medir.

O valor médio, então, de um observável $\mathcal{O}_B = \mathcal{O}_1 \otimes \mathcal{I}_2$ medido por Bob é:

$$\langle \mathcal{O}_B \rangle = Tr_B \{\mathcal{O}_B \rho_B\} \,. \quad (2.221)$$

Finalmente, caso nenhuma medida fosse feita por Alice então teríamos:

$$\begin{aligned} \langle \mathcal{O}_B \rangle &= Tr \{\mathcal{O}_B \rho_{AB}\} \\ & \quad Tr_A Tr_B \{\mathcal{O}_B \rho_{AB}\} \\ & \quad Tr_B \{\mathcal{O}_B Tr_A \{\rho_{AB}\}\} \\ & \quad Tr_B \{\mathcal{O}_B \rho_B\} \,. \end{aligned} \quad (2.222)$$

Como as Eqs.(2.221) e (2.222) são iguais, isso demonstra que as previsões estatísticas feitas por Bob para um dado observável local são independentes do que Alice venha a fazer com sua partícula.

Vale a pena ressaltar que a Eq. (2.220) foi deduzida supondo que Alice não tem controle sobre qual momento k_0 ela mede. Isto está matematicamente representado pela Eq. (2.207):

$$\rho_B(t) = \frac{\int \mathrm{d}k_0 \, |\langle \Psi(t)|k_0\rangle_A|^2 \, |\Phi'(t)\rangle_{B\,B} \langle \Phi'(t)|}{\int \mathrm{d}k_0' \, \left|\langle \Psi(t)|k_0'\rangle_A\right|^2}.$$

Dessa forma, o simples fato de que as previsões da Mecânica Quântica são probabilísticas (regra de Born) implicou na regra do traço e, neste protocolo em particular, na impossibilidade de trasmissão de informação superluminal.

Capítulo 3

Quantificação do Emaranhamento

3.1 Introdução

Sabendo-se da existência de emaranhamento em um sistema quântico, a próxima questão que necessita ser respondida é, naturalmente, quão emaranhado esse sistema está. Novamente nos deparamos com um problema extremamente não trivial. Dificuldades ainda maiores àquelas encontradas na obtenção de critérios operacionais de separabilidade surgem aqui. Além disso, nos deparamos com uma nova complicação. Se ao lidarmos com o problema da separabilidade tínhamos claramente uma definição de estados separáveis ou não emaranhados, agora temos um amontoado de possíveis medidas de emaranhamento.

Para estados puros bipartites, conforme discutimos abaixo, há um consenso sobre qual medida de emaranhamento devemos utilizar. Ela possui uma interpretação física razoável e é facilmente obtida a partir do estado que descreve o sistema. No entanto, ao se tentar quantificar o emaranhamento de estados mistos, ou mesmo estados puros multipartites, muito pouco se avançou. Encontramos muitas definições de medidas de emaranhamento e quase todas sem muito apelo físico. Mesmo que aceitemos algumas dessas medidas, ainda assim não vamos muito longe. Temos poucos resultados analíticos e mesmo os métodos numéricos requerem grande capacidade computacional.

Apresentamos, a seguir, breves descrições de algumas medidas de emaranhamento disponíveis e estudamos detalhadamente uma delas: O Emaranhamento de Formação (EoF). Especial destaque é dado ao EoF para variáveis contínuas, onde calculamos analiticamente dois limitantes inferiores válidos para qualquer tipo de estado Gaussiano (puro ou misto e simétrico ou não simétrico) [73]. Não obstante a profusão de medidas de emaranhamento para sistemas multipartites, propomos uma que, no entanto, possui clara interpretação física [76]. Ela se baseia na eficiência que

determinados estados quânticos têm para realizar codificação superdensa [75] e teletransporte [76]. Para definir essa medida de emaranhamento, generalizamos o protocolo de teletransporte de Bennett *et al.* [11], onde agora podemos teletransportar uma cadeia de spin 1/2 de tamanho arbitrário. Finalizamos o capítulo mostrando que os canais quânticos necessários para teletransportar N qbits (cadeia de spin 1/2) são, na verdade, N canais EPR trabalhando em paralelo [75].

3.2 Estados Puros Bipartites

Existe uma medida de emaranhamento muito natural para estados puros, a qual é praticamente a única medida ao mesmo tempo operacional e de fácil interpretação física. Bennett *et al.* [13] propuseram que é fisicamente justificável definir a entropia de von Neumann de quaisquer partes de um sistema bipartite como medida de emaranhamento. Se $\rho = |\psi\rangle\langle\psi|$ é a matriz densidade que descreve nosso estado puro, a quantidade de emaranhamento de ρ é:

$$E(\psi) = -\mathrm{Tr}\left\{\rho_1 \log_2(\rho_1)\right\} = -\mathrm{Tr}\left\{\rho_2 \log_2(\rho_2)\right\}, \tag{3.1}$$

onde $\rho_1 = \mathrm{Tr}_2\{\rho\}$ e $\rho_2 = \mathrm{Tr}_1\{\rho\}$ são as matrizes reduzidas do sistema bipartite. Escrevendo a decomposição de Schmidt de $|\psi\rangle$,

$$|\psi\rangle = \sum_{i=1}^{N} c_i \left|u_i\right\rangle_A \left|v_i\right\rangle_B, \tag{3.2}$$

obtemos,

$$E(\psi) = -\sum_{i=1}^{N} c_i^2 \log_2(c_i^2), \tag{3.3}$$

onde N pode tender a infinito (caso de variáveis contínuas).

Por essa definição vemos claramente que estados maximamente emaranhados, $|\psi^-\rangle = (1/\sqrt{2})\left(|01\rangle - |10\rangle\right)$, por exemplo, possuem emaranhamento igual a 1, enquanto estados separáveis sempre possuem emaranhamento nulo.

Bennett *et al.* [13] mostraram que n pares no estado puro $|\psi\rangle$ com E 'ebits' de emaranhamento podem ser reversivelmente convertidos em m pares de singletos ($|\psi^-\rangle$), usando-se apenas operações locais e comunicação clássica. Além disso, eles mostraram que m/n tende a E, com a fidelidade da conversão tendendo a 1, se $n \to \infty$. Essa interconvertibilidade foi a justificativa para a definição da entropia de von Neumann como medida de emaranhamento para estados puros bipartites.

3.3 Estados Mistos Bipartites

Como dissemos, para estados mistos a situação se complica sobremaneira. Essa complicação se dá em dois aspectos. Primeiro, não há uma única medida de ema-

ranhamento. Dessas inúmeras medidas de emaranhamento, apenas duas (Emaranhamento de Formação e Emaranhamento Destilável) possuem interpretações físicas razoáveis.

Segundo, não há muitas expressões analíticas que nos forneçam a quantidade de emaranhamento do sistema conhecendo-se apenas sua matriz densidade ρ. Muitas dessas medidas de emaranhamento (Emaranhamento de Formação e Entropia Relativa de Emaranhamento) são definidas como soluções de problemas de minimização extremamente difíceis de se lidar analiticamente. E mesmo numericamente estes problemas se tornam quase inviáveis conforme se aumenta a dimensão do espaço de Hilbert do sistema estudado.

Até hoje, só se descobriu fórmulas analíticas para o Emaranhamento de Formação de sistemas bipartites 2×2 (dois spins 1/2, por exemplo) [99] e para estados Gaussianos simétricos [36]. Apesar dessas dificuldades, conseguimos avançar um pouco mais no entendimento do Emaranhamento de Formação para sistemas bipartites de variáveis contínuas. Mais à frente apresentamos resultados analíticos, os quais fornecem dois limitantes inferiores para o Emaranhamento de Formação de qualquer estado Gaussiano, simétrico ou não [73].

Vamos, agora, definir formalmente as três medidas de emaranhamento citadas no ínicio dessa seção. Escolhemos essas três medidas de emaranhamento pois são amplamente utilizadas e desempenham papéis importantes na nossa compreensão sobre as características do emaranhamento quântico. No restante desta seção, sempre que nos referirmos a uma matriz densidade, está implícito que ela atua sobre um espaço de Hilbert $\mathcal{H}$ tal que $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Isto é, lidamos com sistemas bipartites.

3.3.1 Entropia Relativa de Emaranhamento

Seja σ uma matriz densidade tal que $\sigma \in \mathcal{D}$, onde $\mathcal{D}$ representa o conjunto de todos os estados separáveis. A Entropia Relativa de Emaranhamento para uma matriz densidade ρ é definida como [92, 93]:

$$E_R(\rho) = \min S(\rho||\sigma), \tag{3.4}$$

onde $S(\rho||\sigma) := \mathrm{Tr}\{\rho\ln(\rho) - \rho\ln(\sigma)\}$. Pela definição de E_R vemos que temos um problema de minimização para ser resolvido a fim de calcularmos $E_R(\rho)$. Até hoje nenhuma expressão analítica de caráter geral para E_R foi encontrada, nem mesmo para os sistemas mistos mais simples (2×2). Apenas para alguns sistemas mistos 2×2 (estados isotrópicos), Rains [69] conseguiu uma expressão analítica.

3.3.2 Emaranhamento Destilável

O Emaranhamento Destilável E_D é fisicamente interpretado como o número máximo de singletos que podem ser produzidos a partir de um conjunto de pares de partículas

descritas pelo estado ρ, usando-se apenas operações locais e comunicação clássica (LOCC) [15]. Por sua própria definição, E_D depende da escolha correta do protocolo ótimo de purificação usado para destilar singletos de estados mistos emaranhados. Essa escolha nem sempre é trivial e para diferentes ρ temos, em geral, protocolos ótimos distintos. Dessa forma, não existe uma expressão fechada que forneça o valor de E_D para determinado estado. Pode-se mostrar que E_D é igual a entropia de von Neumann quando ρ é um estado puro.

3.3.3 Emaranhamento de Formação

Fisicamente, o Emaranhamento de Formação EoF representa o número mínimo de singletos necessários para produzir um conjunto de pares de partículas descritas pelo estado ρ, usando-se apenas LOCC [14]. Novamente aqui se pode mostrar que o EoF se reduz a entropia de von Neunmann quando ρ for um estado puro.

Define-se o EoF do seguinte modo:

$$EoF(\rho) = \min \sum_i p_i E(\psi_i), \tag{3.5}$$

onde $\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$ e $E(\psi_i)$ é a entropia de von Neumann para o estado puro ψ_i. Outra vez temos mais uma definição de emaranhamento para estados mistos onde precisamos resolver um problema de minimização. Dentre todas as decomposições de ρ em estados puros (e podemos ter infinitas decomposições) temos de encontrar aquela que minimize o lado direito da Eq. (3.5).

Felizmente aqui temos alguns avanços importantes. Como dissemos, Wootters [99] conseguiu obter uma expressão analítica para sistemas mistos 2×2 e Giedke *et al.* [36] para estados Gaussianos simétricos. Mais à frente nos concentraremos numa dedução do resultado obtido por Wootters e, em especial, na fórmula analítica de Giedke *et al.*, a fim de preparar terreno para o cálculo dos dois limitantes inferiores para o EoF de estados Gaussianos arbitrários.

3.4 Porque Essas Medidas de Emaranhamento

Os Horodeckis [49] mostraram que quaisquer medidas de emaranhamento E que satisfaçam alguns axiomas bem razoáveis, devem ter E_D e EoF como limitantes inferior e superior,[1] respectivamente. Ou seja,

$$E_D \leq E \leq E_F. \tag{3.6}$$

Os axiomas que E deve satisfazer são listados em três grupos [49]:

[1] EoF utilizado na Ref. [49] é, na verdade, a versão regularizada do Emaranhamento de Formação definido aqui: $EoF \to \lim_{n\to\infty} EoF(\rho^{\otimes n})/n$.

1) *Postulados Óbvios.* (a) Não-negatividade: $E(\rho) \geq 0$; (b) Emaranhamento tem que ser nulo para estados separáveis: $E(\rho) = 0$ se ρ é separável; (c) Normalização: $E(\psi^{max}) = \log_2(\dim\mathcal{H}_i)$, onde $\dim\mathcal{H}_i$ é a dimensão do espaço de Hilbert do subsistema de menor dimensão e ψ^{max} é o estado de máximo emaranhamento do sistema em questão. Para o caso 2×2 temos $E(\psi^{max}) = 1$ e para variáveis contínuas podemos ter $E(\psi^{max}) \to \infty$.

2) *Postulados fundamentais: monotonicidade sob LOCC.* (a) Monotonicidade sob operações locais: Se alguma operação é feita em quaisquer dos subsistemas, resultando um estado σ_i com probabilidade p_i, então o emaranhamento do novo sistema não pode crescer:

$$E(\rho) \geq \sum_i p_i E(\sigma_i). \tag{3.7}$$

(b) Convexidade (monotonicidade sob descarte de informação):

$$E\left(\sum_i p_i \rho_i\right) \leq \sum_i p_i E(\rho_i). \tag{3.8}$$

3) *Postulados de regime assimptótico.* (a) Aditividade parcial:

$$E(\rho^{\otimes n}) = nE(\rho); \tag{3.9}$$

(b) Continuidade: Se $\langle\psi^{\otimes n}|\,\rho_n\,|\psi^{\otimes n}\rangle \to 1$ quando $n \to \infty$, então

$$\frac{1}{n}|E(\psi^{\otimes n}) - E(\rho_n)| \to 0, \tag{3.10}$$

onde ρ_n é um estado coletivo de n pares. Como não pretendemos aqui nos deter numa discussão da axiomatização de medidas de emaranhamento, recomendamos a Ref. [49] e as referências lá citadas para uma discussão bem completa de cada um desses postulados. Vale a pena acrescentar, no entanto, que estes postulados são bem gerais e mais fracos do que muitos adotados na literatura, em especial os dois postulados assimptóticos.

3.5 *EoF* para Sistemas 2×2

Usando a decomposição de Schmidt podemos mostrar que qualquer sistema bipartite puro 2×2 pode ser escrito como

$$|\psi\rangle = c_1|01\rangle + c_2|10\rangle, \tag{3.11}$$

onde c_1 e c_2 são reais não negativos e supomos, sem perder em generalidade, que $c_1 \geq c_2$. Assim, por meio da Eq. (3.3), seu emaranhamento vale

$$E(\psi) = -c_1^2 \log_2 c_1^2 - (1 - c_1^2)\log_2(1 - c_1^2). \tag{3.12}$$

Para obter o resultado acima usamos que $c_1^2 + c_2^2 = 1$. Podemos deixar o emaranhamento E do estado ψ em função de uma grandeza chamada concorrência (*concurrence*), a qual é definida como:

$$C(\psi) \equiv |\langle\tilde{\psi}|\psi\rangle|, \tag{3.13}$$

onde

$$\begin{aligned} |\tilde{\psi}\rangle &= \sigma_y^A \otimes \sigma_y^B |\psi^*\rangle, \\ |\psi^*\rangle &= c_1^*|01\rangle + c_2^*|10\rangle. \end{aligned}$$

Lembrando que c_1 e c_2 são reais temos $|\tilde{\psi}\rangle = c_1|10\rangle + c_2|01\rangle$ e, portanto,

$$C(\psi) = 2\, c_1\, c_2. \tag{3.14}$$

Seja, agora, a função abaixo,

$$\mathcal{E}(C) = h\left(\frac{1+\sqrt{1-C^2}}{2}\right), \tag{3.15}$$

onde,

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

Substituindo o valor da concorrência no argumento da função h da Eq. (3.15) vemos que $(1+\sqrt{1-C^2})/2 = c_1^2$. Assim, o emaranhamento de ψ é dado por $\mathcal{E}(C)$, o qual é uma função monotonicamente crescente de C. Em outras palavras, $E(\psi) = \mathcal{E}(C(\psi))$.

Para estados mistos, a partir da definição de Emaranhamento de Formação dada pela Eq. (3.5), apresentamos em forma de teorema a expressão analítica que nos permite calcular o EoF para estados mistos 2×2 [99].

Teorema 10 *O EoF de qualquer estado ρ de dois qbits, puro ou não, é*

$$EoF(\rho) = \mathcal{E}(C(\rho)), \tag{3.16}$$

onde $C(\rho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$. Os λ_i's são as raízes quadradas dos autovalores, em ordem decrescente, da matriz não hermitiana $R = \rho\tilde{\rho}$. Aqui, $\tilde{\rho} = (\sigma_y^A \otimes \sigma_y^B)\rho^*(\sigma_y^A \otimes \sigma_y^B)$.

Prova:
Escrevendo ρ na base onde ele é diagonal obtemos

$$\rho = \sum_{i=1}^{n} p_i |u_i\rangle\langle u_i|. \tag{3.17}$$

A partir da decomposição anterior, definimos os estados 'subnormalizados' $|v_i\rangle = \sqrt{p_i}|u_i\rangle$. Eles são chamados subnormalizados pois seu produto escalar $\langle v_i|v_j\rangle = p_j\delta_{ij}$

nos dá diretamente o i-ésimo autovalor de ρ. Usando um resultado demonstrado na Ref. [50], qualquer decomposição de ρ pode ser escrita como:

$$\rho = \sum_{i=1}^{m} |w_i\rangle\langle w_i|, \tag{3.18}$$

onde $m \geq n = \text{ranque}(\rho) \leq 4$ e

$$|w_i\rangle = \sum_{j=1}^{n} U_{ij}^{*} |v_j\rangle. \tag{3.19}$$

Na expressão anterior U é uma transformação unitária $m \times m$, ranque(ρ) é o número de autovalores de ρ não nulos e o complexo conjugado foi usado para simplificar notação mais à frente.

Vamos separar a demonstração em duas partes: 1) matrizes densidade nas quais $\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 \geq 0$ e 2) matrizes densidade nas quais $\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 < 0$.

Caso 1) A partir da decomposição de ρ em termos dos estados subnormalizados $|v_i\rangle$ vamos, sucessivamente, obter três outras. A última é a decomposição ótima procurada, i. e., ela atinge o mínimo da definição do EoF para estados mistos. Cada uma dessas decomposições possui n estados puros, onde $n = \text{ranque}(\rho)$.

Decomposição 1:

$$\rho = \sum_{i=1}^{n} |x_i\rangle\langle x_i|, \qquad \langle x_i|\tilde{x}_j\rangle = \lambda_i \delta_{ij}. \tag{3.20}$$

Lembrando que qualquer decomposição pode ser escrita como a Eq. (3.18), onde os vetores dessa decomposição são dados pela Eq. (3.19), então,

$$|x_i\rangle = \sum_{j=1}^{n} U_{ij}^{*} |v_j\rangle, \qquad |\tilde{x}_i\rangle = \sum_{j=1}^{n} U_{ij} |\tilde{v}_j\rangle, \qquad i = 1, \ldots, n. \tag{3.21}$$

Dessa forma,

$$\begin{aligned} \langle x_i|\tilde{x}_j\rangle &= \left(\sum_{k=1}^{n} U_{ik}\langle v_k|\right)\left(\sum_{l=1}^{n} U_{jl}|\tilde{v}_l\rangle\right) \\ &= \sum_{k,l=1}^{n} U_{ik}\langle v_k|\tilde{v}_l\rangle U_{jl} \\ &= \sum_{k,l=1}^{n} U_{ik}\tau_{kl}U_{lj}^{T} \\ &= \left(U\tau U^{T}\right)_{ij}, \end{aligned} \tag{3.22}$$

onde $\tau_{ij} = \langle v_i|\tilde{v}_j\rangle$. Usando o fato de que $\sigma_y^A \otimes \sigma_y^B$ é matriz real e igual a sua transposta, podemos mostrar que τ_{ij} é matriz simétrica:

$$\begin{aligned} \tau_{ij} &= \langle v_i|\tilde{v}_j\rangle = \langle v_i|\sigma_y^A \otimes \sigma_y^B|v_j^{*}\rangle = \langle v_j^{*}|\sigma_y^A \otimes \sigma_y^B|v_i\rangle^{*} \\ &= \langle v_j|\sigma_y^A \otimes \sigma_y^B|v_i^{*}\rangle = \langle v_j|\tilde{v}_i\rangle = \tau_{ji}. \end{aligned}$$

Agora, usando um resultado demonstrado na Ref. [45], sempre existe uma transformação unitária U que diagonaliza uma matriz *simétrica* τ por meio da operação $U\tau U^T$, deixando seus autovalores reais e não negativos. Assim, escolhendo apropriadamente U, obtemos a decomposição 1. Além disso, U diagonaliza $\tau\tau^*$ da maneira usual, i. e. $U\tau\tau^*U^\dagger$ é diagonal, veja:

$$\begin{aligned} U\tau\tau^*U^\dagger &= U\tau(U^\dagger U)^*\tau^*U^\dagger = (U\tau U^T)(U\tau U^T)^* \\ &= \mathrm{diag}(\tau)\mathrm{diag}(\tau^*) = \mathrm{diag}(\tau\tau^*). \end{aligned}$$

Dessa forma, diagonalizando-se $\tau\tau^*$ e tomando as raízes quadradas de seus autovalores obtemos os autovalores de τ. Mas os autovalores de $\tau\tau^*$ são idênticos aos autovalores de $\rho\tilde{\rho}$. Para provarmos isso, precisamos dos elementos de matriz de $\rho\tilde{\rho}$, i.e, precisamos calcular $\langle u_i|\rho\tilde{\rho}|u_j\rangle = \langle v_i|\rho\tilde{\rho}|v_j\rangle/\sqrt{p_ip_j}$. Mas,

$$\begin{aligned} \langle v_i|\rho\tilde{\rho}|v_j\rangle &= \langle v_i|\left(\sum_{k=1}^{n}|v_k\rangle\langle v_k|\right)\left(\sum_{l=1}^{n}|\tilde{v}_l\rangle\langle\tilde{v}_l|\right)|v_j\rangle \\ &= \sum_{k,l=1}^{n}\langle v_i|v_k\rangle\langle v_k|\tilde{v}_l\rangle\langle\tilde{v}_l|v_j\rangle = \sum_{k,l=1}^{n}p_i\delta_{ik}\langle v_k|\tilde{v}_l\rangle\langle v_j|\tilde{v}_l\rangle^* \\ &= \sum_{l=1}^{n}p_i\tau_{il}\tau_{jl}^* = \sum_{l=1}^{n}p_i\tau_{il}\tau_{lj}^* = p_i(\tau\tau^*)_{ij}. \end{aligned}$$

Dessa forma, os elementos de matriz de $\rho\tilde{\rho}$ são

$$(\rho\tilde{\rho})_{ij} = \langle u_i|\rho\tilde{\rho}|u_j\rangle = \sqrt{\frac{p_i}{p_j}}(\tau\tau^*)_{ij}.$$

Sejam $A_{ij} = (\rho\tilde{\rho})_{ij}$ e $B_{ij} = (\tau\tau^*)_{ij}$. Só nos resta mostrar que duas matrizes quadradas A e B, de dimensão n, nas quais seus elementos de matriz satisfazem a relação $A_{ij} = \sqrt{p_i/p_j}B_{ij}$ possuem os mesmos autovalores. Suponhamos que A já esteja diagonalizada e seus autovetores sejam dados por $\mathbf{a}_i = (a_{1i},\ldots,a_{ni})^T$ e seus autovalores por λ_i. Sendo assim, $A\mathbf{a}_i = \lambda_i\mathbf{a}_i$. Escrevendo esta última relação em termos de suas componenentes

$$\sum_{j=1}^{n}A_{kj}a_{ji} = \lambda_i a_{ki}, \qquad k = 1,\ldots,n.$$

Se queremos diagonalizar B, devemos resolver um sistema de equações semelhante. Numa notação óbvia,

$$\sum_{j=1}^{n}B_{kj}b_{ji} = \gamma_i b_{ki}, \qquad k = 1,\ldots,n.$$

Usando a relação entre as matrizes A e B,

$$\sum_{j=1}^{n}B_{kj}b_{ji} = \gamma_i b_{ki} \Longrightarrow \sum_{j=1}^{n}A_{kj}\sqrt{p_j}b_{ji} = \gamma_i\sqrt{p_k}b_{ki}.$$

Supondo $b_{ji} = a_{ji}/\sqrt{p_j}$, o sistema acima adimite solução apenas quando $\gamma_i = \lambda_i$, mostrando que A e B possuem os mesmos autovalores. Logo, retornando ao problema original, diagonalizando-se $\rho\tilde{\rho}$ e tomando as raízes quadradas de seus autovalores obtemos todos os λ_i's (autovalores de τ).

Decomposição 2:

$$\rho = \sum_{i=1}^{n} |y_i\rangle\langle y_i|, \quad \langle y_1|\tilde{y}_j\rangle = \lambda_1\delta_{1j} \text{ e } \langle y_i|\tilde{y}_j\rangle = -\lambda_i\delta_{ij} \text{ se } i,j > 1. \tag{3.23}$$

Essa decomposição é facilmente obtida a partir da anterior, bastando redefinir as fases globais dos vetores $|x_j\rangle$ da seguinte forma,

$$\begin{aligned} |y_1\rangle &= |x_1\rangle, \\ |y_j\rangle &= \mathrm{i}|x_j\rangle, \text{ se } j \neq 1. \end{aligned}$$

Vamos definir a 'pré-concorrência' ($c(\psi)$), a qual nada mais é do que a concorrência sem seu valor absoluto, ou seja,

$$c(\psi) = \frac{\langle\psi|\tilde{\psi}\rangle}{\langle\psi|\psi\rangle}. \tag{3.24}$$

Usando a decomposição 2 de ρ e lembrando que a proporção de cada estado nessa decomposição vale $\langle y_i|y_i\rangle$ (estados subnormalizados), obtemos para sua pré-concorrência média,

$$\langle c\rangle = \sum_{i=1}^{n}\langle y_i|y_i\rangle\frac{\langle y_i|\tilde{y}_i\rangle}{\langle y_i|y_i\rangle} = \sum_{i=1}^{n}\langle y_i|\tilde{y}_i\rangle = \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 = C(\rho). \tag{3.25}$$

A grandeza $C(\rho)$ foi definida quando apresentamos o teorema 10 e usamos a convenção na qual $\lambda_i = 0$ quando $i > n$ e $n < 4$.

Decomposição 3:

A última decomposição procurada é aquela onde além de $\langle c\rangle = C(\rho)$, cada estado $|z_i\rangle$ também tenha a mesma pré-concorrência: $c(z_1) = \ldots = c(z_n)$. Dessa forma, $\langle c\rangle = c(z_i)$ e, portanto, o emaranhamento médio para essa decomposição (EoF_z) vale

$$EoF_z = \sum_{i=1}^{n} p_i\mathcal{E}(c(z_i)) = \sum_{i=1}^{n} p_i\mathcal{E}(C(\rho)) = \mathcal{E}(C(\rho)).$$

Agora temos de mostrar que é possível obter essa decomposição e que EoF_z é mínimo, sendo, pois, o Emaranhamento de Formação procurado.

Seja $\rho = \sum_i |z_i\rangle\langle z_i|$ a decomposição procurada. A sua pré-concorrência média vale $\langle c\rangle = \sum_i\langle z_i|\tilde{z}_i\rangle$. E como qualquer estado $|z_i\rangle$ pode ser obtido dos estados $|y_i\rangle$ via a transformação de coordenadas abaixo [50],

$$|z_i\rangle = \sum_{j=1}^{n} V_{ij}^{*}|y_j\rangle,$$

onde V é transformação unitária, a média da pré-concorrência vale

$$\begin{aligned}\langle c\rangle &= \sum_{i=1}^{n}\left(\sum_{j=1}^{n}V_{ij}\langle y_j|\right)\left(\sum_{k=1}^{n}V_{ik}|\tilde{y}_k\rangle\right)=\sum_{i,j,k=1}^{n}V_{ij}\langle y_j|\tilde{y}_k\rangle V_{ik}\\ &= \sum_{i,j,k=1}^{n}V_{ij}Y_{jk}V_{ki}^{T}=\sum_{i=1}^{n}\left(VYV^{T}\right)_{ii}=\mathrm{Tr}\left(VYV^{T}\right). \qquad (3.26)\end{aligned}$$

Aqui $Y_{jk}=\langle y_j|\tilde{y}_k\rangle$ é matriz diagonal real. A Eq. (3.26) mostra que $\langle c\rangle$ é invariante por transformações unitárias reais (transformações ortogonais): $\mathrm{Tr}(VYV^T)=\mathrm{Tr}(YV^TV)=\mathrm{Tr}(Y)$. Restringindo-nos a esse tipo de transformação podemos equalizar as pré-concorrências sem alterar seu valor médio $\langle c\rangle$. Para ver isso, sejam $|z_a\rangle$ e $|z_b\rangle$ dois vetores da expansão de ρ de modo que o primeiro tenha a maior pré-concorrência e o segundo a menor. Sejam as transformações ortogonais I (matriz identidade) e

$$J=\begin{pmatrix}0&0&0&1\\0&1&0&0\\0&0&1&0\\1&0&0&0\end{pmatrix}.$$

A identidade não altera nada e J troca $|z_a\rangle$ por $|z_b\rangle$, i. e., permuta a maior pré-concorrência pela menor. Por continuidade, existe uma transformação intermediária que iguale a pré-concorrência de $|z_a\rangle$ a $C(\rho)$. Repetindo esse procedimento mais duas vezes com os vetores restantes, equalizamos todas as pré-concorrências a $C(\rho)$.

Para provar que EoF_z é o valor mínimo dentre todas as possíveis decomposições, basta mostrar que nenhuma outra decomposição possui um valor médio para a concorrência menor que $C(\rho)$, haja vista que $\mathcal{E}$ é função convexa[2] e monotonicamente crescente. Podemos escrever a concorrência média de uma decomposição qualquer como a média dos valores absolutos das pré-concorrências. Então, procedendo da mesma maneira que nos levou à Eq. (3.26),

$$\langle C\rangle=\sum_{i=1}^{m}|\left(VYV^{T}\right)_{ii}|. \qquad (3.27)$$

Agora, V pode ter dimensão $m\times n$, mas suas colunas continuam sendo vetores ortonormais. Isso ocorre pois podemos ter, em geral, mais de n termos numa decomposição de ρ. Podemos reescrever a Eq. (3.27) da seguinte forma,

$$\langle C\rangle=\sum_{i=1}^{m}\left|\sum_{k,l=1}^{n}V_{ik}Y_{kl}V_{li}^{T}\right|=\sum_{i=1}^{m}\left|\sum_{k,l=1}^{n}V_{ik}V_{il}Y_{kl}\right|.$$

[2]Uma função é convexa se $\mathcal{E}\left(\sum_i p_iC(x_i)\right)\leq\sum_i p_i\mathcal{E}(C(x_i))$.

Lembrando que a matriz Y é diagonal e definindo $\alpha_{ik} = (V_{ik})^2$,

$$\langle C \rangle = \sum_{i=1}^{m} \left| \sum_{k=1}^{n} \alpha_{ik} Y_{kk} \right| \geq \left| \sum_{i=1}^{m} \sum_{k=1}^{n} \alpha_{ik} Y_{kk} \right| = \left| \sum_{i=1}^{m} \alpha_{i1} Y_{11} + \sum_{k=2}^{n} \sum_{i=1}^{m} \alpha_{ik} Y_{kk} \right|.$$

Substituindo os elementos da matriz Y na expressão anterior,

$$\langle C \rangle \geq \left| \lambda_1 \sum_{i=1}^{m} \alpha_{i1} - \sum_{k=2}^{n} \lambda_k \sum_{i=1}^{m} \alpha_{ik} \right|. \tag{3.28}$$

Podemos sempre definir a matriz V de maneira que todos os α_{i1}'s sejam reais e positivos. Isso é equivalente a uma redefinição das fases globais dos estados da decomposição de ρ obtidos a partir dos estados $|y_i\rangle$ por meio da transformação V. Assim, como as colunas de V são vetores ortonormais e os elementos da primeira coluna são todos reais positivos, $\sum_i \alpha_{i1} = 1$. Substituindo esse último resultado na Eq. (3.28),

$$\begin{aligned} \langle C \rangle &\geq \left| \lambda_1 - \sum_{k=2}^{n} \lambda_k \sum_{i=1}^{m} \alpha_{ik} \right| \geq \lambda_1 - \left| \sum_{k=2}^{n} \lambda_k \sum_{i=1}^{m} \alpha_{ik} \right| \\ &\geq \lambda_1 - \sum_{k=2}^{n} \lambda_k \sum_{i=1}^{m} |\alpha_{ik}| = \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4. \end{aligned}$$

Portanto, notando que $\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 = C(\rho)$,

$$\langle C \rangle \geq C(\rho) \Longrightarrow EoF(\rho) = EoF_z. \tag{3.29}$$

Caso 2) Consideremos, agora, que $\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 < 0$. Para que a condição anterior seja satisfeita, devemos ter, no mínimo, $n \geq 3$. Caso $n = 3$, usamos um estado auxiliar $|x_4\rangle$ (igual ao vetor nulo). Seja a decomposição 1 obtida anteriormente:

$$\rho = \sum_{i=1}^{n} |x_i\rangle\langle x_i|, \qquad \langle x_i|\tilde{x}_j\rangle = \lambda_i \delta_{ij}.$$

A partir do conjunto de vetores $\{|x_i\rangle\}$ construímos os estados,

$$\begin{aligned} |z_1\rangle &= \frac{1}{2}(\mathrm{e}^{\mathrm{i}\theta_1}|x_1\rangle + \mathrm{e}^{\mathrm{i}\theta_2}|x_2\rangle + \mathrm{e}^{\mathrm{i}\theta_3}|x_3\rangle + \mathrm{e}^{\mathrm{i}\theta_4}|x_4\rangle), \\ |z_2\rangle &= \frac{1}{2}(\mathrm{e}^{\mathrm{i}\theta_1}|x_1\rangle + \mathrm{e}^{\mathrm{i}\theta_2}|x_2\rangle - \mathrm{e}^{\mathrm{i}\theta_3}|x_3\rangle - \mathrm{e}^{\mathrm{i}\theta_4}|x_4\rangle), \\ |z_3\rangle &= \frac{1}{2}(\mathrm{e}^{\mathrm{i}\theta_1}|x_1\rangle - \mathrm{e}^{\mathrm{i}\theta_2}|x_2\rangle + \mathrm{e}^{\mathrm{i}\theta_3}|x_3\rangle - \mathrm{e}^{\mathrm{i}\theta_4}|x_4\rangle), \\ |z_4\rangle &= \frac{1}{2}(\mathrm{e}^{\mathrm{i}\theta_1}|x_1\rangle - \mathrm{e}^{\mathrm{i}\theta_2}|x_2\rangle - \mathrm{e}^{\mathrm{i}\theta_3}|x_3\rangle + \mathrm{e}^{\mathrm{i}\theta_4}|x_4\rangle). \end{aligned}$$

Os estados acima formam uma decomposição de ρ,

$$\rho = \sum_{i=1}^{n} |z_i\rangle\langle z_i|.$$

Calculando a concorrência para $|z_i\rangle$,

$$C(z_i) = |\langle z_i|\tilde{z}_i\rangle| = \frac{1}{4}\left|\sum_{j=1}^{n} \mathrm{e}^{-\mathrm{i}2\theta_j}\langle x_j|\tilde{x}_j\rangle\right| = \frac{1}{4}\left|\sum_{j=1}^{n}\lambda_j \mathrm{e}^{-\mathrm{i}2\theta_j}\right|.$$

Sempre podemos, no entanto, escolher as fases θ_j apropriadamente de tal forma que $C(z_i)$ seja nulo. Na verdade, queremos $\sum_j \lambda_j \mathrm{e}^{-\mathrm{i}2\theta_j} = 0$. Mas isso só pode ser feito quando $\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 < 0$, justamente a condição sobre os λ's que temos agora. Veja,

$$\begin{aligned}
\sum_j \lambda_j \mathrm{e}^{-\mathrm{i}2\theta_j} = 0 \quad &\Longleftrightarrow \quad \lambda_1 \mathrm{e}^{-\mathrm{i}2\theta_1} = -\sum_{j=2}^{4}\lambda_j \mathrm{e}^{-\mathrm{i}2\theta_j} \\
&\Longleftrightarrow \quad \left|\lambda_1 \mathrm{e}^{-\mathrm{i}2\theta_1}\right| = \left|\sum_{j=2}^{4}\lambda_j \mathrm{e}^{-\mathrm{i}2\theta_j}\right| \\
&\Longleftrightarrow \quad \lambda_1 \leq \sum_{j=2}^{4}\lambda_j \left|\mathrm{e}^{-\mathrm{i}2\theta_j}\right| \\
&\Longleftrightarrow \quad \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 \leq 0.
\end{aligned}$$

Assim, como para todo i, $C(z_i) = 0$, necessariamente devemos ter $EoF = 0$ e provamos o teorema. □

3.6 *EoF* para Estados Gaussianos Simétricos

Agora vamos detalhar a obtenção do *EoF* para estados Gaussianos simétricos conforme apresentada por Giedke *et al.* [36]. Após a apresentação desse resultado estaremos aptos a dar um passo à frente e obter os dois limitantes inferiores para o *EoF* de estados Gaussianos arbitrários [73].

Um dos conceitos centrais na dedução do *EoF* para estados simétricos está no reconhecimento da importância dos estados comprimidos de dois modos (*two-mode squeezed states*):

$$|\Psi_s(r)\rangle = \frac{1}{\cosh(r)}\sum_{n=0}^{\infty}\tanh^n(r)\,|n\rangle_1 \otimes |n\rangle_2\,, \tag{3.30}$$

onde $|n\rangle_j$ é o n-ésimo estado de Fock, i. e., $a_j^\dagger a_j\,|n\rangle_j = n\,|n\rangle_j$, j=1,2, $r \in (0,\infty)$ é o parâmetro de compressão (*squeezing parameter*) e $a_j = (X_j + iP_j)/\sqrt{2}$ é operador de destruição. $|\Psi_s(r)\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ e $X_{1,2}$ e $P_{1,2}$ são operadores canônicos.

A Eq. (3.30) pode ser posta da seguinte forma:

$$|\Psi_s(r)\rangle = e^{-r\left(a_1 a_2 - a_1^\dagger a_2^\dagger\right)}\,|00\rangle\,, \tag{3.31}$$

onde $|00\rangle$ é o estado de vácuo de Fock. Para ver que as Eqs. (3.30) e (3.31) são equivalentes basta lembrar que [83]

$$e^{-r\left(a_1 a_2 - a_1^\dagger a_2^\dagger\right)} = \frac{1}{\cosh(r)} e^{a_1^\dagger a_2^\dagger \tanh(r)} e^{-(a_1^\dagger a_1 + a_2^\dagger a_2)\ln(\cosh(r))} e^{-a_1 a_2 \tanh(r)}. \quad (3.32)$$

Aplicando o operador do lado direito da Eq. (3.32) em $|00\rangle$ obtemos a Eq. (3.30).

Os estados comprimidos estão, de um certo modo, intimamente relacionados às relações de incerteza de Heisenberg. Afirma-se isso pois eles são os estados que atingem o menor valor permitido para o produto das incertezas das variáveis canônicas posição ($X_{1,2}$) e momento ($P_{1,2}$). Além disso, eles são os estados que mais se aproximam do estado EPR original [30], só que com norma finita. Para realçar essa característica, vamos definir a seguinte relação de incerteza-EPR (Einstein, Podolsky e Rosen):

$$\Delta(\psi) \equiv \min\left\{1, \frac{1}{2}\left[\Delta_\psi^2(X_1 - X_2) + \Delta_\psi^2(P_1 + P_2)\right]\right\}, \quad (3.33)$$

onde $\Delta_\psi^2(R_j) = \langle R_j^2\rangle_\psi - \langle R_j\rangle_\psi^2$ é a dispersão do observável R_j. Essa expressão mede o grau de não-localidade do estado ψ e é zero para o estado EPR original. Isso significa que quanto mais um estado é não-local, mais a Eq. (3.33) aproxima-se de zero. Dizemos que um sistema com mínimo $\Delta(\psi)$ possui máxima correlação-EPR. Qualquer estado com $\Delta(\psi) < 1$ possui um certo grau de não-localidade. Quanto maior esse grau de não-localidade, mais próximo de zero $\Delta(\psi)$ se aproxima.

Para o estado comprimido dado pela Eq. (3.31), escrevendo sua incerteza-EPR em termos dos operadores de criação e destruição temos

$$\Delta(\Psi_s) = \min\left\{1, 1 + \left\langle a_1^\dagger a_1\right\rangle_{\Psi_s(r)} + \left\langle a_2^\dagger a_2\right\rangle_{\Psi_s(r)} - 2\mathrm{Re}\left(\langle a_1 a_2\rangle_{\Psi_s(r)}\right)\right\}. \quad (3.34)$$

Para simplificar a expressão anterior, precisamos das seguintes relações [8]:

$$S^\dagger(r) a_1 S(r) = a_1\cosh(r) + a_2^\dagger \sinh(r), \quad (3.35)$$
$$S^\dagger(r) a_2 S(r) = a_2\cosh(r) + a_1^\dagger \sinh(r), \quad (3.36)$$

onde $S(r) = e^{-r\left(a_1 a_2 - a_1^\dagger a_2^\dagger\right)}$ é o operador de compressão (*squeezing operator*). Dessa forma temos:

$$\begin{aligned}
\left\langle a_1^\dagger a_1\right\rangle_{\Psi_s(r)} &= \langle 00|\, S^\dagger(r) a_1^\dagger a_1 S(r)\, |00\rangle \\
&= \langle 00|\, S^\dagger(r) a_1^\dagger S(r) S^\dagger(r) a_1 S(r)\, |00\rangle \\
&= \langle 00|\, (a_1^\dagger\cosh(r) + a_2\sinh(r))(a_1\cosh(r) + a_2^\dagger\sinh(r))\, |00\rangle \\
&= \langle 01|\, (\sinh(r))(\sinh(r))\, |01\rangle \\
&= \sinh^2(r). \quad (3.37)
\end{aligned}$$

Por simetria $\left\langle a_2^\dagger a_2 \right\rangle_{\Psi_s(r)} = \left\langle a_1^\dagger a_1 \right\rangle_{\Psi_s(r)}$. Só nos resta calcular $\langle a_1 a_2 \rangle_{\Psi_s(r)}$:

$$\begin{aligned}
\langle a_1 a_2 \rangle_{\Psi_s(r)} &= \langle 00| S^\dagger(r) a_1 a_2 S(r) |00\rangle \\
&= \langle 00| S^\dagger(r) a_1 S(r) S^\dagger(r) a_2 S(r) |00\rangle \\
&= \langle 00| \left(a_1 \cosh(r) + a_2^\dagger \sinh(r)\right)\left(a_2 \cosh(r) + a_1^\dagger \sinh(r)\right) |00\rangle \\
&= \langle 10| \left(\cosh(r)\right)\left(\sinh(r)\right) |10\rangle \\
&= \sinh(r)\cosh(r). \qquad (3.38)
\end{aligned}$$

Assim, a Eq. (3.34) fica:

$$\begin{aligned}
\Delta(\Psi_s) &= \min\left\{1, 1 + 2\sinh^2(r) - 2\sinh(r)\cosh(r)\right\} \\
&= \min\left\{1, e^{-2r}\right\} \\
&= e^{-2r}. \qquad (3.39)
\end{aligned}$$

Agora que já temos a incerteza-EPR para os estados comprimidos, é natural tentar relacioná-la com sua quantidade de emaranhamento. Como os estados comprimidos são estados puros, seu emaranhamento é quantificado pela entropia de von Neunmann, que também é idêntica ao EoF. Usando as Eqs. (3.2), (3.3) e (3.30) temos:

$$EoF(\Psi_s) = -\sum_{n=0}^{\infty} \frac{\tanh^{2n}(r)}{\cosh^2(r)} \log_2\left(\frac{\tanh^{2n}(r)}{\cosh^2(r)}\right). \qquad (3.40)$$

Usando o fato de que $\log_2(a^m/b^n) = m\log_2(a) - n\log_2(b)$ na expressão anterior temos:

$$\begin{aligned}
EoF(\Psi_s) &= \frac{\log_2(\cosh^2(r))}{\cosh^2(r)} \sum_{n=0}^{\infty}(1+n)\tanh^{2n}(r) \\
&\quad - \frac{\log_2(\sinh^2(r))}{\cosh^2(r)} \sum_{n=0}^{\infty} n \tanh^{2n}(r). \qquad (3.41)
\end{aligned}$$

Calculando $\langle \Psi_s |\ \Psi_s \rangle$ usando as Eqs. (3.30) e (3.31) obtemos:

$$\sum_{n=0}^{\infty} \tanh^{2n}(r) = \cosh^2(r). \qquad (3.42)$$

Calculando $\left\langle a_1^\dagger a_1 \right\rangle_{\Psi_s(r)}$ usando a Eq. (3.30) e comparando com seu valor dado pela Eq. (3.37) temos:

$$\sum_{n=0}^{\infty} n \tanh^{2n}(r) = \sinh^2(r)\cosh^2(r). \qquad (3.43)$$

Usando as Eqs. (3.42) e (3.43) na Eq. (3.41) obtemos:

$$EoF(\Psi_s(r)) = \cosh^2(r)\log_2\left(\cosh^2(r)\right) - \sinh^2(r)\log_2\left(\sinh^2(r)\right). \qquad (3.44)$$

Definindo a função

$$f(\Delta) = c_+(\Delta)\,\log_2[c_+(\Delta)] - c_-(\Delta)\,\log_2[c_-(\Delta)], \tag{3.45}$$

onde $c_\pm = (\Delta^{-1/2} \pm \Delta^{1/2})^2/4$ e usando o fato de que $\Delta(\Psi_s) = e^{-2r}$ vemos que

$$EoF\,(\Psi_s(r)) = f\,[\Delta(\Psi_s(r))]\,. \tag{3.46}$$

Ou seja, conhecendo-se a incerteza-EPR, Eq. (3.34), é possível obter o emaranhamento do estado comprimido, Eq. (3.30), usando a Eq. (3.45). A Eq. (3.46) é a relação procurada entre incerteza-EPR e emaranhamento para estados comprimidos.

Precisamos, agora, definir uma expressão que nos será útil mais à frente.

$$\delta(c) \equiv 1 + 2\sum_{n=0}^{\infty} n(c_n^2 - c_n c_{n-1}), \tag{3.47}$$

onde c_n, n natural, são os coeficientes de Schmidt de um estado ψ qualquer. Rotulamos os autovetores da decomposição de Schmidt de tal forma que $c_n \geq c_{n+1}$. Dessa forma, $c_n^2 - c_n c_{n-1} \leq 0$, o que implica

$$\delta(c) \leq 1. \tag{3.48}$$

Além disso, para um estado simétrico ψ com decomposição de Schmidt cujas bases sejam os estados de Fock,

$$|\psi\rangle = \sum_{n=0}^{\infty} c_n\,|n\rangle_1\,|n\rangle_2\,, \tag{3.49}$$

temos que

$$\left\langle a_1^\dagger a_1 \right\rangle_\psi = \sum_{n=0}^{\infty} n c_n^2, \tag{3.50}$$

$$\langle a_1 a_2 \rangle_\psi = \sum_{n=0}^{\infty} n c_n c_{n-1}. \tag{3.51}$$

Substituindo as duas últimas Eqs. na Eq. (3.34) vemos que

$$\Delta(\psi) = \delta(c). \tag{3.52}$$

Ou seja, para estados com decomposição de Schmidt cujas bases são estados de Fock corretamente ordenados, a dispersão-EPR é igual a $\delta(c)$.

Com os resultados e definições anteriores, estamos prontos para demonstrar o seguinte lema:

Lema 7 *Para todos os estados ψ com decomposição de Schmidt*

$$|\psi\rangle = \sum_{n=0}^{\infty} c_n \, |u_n\rangle_1 \, |v_n\rangle_2 \,, \tag{3.53}$$

onde $\langle u_n \, | u_m \rangle = \langle v_n \, | v_m \rangle = \delta_{nm}$ e $c_n \geq c_{n+1}$ temos,

$$\Delta(\psi) \geq \delta(c). \tag{3.54}$$

Usando a Eq. (3.54), o lema 7 mostra que, dentre todos os possíveis estados ψ, aqueles com decomposição de Schmidt cujos autovetores sejam estados de Fock ordenados conforme a Eq. (3.49) possuem máxima correlação-EPR (mínimo $\Delta(\psi)$).
Prova: Como $\delta(c) \leq 1$ temos apenas que analisar a situação onde $\Delta(\psi) < 1$. Para simplificar a prova, supomos, sem perder em generalidade, que $\langle \psi | \, a_i \, | \psi \rangle = 0$, i=1,2. Caso ψ não satisfizesse a condição anterior, bastaria efetuar uma transformação unitária local para alcançar essa condição sem, no entanto, alterar os coeficientes de Schmidt e a incerteza-EPR de ψ [36]. Para ψ dado pela Eq. (3.53),

$$\begin{aligned}
\Delta(\psi) &= 1 + \langle \psi | \, a_1^\dagger a_1 \, | \psi \rangle + \langle \psi | \, a_2^\dagger a_2 \, | \psi \rangle - \langle \psi | \, a_1 a_2 \, | \psi \rangle - \langle \psi | \, a_1 a_2 \, | \psi \rangle^* \\
&= 1 + \sum_{n=0}^{\infty} c_n^2 \, \langle u_n | \, a_1^\dagger a_1 \, | u_n \rangle + \sum_{n=0}^{\infty} c_n^2 \, \langle v_n | \, a_2^\dagger a_2 \, | v_n \rangle \\
&\quad - \sum_{n,m=0}^{\infty} c_n c_m \left(\langle u_n | \, a_1 \, | u_m \rangle \, \langle v_n | \, a_2 \, | v_m \rangle + c.c. \right),
\end{aligned} \tag{3.55}$$

onde c.c. representa o complexo conjugado da expressão dentro dos parênteses. Sejam,

$$Z(u) \equiv 1 + 2 \sum_{n=0}^{\infty} c_n^2 \, \langle u_n | \, a_1^\dagger a_1 \, | u_n \rangle - 2 \sum_{n,m=0}^{\infty} c_n c_m \left| \langle u_n | \, a_1^\dagger \, | u_m \rangle \right|^2, \tag{3.56}$$

$$Z(v) \equiv 1 + 2 \sum_{n=0}^{\infty} c_n^2 \, \langle v_n | \, a_2^\dagger a_2 \, | v_n \rangle - 2 \sum_{n,m=0}^{\infty} c_n c_m \left| \langle v_n | \, a_2^\dagger \, | v_m \rangle \right|^2. \tag{3.57}$$

Agora,

$$\begin{aligned}
I(u,v) &\equiv \Delta(\psi) - \frac{Z(u) + Z(v)}{2} \\
&= \sum_{n,m=0}^{\infty} c_n c_m \left(\left| \langle u_n | \, a_1^\dagger \, | u_m \rangle \right|^2 + \left| \langle v_n | \, a_2^\dagger \, | v_m \rangle \right|^2 \right) \\
&\quad - \sum_{n,m=0}^{\infty} c_n c_m \left(\langle u_n | \, a_1 \, | u_m \rangle \, \langle v_n | \, a_2 \, | v_m \rangle + c.c. \right).
\end{aligned} \tag{3.58}$$

Definindo o número complexo

$$z = \langle u_n | \, a_1^\dagger \, | u_m \rangle - \langle v_n | \, a_2^\dagger \, | v_m \rangle^* \,, \tag{3.59}$$

e usando o fato de que $zz^* \geq 0$ temos

$$zz^* \equiv \sum_{n,m=0}^{\infty} c_n c_m \left(\left| \langle u_n | a_1^\dagger | u_m \rangle \right|^2 + \left| \langle v_n | a_2^\dagger | v_m \rangle \right|^2 \right) - \sum_{n,m=0}^{\infty} c_n c_m \left(\langle u_n | a_1 | u_m \rangle \langle v_n | a_2 | v_m \rangle + c.c. \right). \quad (3.60)$$

Comparando as Eqs. (3.58) e (3.60) vemos que ambas são idênticas. Dessa forma,

$$I(u,v) \geq 0 \rightarrow \Delta(\psi) \geq \frac{Z(u) + Z(v)}{2} \quad (3.61)$$

Assim,

$$\Delta(\psi) \geq \min\{Z(u), Z(v)\}. \quad (3.62)$$

Sem perda de generalidade podemos supor que $\min\{Z(u), Z(v)\} = Z(u) \equiv Z$. Por meio de uma sútil manipulação algébrica mostra-se que [36] $Z \geq \delta(c)$. Dessa forma, temos que $\Delta(\psi) \geq \delta(c)$. □

Vamos agora demonstrar o lema 8, que junto com o lema 7 nos permitirá demonstrar um teorema que nos será útil na determinação do EoF para estados Gaussianos simétricos.

Lema 8 *Para qualquer* $\Delta \in (0,1)$ *e qualquer sequência* $c = \{c_1, \ldots, c_n\}$, $c_n \geq c_{n+1}$, *onde* $\delta(c) = \Delta$, *temos que* $\mathbf{e}(c) \geq E(\Psi_s(r_\Delta))$. *Aqui,*

$$\mathbf{e}(c) = -\sum_{n=0}^{\infty} c_n^2 \log_2(c_n^2). \quad (3.63)$$

O lema 8 diz que para uma incerteza-EPR Δ fixa, os coeficientes de Schmidt $\{c_1, \ldots, c_n\}$ que minimizam o emaranhamento $E = \mathbf{e}(c)$ são aqueles que geram um estado comprimido de dois modos.

Prova: Para demonstrar esse lema temos que resolver um problema de minimização com duas restrições. Uma delas é a normalização dos coeficientes c_n: $||c|| = \sum_n c_n^2 = 1$ e a outra diz respeito a exigência posta pela própria tese do lema: $\delta(c) = \Delta$, i. e., o valor da função $\delta(c)$ tem que ser igual a incerteza-EPR Δ. As nossas variáveis no problema de otimização são os coeficientes c_n e a função que queremos minimizar é o emaranhamento $\mathbf{e}(c)$. Para minimizar $\mathbf{e}(c)$ temos que usar o método dos multiplicadores de Lagrange. Se $\mathbf{e}(c)$ é nossa função, $g_1(c) = 0$ e $g_2(c) = 0$ as restrições, e α_1 e α_2 os multiplicadores de Lagrange, então nosso problema é equivalente a minimizar a função

$$F(c) = \mathbf{e}(c) + \alpha_1 g_1(c) + \alpha_2 g_2(c). \quad (3.64)$$

No nosso caso, $g_1 = \delta(c) - \Delta$ e $g_2 = ||c|| - 1$. Escolhemos $\alpha_1 = \lambda/(2\ln(2))$ e $\alpha_2 = (\mu + 1)/\ln(2)$ para deixar expressões que estão por vir numa forma mais

enxuta. A função que temos de minimizar é,

$$F(c) = \mathbf{e}(c) + \frac{\lambda}{2\ln(2)}(\delta(c) - \Delta) + \frac{\mu+1}{\ln(2)}(||c|| - 1). \tag{3.65}$$

Para encontrarmos o mínimo,

$$\frac{\partial F(c)}{\partial c_N} = 0. \tag{3.66}$$

Ou seja,

$$\frac{\partial \mathbf{e}(c)}{\partial c_N} + \frac{\lambda}{2\ln(2)}\frac{\partial \delta(c)}{\partial c_N} + \frac{\mu+1}{\ln(2)}\frac{\partial ||c||}{\partial c_N} = 0. \tag{3.67}$$

Mas,

$$\frac{\partial \mathbf{e}(c)}{\partial c_N} = -\frac{2c_N}{\ln(2)}(1 + \ln(c_N^2)), \tag{3.68a}$$

$$\frac{\partial \delta(c)}{\partial c_N} = 2\left(2Nc_N - Nc_{N-1} - (1+N)c_{N+1}\right), \tag{3.68b}$$

$$\frac{\partial ||\mathbf{c}||}{\partial c_N} = 2c_N. \tag{3.68c}$$

Substituindo a Eq. (3.68) na Eq. (3.67) temos:

$$2c_N\left[N\lambda + \mu - \ln(c_N^2)\right] = \lambda\left[Nc_{N-1} + (N+1)c_{N+1}\right], \tag{3.69}$$

onde convenciona-se que $c_{-1} = 1$. Dessa forma, como não temos nenhum c_N igual a zero podemos dividir a Eq. (3.69) por c_N:

$$2\left[N\lambda + \mu - \ln(c_N^2)\right] = \lambda\left[Nx_{N-1}^{-1} + (N+1)x_N\right], \tag{3.70}$$

onde usamos

$$\frac{c_{N+1}}{c_N} \equiv x_N \equiv e^{-2r_N}. \tag{3.71}$$

Essa definição é válida pois $c_{N+1}/c_N \leq 1$ e sempre podemos encontrar um r_N tal que $e^{-2r_N} = x_N$. Escrevendo Eq. (3.70) para $N+1$ temos

$$2\left[(N+1)\lambda + \mu - \ln(c_{N+1}^2)\right] = \lambda\left[(N+1)x_N^{-1} + (N+2)x_{N+1}\right]. \tag{3.72}$$

Subtraindo a Eq. (3.70) da Eq. (3.72) e após um pouco de álgebra:

$$x_{N+1} = x_N - A_N - B_N, \tag{3.73}$$

onde

$$A_N = \frac{4}{N+2}\left[\sinh^2(r_N) - \frac{r_N}{r}\sinh^2(r)\right], \tag{3.74a}$$

$$B_N = \frac{N}{N+2}\left[\frac{1}{x_N} - \frac{1}{x_{N-1}}\right], \tag{3.74b}$$

$$\lambda = \frac{2r}{\sinh^2(r)}. \tag{3.74c}$$

Vamos agora determinar r_N. Fixando $r > 0$ há apenas três casos que temos de considerar: (i) $x_0 < e^{-2r}$, (ii) $x_0 > e^{-2r}$ e (iii) $x_0 = e^{-2r}$.
Caso (i): Aqui temos $r_0 > r$. Além disso, $A_0 = 2[\sinh^2(r_0) - (r/r_0)\sinh^2(r)]$ e $B_0 = 0$. Usando o fato de que $2\sinh^2(r) = (\cosh(2r) - 1)$ temos

$$A_0 = 2\sinh^2(r_0)\left[1 - \frac{r}{r_0}\frac{\cosh(2r) - 1}{\cosh(2r_0) - 1}\right]. \tag{3.75}$$

Mas sabemos que a expansão em série de Taylor de $\cosh(r)$ é

$$\cosh(r) = \sum_{n=0}^{\infty} \frac{r^{2n}}{(2n)!}. \tag{3.76}$$

Substituindo a Eq. (3.76) na Eq. (3.75) temos

$$A_0 = 2\sinh^2(r_0)\left[1 - \frac{\sum_{n=1}^{\infty} a_n r^{2n+1}}{\sum_{n=1}^{\infty} a_n r_0^{2n+1}}\right], \tag{3.77}$$

onde $a_n = 2^{2n}/(2n)!$. Mas como $r_0 > r$ então $\sum_{n=1}^{\infty} a_n r_0^{2n+1} > \sum_{n=1}^{\infty} a_n\ r^{2n+1}$. Portanto, $A_0 > 0$. Assim, como $x_1 = x_0 - A_0$ então $x_1 < x_0$, o que implica $r_1 > r_0 > r$. Dessa forma, repetindo o mesmo procedimento, só que agora trocando r_0 por r_1, vemos que $A_1 > 0$ e $B_1 > 0$, ou seja, $x_2 < x_1$. Continuando esse raciocínio, vemos que sempre teremos $x_{N+1} < x_N$, i. e., x_N é decrescente. Mas como $N \to \infty$ isso levará a um $x_N < 0$ para um dado N finito [36], fato que contradiz a definição de x_N. Dessa forma, não é possível que $x_0 < e^{-2r}$.
Caso(ii): Agora, $r_0 < r$. Usando o mesmo procedimento do item (i) é fácil mostrar que $A_0 < 0$. E como $B_0 = 0$ então $x_1 > x_0$. Procedendo por indução vemos que $A_N < 0$ e $B_N < 0$, ou seja, $x_{N+1} > x_N$. Mas o fato de x_N ser crescente faz com que os coeficientes c_N's sejam cada vez maiores. Mas isso inviabiliza a condição de normalização, i. e., temos $||c|| > 1$. Dessa forma, não é possível que $x_0 > e^{-2r}$.
Caso (iii): Só nos resta a condição onde $r = r_0$. Nesse caso, $A_N = B_N = 0$. Ou seja, $x_N = x_{N+1}$. Assim, $x_N = e^{-2r}$ para qualquer N. Isto quer dizer que os coeficientes c_N's obedecem uma progressão geométrica com razão x_N. Redefinindo r como $r = -(1/2)\ln(\tanh(s))$ vemos que $x_N = \tanh(s)$. Mas essa é justamente a razão da progressão geométrica dos coeficientes de um estado comprimido de dois modos com parâmetro de compressão s. (Veja Eq. (3.30)). Portanto, os c_N's só podem ser os coeficientes de um estado comprimido de dois modos. □

Posto que temos à mão os lemas 7 e 8, estamos aptos a apresentar e demonstrar o seguinte teorema:

Teorema 11 *Para qualquer estado puro $\psi \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, com incerteza-EPR $\Delta(\psi)$, seu emaranhamento $E(\psi)$ é nunca menor que o emaranhamento $E[\Psi_s(r_{\Delta(\psi)})]$ do estado comprimido $\Psi_s(r_{\Delta(\psi)})$ com mesma incerteza-EPR, i. e.,*

$$E(\psi) \geq E[\Psi_s(r_{\Delta(\psi)})],$$

onde $\Delta(\psi) = \Delta(\Psi_s) = e^{-2r_{\Delta(\psi)}}$.

Prova: Há dois casos para analisar.
(i) Se $\Delta(\psi) = 1$, então pela Eq. (3.39), $r_{\Delta(\psi)} = 0$. Mas pela Eq. (3.44), $E[\Psi_s(r_{\Delta(\psi)})]$ $= 0$. Como por definição $E(\psi) \geq 0$, logo $E(\psi) \geq E[\Psi_s(r_{\Delta(\psi)})]$.
(ii) Se $\Delta(\psi) < 1$, então pelas Eqs. (3.3) e (3.63) temos que $E(\psi) = \mathbf{e}(c)$. Mas pelo lema 8 sabemos que para uma incerteza-EPR dada por $\delta(\mathbf{c})$ os estados comprimidos são aqueles de menor emaranhamento: $\mathbf{e}(c) \geq E[\Psi_s(r_{\delta(c)})]$. Dessa forma, $E(\psi) \geq E[\Psi_s(r_{\delta(c)})]$. Por outro lado, o lema 7 afirma que a incerteza-EPR é menor para estados simétrios na base de Fock com coeficientes de expansão ordenados de maneira decrescente. Mas este é justamente o caso dos estados comprimidos. Então, $\Delta(\psi) \geq \delta(c) \Longrightarrow e^{-2r_{\Delta(\psi)}} \geq e^{-2r_{\delta(c)}} \Longrightarrow r_{\Delta(\psi)} \leq r_{\delta(c)}$. Mas como $E[\Psi_s(r)]$ é função monotonicamente crescente[3] de r temos que se $r_{\Delta(\psi)} \leq r_{\delta(c)}$ então $E[\Psi_s(r_{\Delta(\psi)})] \leq E[\Psi_s(r_{\delta(c)})]$. Portanto, $E(\psi) \geq E[\Psi_s(r_{\Delta(\psi)})]$. □

Precisamos esclarecer só mais algumas propriedades de estados Gaussianos simétricos para que, finalmente, possamos encontrar a expressão que nos forneça o EoF.

Um estado Gaussiano ρ é completamente especificado, por definição, se conhecemos sua matriz de covariância (CM) γ. Ela é definida da seguinte forma:

$$\gamma_{ij} \equiv \mathrm{Tr}[(R_i R_j + R_j R_i)\rho] - 2\mathrm{Tr}(R_i\rho)\mathrm{Tr}(R_j\rho), \tag{3.78}$$

onde $\{R_i, i = 1, \ldots, 4\} \equiv \{X_1, P_1, X_2, P_2\}$. Por meio de transformações unitárias locais, como mostramos no Cap. 2, podemos deixá-la da seguinte forma:

$$\gamma = \begin{pmatrix} n & 0 & k_x & 0 \\ 0 & n & 0 & -k_p \\ k_x & 0 & m & 0 \\ 0 & -k_p & 0 & m \end{pmatrix}. \tag{3.79}$$

Como lidamos com um estado Gaussiano simétrico e emaranhado então $n = m$ e podemos supor sem perda de generalidade que $k_x \geq k_p \geq 0$. Para que γ represente uma matriz fisicamente realizável, suas dispersões da posição e do momento devem satisfazer as relações de incerteza de Heisenberg. Aliado ao princípio de incerteza de Heisenberg, o teorema de Williamson [96] nos diz que

$$\det\gamma = (n^2 - k_p^2)(n^2 - k_x^2) \geq 1, \tag{3.80}$$

para que γ represente um estado físico. Lembrando que $k_x \geq k_p$ vemos que a condição acima é equivalente a

$$n^2 - k_x^2 \geq 1. \tag{3.81}$$

[3]Basta calcular a derivada de $E[\Psi_s(r)]$ em relação a r que facilmente vemos que ela é sempre positiva.

Aplicando a critério de separabilidade de Simon [88] para um estado Gaussiano simétrico e usando a Eq. (3.81) vemos que ele é emaranhado se

$$(n-k_x)(n-k_p)<1. \tag{3.82}$$

Implementando a transformação simplética local (fato este que não altera a quantidade de emaranhamento da matriz γ original),

$$S=S_1\otimes S_2=\begin{pmatrix} \left(\frac{n-k_p}{n-k_x}\right)^{\frac{1}{4}} & 0 & 0 & 0 \\ 0 & \left(\frac{n-k_x}{n-k_p}\right)^{\frac{1}{4}} & 0 & 0 \\ 0 & 0 & \left(\frac{n-k_p}{n-k_x}\right)^{\frac{1}{4}} & 0 \\ 0 & 0 & 0 & \left(\frac{n-k_x}{n-k_p}\right)^{\frac{1}{4}} \end{pmatrix}, \tag{3.83}$$

as variáveis canônicas se transformam da seguinte forma:

$$X_i \longrightarrow X_i'=\left(\frac{n-k_p}{n-k_x}\right)^{\frac{1}{4}}X_i, \tag{3.84}$$

$$P_i \longrightarrow P_i'=\left(\frac{n-k_x}{n-k_p}\right)^{\frac{1}{4}}P_i. \tag{3.85}$$

Calculando a incerteza-EPR $\Delta(\rho)$ para essas novas variáveis canônicas temos:

$$\Delta(\rho)\equiv\min\left\{1,\frac{1}{2}\left[\Delta_\rho^2(X_1'-X_2')+\Delta_\rho^2(P_1'+P_2')\right]\right\}. \tag{3.86}$$

Mas

$$\Delta_\rho^2(X_1'-X_2') = \left(\frac{n-k_p}{n-k_x}\right)^{\frac{1}{2}}(\gamma_{11}-\gamma_{13}), \tag{3.87}$$

$$\Delta_\rho^2(P_1'+P_2') = \left(\frac{n-k_x}{n-k_p}\right)^{\frac{1}{2}}(\gamma_{22}+\gamma_{24}). \tag{3.88}$$

Assim,

$$\Delta(\rho)=\min\left\{1,\sqrt{(n-k_x)(n-k_p)}\right\}. \tag{3.89}$$

Usando a Eq. (3.82) vemos que:

$$\Delta(\rho)=\sqrt{(n-k_x)(n-k_p)}\equiv\delta. \tag{3.90}$$

Por definição, o Emaranhamento de Formação de ρ é

$$EoF\equiv\inf_D\mathcal{E}(D), \tag{3.91}$$

onde o ínfimo é tomado com respeito a todos os conjuntos $D = \{p_i, \psi_i\}$ que geram uma decomposição de ρ, i. e.,

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| . \tag{3.92}$$

Para o conjunto D,

$$\mathcal{E}(D) \equiv \sum_i p_i E(\psi_i). \tag{3.93}$$

A somatória da Eq. (3.92) pode conter indíces contínuos (podemos ter integração), conforme veremos abaixo. Uma possível decomposição [36] D_0 de ρ é

$$\rho \propto \int_{\mathcal{R}^4} d\xi W(\xi) \left|\Psi_s(r_\delta)\right\rangle \left\langle\Psi_s(r_\delta)\right| W^\dagger(\xi) e^{-\frac{1}{4}\xi^T(\gamma-\gamma_\delta)^{-1}\xi}, \tag{3.94}$$

onde $W(\xi) = e^{i\xi^T R}$ é o operador de deslocamento de Weil, $\gamma_\delta \leq \gamma$ é a matriz de correlação do estado comprimido de dois modos dado pela Eq. (3.30), na qual $\Delta(\Psi_s(r_\delta)) = \delta$ e ξ é vetor real de dimensão quatro. Como $W(\xi)$ é operador local, então

$$\mathcal{E}(D_0) = E[\Psi_s(r_\delta)] = f\left[\Delta(\Psi_s(r_\delta))\right] = f(\delta). \tag{3.95}$$

Onde a penúltima igualdade decorre da Eq. (3.46).

Agora estamos finalmente prontos para apresentar e provar o teorema que nos diz quanto vale o *EoF* para estados Gaussianos simétricos.

Teorema 12 *$EoF(\rho) = f\left(\sqrt{(n-k_x)(n-k_p)}\right)$, onde ρ é estado Gaussiano simétrico e n, k_x e k_p são os elementos da matriz de covariância γ de ρ escrita em sua forma padrão, Eq. (3.79).*

Prova: Acabamos de mostrar que $\mathcal{E}(D_0) = f(\delta)$. Só nos resta agora provar que para qualquer outra decomposição D, $\mathcal{E}(D) \geq f(\delta)$, indicando que $\mathcal{E}(D_0)$ é o ínfimo procurado e, conseqüentemente, o Emaranhamento de Formação.

$$\begin{aligned} \mathcal{E}(D) &= \sum_i p_i E(\psi_i) && (3.96)\\ &\geq \sum_i p_i E[\Psi_s(r_{\Delta(\psi_i)})] && (3.97)\\ &= \sum_i p_i f[\Delta(\psi_i)]. && (3.98) \end{aligned}$$

A Eq. (3.96) vem da definição de $\mathcal{E}(D)$, a desigualdade dada pela Eq. (3.97) decorre do teorema 11 e a Eq. (3.98) advem da Eq. (3.46). Usando o fato de que a função f é convexa, i. e., $\sum_i p_i f(\Delta(\psi_i)) \geq f(\sum_i p_i \Delta(\psi_i))$ [36] temos

$$\mathcal{E}(D) \geq f\left(\sum_i p_i \Delta(\psi_i)\right). \tag{3.99}$$

Finalmente, usando o fato de que f é função decrescente de seus argumentos e de que $\delta \equiv \Delta(\rho)$ é função côncava [73], i. e., $\Delta(\rho) = \Delta(\sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|) \geq \sum_i p_i \Delta(\psi_i)$ temos

$$\mathcal{E}(D) \geq f\left[\Delta\left(\sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|\right)\right] = f[\Delta(\rho)] = f(\delta). \qquad \square \tag{3.100}$$

3.7 Limitantes Inferiores para o EoF

De posse do teorema 12 podemos demonstrar os dois limitantes inferiores [73] para o Emaranhamento de Formação de estados Gaussianos arbitrários. Para obter o primeiro usamos um procedimento de medida local que simetriza nosso estado Gaussiano e o fato de que é impossível aumentar o teor de emaranhamento do nosso sistema por meio de operações locais e comunicação clássica. O segundo é obtido via uma generalização para estados mistos do teorema 11 demonstrado na seção anterior.

3.7.1 Primeiro Limitante Inferior

Seja um estado Gaussiano qualquer. Supondo, sem perder em generalidade, que seus momentos de primeira ordem sejam nulos, ele pode ser representado de duas maneiras equivalentes [20]. Por sua função característica

$$\chi(r) = e^{-\frac{1}{4} r^T \gamma r}, \tag{3.101}$$

onde T significa transposição e $r = (x_1, p_1, x_2, p_2)^T$ é um vetor coluna real. Ou por sua distribuição de Wigner

$$W(r) = \frac{1}{\pi^2} \frac{1}{\sqrt{\det \gamma_W}} e^{-r^T \gamma_W r}. \tag{3.102}$$

As matrizes de covariância γ e γ_W satisfazem a seguinte relação:

$$\gamma_W = J^T \gamma^{-1} J, \tag{3.103}$$

onde $J = \bigoplus_{k=1}^{2} J_1$ é uma matriz 4×4 com $J_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Elas podem ser postas na seguinte forma padrão via transformações simpléticas locais:

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{3.104}$$

onde

$$A = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}, \quad B = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}, \quad C = \begin{pmatrix} k_x & 0 \\ 0 & k_p \end{pmatrix}. \tag{3.105}$$

Temos os mesmos conjuntos de equações para γ_W:

$$\gamma_W = \begin{pmatrix} A_W & C_W \\ C_W^T & B_W \end{pmatrix}, \tag{3.106}$$

onde

$$A_W = \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix}, \quad B_W = \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}, \quad C_W = \begin{pmatrix} K_x & 0 \\ 0 & K_p \end{pmatrix}. \tag{3.107}$$

Como já dissemos, os quatro parâmetros reais (n, m, k_x, k_p) caracterizam completamente um estado Gaussiano de dois modos e estão relacionados com os seguintes quatro invariantes por transformações simpléticas locais:

$$I_1 = n = \sqrt{\det A}, \tag{3.108a}$$

$$I_2 = m = \sqrt{\det B}, \tag{3.108b}$$

$$I_3 = k_x k_p = \det C, \tag{3.108c}$$

$$I_4 = nm(k_x^2 + k_p^2) = \mathrm{tr}\left(A J_1^T C J_1^T B J_1^T C^T J_1^T\right). \tag{3.108d}$$

Da mesma forma (N, M, K_x, K_p) também completamente especificam um estado Gaussiano de dois modos. Eles também podem ser obtidos de invariantes por transformações simpléticas locais. Estes invariantes, W_1, W_2, W_3 e W_4, satisfazem a Eq. (3.108), bastando trocar A, B e C por A_W, B_W e C_W e (n, m, k_x, k_p) por (N, M, K_x, K_p).

Depois dessa introdução a estados Gaussianos de dois modos, onde definimos e apresentamos grandezas que vamos usar mais à frente, podemos começar propriamente o cálculo do primeiro limitante inferior. Daqui em diante, todo parâmetro associado a um estado Gaussiano simétrico terá um acento til para diferenciá-lo dos parâmetros de um estado Gaussiano arbitrário. Seja, então, σ nosso estado simétrico e ρ nosso estado arbitrário. Supomos, sem perder em generalidade, que $\tilde{k}_x > 0$ e $\tilde{k}_p < 0$. Conforme mostramos na seção anterior, o EoF para estados simétricos é:

$$EoF(\sigma) = f\left(\sqrt{(\tilde{n} - |\tilde{k}_x|)(\tilde{n} - |\tilde{k}_p|)}\right), \tag{3.109}$$

onde,

$$f(\delta) = c_+(\delta)\, \log_2[c_+(\delta)] - c_-(\delta)\, \log_2[c_-(\delta)]. \tag{3.110}$$

Aqui $c_\pm = (\delta^{-1/2} \pm \delta^{1/2})^2/4$. Usando a Eq. (3.108) podemos escrever EoF em termos dos invariantes:

$$EoF(\sigma) = f\left(\sqrt{\tilde{I}_1 - \tilde{I}_3 - \sqrt{\tilde{I}_4 - 2\tilde{I}_1\tilde{I}_3}}\right). \tag{3.111}$$

Usando as Eqs. (3.103) e (3.108) obtemos as seguintes relações entre os invariantes de γ e γ_W:

$$I_1 = \frac{W_2}{W_5},\ I_2 = \frac{W_1}{W_5},\ I_3 = \frac{W_3}{W_5},\ I_4 = \frac{W_4}{W_5^2},\ I_5 = \frac{1}{W_5}, \tag{3.112}$$

onde $W_5 = \det\gamma_W$ e $I_5 = \det\gamma$.

Assim, devido à Eq. (3.112), o EoF para estados simétricos, Eq. (3.111), fica:

$$EoF(\sigma) = f\left(\sqrt{\frac{\tilde{W}_1 - \tilde{W}_3 - \sqrt{\tilde{W}_4 - 2\tilde{W}_1\tilde{W}_3}}{\tilde{W}_5}}\right). \tag{3.113}$$

Mas Giedke *et al.* [35] mostraram que um estado arbitrário Gaussiano ρ pode ser simetrizado no estado σ por meio de LOCC. Isso implica $EoF(\rho) \geq EoF(\sigma)$. Esquematicamente temos:

$$\rho \stackrel{LOCC}{\longrightarrow} \sigma \Longrightarrow EoF(\rho) \geq EoF(\sigma). \tag{3.114}$$

Só temos agora que reescrever a Eq. (3.113) em termos dos invariantes da matriz γ de ρ. É nesse passo que usamos o procedimento desenvolvido por Giedke *et al.* [35].

Seja ρ nosso estado arbitrário e γ_W sua matriz de covariância, onde supomos, sem perda de generalidade, $N > M$. Podemos por meio de LOCC obter um estado simétrico com a seguinte matriz $\tilde{\gamma}_W$:

$$\gamma_W = \begin{pmatrix} A_W & C_W \\ C_W^T & B_W \end{pmatrix}, \stackrel{LOCC}{\longrightarrow} \tilde{\gamma}_W = \begin{pmatrix} \tilde{A}_W & \tilde{C}_W \\ \tilde{C}_W^T & \tilde{B}_W \end{pmatrix}, \tag{3.115}$$

onde

$$\tilde{A}_W = \begin{pmatrix} \frac{N\cos^2\theta + (NM - K_x^2)\sin^2\theta}{\cos^2\theta + M\sin^2\theta} & 0 \\ 0 & \frac{N\cos^2\theta + NM\sin^2\theta}{\cos^2\theta + M\sin^2\theta} \end{pmatrix}, \tag{3.116}$$

$$\tilde{B}_W = \begin{pmatrix} \frac{M}{\cos^2\theta + M\sin^2\theta} & 0 \\ 0 & \sin^2\theta + M\cos^2\theta \end{pmatrix}, \tag{3.117}$$

$$\tilde{C}_W = \begin{pmatrix} \frac{K_x\cos\theta}{\cos^2\theta + M\sin^2\theta} & 0 \\ 0 & K_p\cos\theta \end{pmatrix}, \tag{3.118}$$

$$\tan^2\theta = \frac{N^2 - M^2}{M - N(NM - K_x^2)}. \tag{3.119}$$

A Eq. (3.119) garante que $\det\tilde{A}_W = \det\tilde{B}_W$. Essa condição representa o fato de que o estado Gaussiano com a matriz $\tilde{\gamma}_W$ acima é simétrico.

Usando as Eqs. (3.108, 3.116-3.118) e a hipótese de que $|K_x| \geq |K_p|$ podemos escrever a Eq. (3.113) do seguinte modo:[4]

$$EoF(\sigma) = f\left(\sqrt{\frac{\alpha - \sqrt{\beta}}{\epsilon}}\right), \tag{3.120}$$

[4]A hipótese de que $|K_x| \geq |K_p|$ é mera conveniência. Não há perda de generalidade por essa escolha. Precisamos dela para expressar corretamente K_x^2 em termos dos invariantes de γ_W, i. e., $K_x^2 = \frac{W_4 + \sqrt{W_4^2 - 4W_1W_2W_3^2}}{2\sqrt{W_1W_2}}$. Se tivéssemos suposto que $|K_x| < |K_p|$ teríamos um sinal negativo antes da raiz quadrada.

onde

$$\alpha = W_2 - W_3 + \sqrt{W_2}\tan^2\theta, \tag{3.121}$$

$$\epsilon = W_5 + \sqrt{W_1}(\sqrt{W_1 W_2} - K_x^2)\tan^2\theta, \tag{3.122}$$

$$\begin{aligned}\beta &= W_4 - 2W_2W_3 + \tan^2\theta\left[(W_4 - 2W_3 - W_3^2)\sqrt{W_2}\right. \\ &\left. +(1-W_2)K_x^2\sqrt{W_1}\right], \end{aligned}\tag{3.123}$$

$$\tan^2\theta = \frac{W_1 - W_2}{\sqrt{W_2} - \sqrt{W_1}(\sqrt{W_1W_2} - K_x^2)}, \tag{3.124}$$

$$K_x^2 = \frac{W_4 + \sqrt{W_4^2 - 4W_1W_2W_3^2}}{2\sqrt{W_1W_2}}. \tag{3.125}$$

Agora usando a Eq. (3.112) podemos colocar a Eq. (3.120) em termos dos invariantes da matriz γ. Logo, se trabalhamos com γ na sua forma padrão, Eq. (3.104), onde supomos, sem perda de generalidade, que $|k_x| \geq |k_p|$, a Eq. (3.120) é reescrita após uma longa manipulação algébrica como:[5]

$$EoF(\sigma) = f\left(\sqrt{\frac{nmh(n,m) - k_xk_ph(m,n) + |mk_x - nk_p|\sqrt{h(n,m)h(m,n)}}{g(n,m)}}\right), \tag{3.126}$$

onde

$$h(n,m) = n - m(nm - k_p^2) \tag{3.127a}$$

$$g(n,m) = m(1-m^2) + nk_p^2. \tag{3.127b}$$

A Eq. (3.126) é nosso primeiro limitante inferior para o EoF de estados Gaussianos arbitrários. Realçamos que, quando $n = m$, recuperamos o EoF para estados simétricos.

3.7.2 Segundo Limitante Inferior

Para demonstrar o segundo limitante inferior precisamos provar o seguinte teorema:

Teorema 13 *Para todos os estados Gaussianos bipartites ρ, $EoF(\rho) \geq EoF(\sigma)$, se $\Delta(\rho) = \Delta(\sigma)$ e σ é um estado simétrico Gaussiano.*

Aqui $\Delta(\rho)$ é a incerteza-EPR, Eq. (3.33).

Prova: Implementando uma transformação simplética local apropriada [36] na forma padrão da matriz γ de σ vemos que a incerteza-EPR para essa matriz é $\Delta(\sigma) =$

[5] Temos $m \geq n$ na forma padrão de γ porque supomos $N \geq M$ na forma padrão de γ_W. Isso é verdade pois pela Eq. (3.112) temos $n^2 = M^2/\det\gamma_W$ e $m^2 = N^2/\det\gamma_W$.

$\sqrt{\left(\tilde{n}-|\tilde{k}_x|\right)\left(\tilde{n}-|\tilde{k}_p|\right)}$. Mas a quantidade de emaranhamento é invariante por transformações locais. Isso significa que $EoF(\sigma) = f\left[\Delta(\sigma)\right] = f\left[\Delta(\rho)\right]$. Escrevendo ρ como

$$\rho = \sum_j p_j \left|\varphi_j\right\rangle \left\langle\varphi_j\right|, \tag{3.128}$$

onde a decomposição acima é aquela que forncece o EoF de ρ, i. e.,

$$EoF(\rho) = \sum_j p_j E(\varphi_j), \tag{3.129}$$

temos que

$$\begin{aligned} EoF(\sigma) &= f\left[\Delta\left(\sum_j p_j \left|\varphi_j\right\rangle \left\langle\varphi_j\right|\right)\right] \\ &\leq f\left[\sum_j p_j \Delta(\varphi_j)\right] \\ &\leq \sum_j p_j f\left[\Delta(\varphi_j)\right]. \end{aligned} \tag{3.130}$$

A primeira desigualdade é consequência da concavidade[6] de $\Delta(\rho)$ e do fato de que f é função decrescente de seu argumento. A segunda desigualdade é devida a convexidade de f. Agora usamos o fato de que um estado comprimido pode assumir qualquer valor de emaranhamento, bastando para isso variar seu parâmetro de compressão apropriadamente. Para cada estado puro da decomposição de ρ acima, associamos um estado comprimido com a mesma quantidade de emaranhamento: $E(\varphi_j) = E[\Psi_s(r_j)]$. Dessa forma, temos a seguinte relação para o EoF de ρ:

$$\begin{aligned} EoF(\rho) &= \sum_j p_j E(\varphi_j) = \sum_j p_j E[\Psi_s(r_j)] \\ &= \sum_j p_j f\left[\Delta[\Psi_s(r_j)]\right]. \end{aligned} \tag{3.131}$$

Agora, devido ao teorema 11, que provamos na seção anterior, sabemos que $\Delta(\varphi_j) \geq \Delta[\Psi_s(r_j)]$. Logo, usando este fato na Eq. (3.130) e que f é função decrescente de seu argumento temos:

$$EoF(\sigma) \leq \sum_j p_j f\left[\Delta(\varphi_j)\right] \leq \sum_j p_j f\left[\Delta\left[\Psi_s(r_j)\right]\right]. \tag{3.132}$$

Combinando as Eqs. (3.131) e (3.132) vemos que

$$EoF(\sigma) \leq EoF(\rho). \qquad \square \tag{3.133}$$

[6] Veja Apêndice E.

O teorema que acabamos de demonstrar nos diz que estados mistos Gaussianos simétricos são aqueles com menor EoF para uma dada incerteza-EPR. É interessante atentar que σ pode ser qualquer estado Gaussiano simétrico que tenha mesma incerteza-EPR que ρ, incluindo estados simétricos escritos como superposições de estados comprimidos.

Este teorema nos fornece como corolário o seguinte limitante inferior para o EoF de um estado Gaussiano arbitrário. Usando a Eq. (3.133) temos:

$$EoF(\rho) \geq EoF(\sigma) = f\left[\Delta(\rho)\right]. \tag{3.134}$$

Finalmente, implementamos uma transformação simplética local na matriz γ de ρ, Eq. (3.104), antes de calcular sua incerteza-EPR. Esta transformação pode ser vista como uma extensão a estados Gaussianos não-simétricos daquela introduzida por Giedke *et al.* [36] para estados simétricos. Esta transformação multiplica X_j por $\{[(n+m)/2 - |k_p|]/[(n+m)/2 - |k_x|]\}^{1/4}$. P_j é dividido pela mesma quantia. Calculanado agora $\Delta(\rho)$ obtemos:

$$EoF(\rho) \geq f\left[\min\left\{1, \sqrt{\left(\frac{n+m}{2} - |k_x|\right)\left(\frac{n+m}{2} - |k_p|\right)}\right\}\right]. \tag{3.135}$$

De novo vemos que esse limitante inferior se iguala ao EoF para estados simétricos sempre que $n = m$.

3.7.3 Utilidade dos Limitantes Inferiores

Vamos usar, agora, os dois limitantes inferiores que acabamos de deduzir, Eqs. (3.126) e (3.135), a fim de retratar sua utilidade na análise de alguns estados Gaussianos. Por completeza, apresentamos em termos dos invariantes (n, m, k_x, k_p) três desigualdades, as quais eles devem satisfazer, para que possam ser considerados parâmetros descrevendo estados Gaussianos emaranhados [35]. Supomos, sem perder em generalidade, $m \geq n$ e $|k_x| \geq |k_p|$.

$$\det\gamma + 1 \geq n^2 + m^2 + 2k_x k_p, \tag{3.136a}$$

$$nm - k_x^2 \geq 1, \tag{3.136b}$$

$$\det\gamma + 1 < n^2 + m^2 - 2k_x k_p. \tag{3.136c}$$

A última desigualdade é uma restrição que toda matriz γ deve satisfazer, posto que ela representa um estado Gaussiano emaranhado.

A Tabela abaixo mostra seis estados Gaussianos emaranhados e os valores de seus limitantes inferiores (LB1 e LB2). Estes seis sistemas Gaussianos são bem representativos. Olhando para esses limitantes inferiores, vemos que dependendo dos parâmetros do sistema, ora LB1 ou ora LB2 é o limitante inferior mais forte.

Tabela 3.1: A primeira coluna mostra os parâmetros da matriz γ quando escrita em sua forma padrão. As segunda e terceira colunas representam os dois limitantes inferiores para o *EoF* de estados Gaussianos mistos. O limitante inferior 1 é dado pela Eq. (3.126) e o limitante inferior 2 pela Eq. (3.135).

n, m, k_x, k_p	LB1	LB2
1.5, 2, 1.2, -1	0.14635	0.28919
1.5, 2, 1, -1	0.08687	0.14672
2, 3, 1.8, -1.2	0.02448	0.00681
1.7, 2.6, 1.3, -0.9	0.00549	0
2, 3, 1.7, -1.2	0.00725	0.00142
2, 2.5, 1.3, -1.2	0.00173	0.00001

Por exemplo, os primeiros dois sistemas possuem LB2 como limitante mais forte, enquanto os quatro últimos sistemas têm LB1 como o limitante mais forte. LB1 e LB2 também são úteis para nos ajudar a descartar possíveis candidatos ao *EoF* de um estado Gaussiano arbitrário. Consideremos, por exemplo, as funções

$$f_1 = f\left(\sqrt{\left(\sqrt{nm} - |k_x|\right)\left(\sqrt{nm} - |k_p|\right)}\right), \tag{3.137}$$

$$f_2 = f\left(\sqrt{\left(\sqrt{\frac{n^2+m^2}{2}} - |k_x|\right)\left(\sqrt{\frac{n^2+m^2}{2}} - |k_p|\right)}\right). \tag{3.138}$$

Tanto f_1 quanto f_2 são iguais ao *EoF* para estados simétricos quando $n = m$. Para o estado Gaussiano com $(n, m, k_x, k_p) = (2, 2.5, 1.3, -1.2)$ temos LB1 = 0.00173 > f_1 = 0.00091 e para $(n, m, k_x, k_p) = (1.5, 2, 1.1, -1)$ obtemos LB2 = 0.208853 > f_2 = 0.18621. Estes resultados mostram que tanto f_1 quanto f_2 não podem ser o EoF para estados arbitrários Gaussianos pois temos limitantes inferiores maiores do que f_1 e f_2.

3.8 Teletransporte e Medida de Emaranhamento Multipartite

Mostramos, no Cap. 1, o protocolo de teletransporte proposto, em 1993, por Bennett *et al.* [11]. Neste protocolo, o canal quântico necessário para efetuar o teletransporte de um qbit é um estado de Bell ($|\phi^+\rangle = (1/\sqrt{2})\ (|00\rangle + |11\rangle)$, por exemplo). Por meio de uma medida conjunta (medida de Bell) no qbit a ser teleportado e no seu qbit do canal quântico, Alice é capaz de transmitir o estado quântico que descreve

seu qbit, desde que ela também transmita 2 bits clássicos para Bob informando o resultado de sua medida.

Naturalmente somos levados a questionar se este protocolo se restringe a um qbit ou se é possível uma generalização para N qbits. Lee *et al.* [57], num artigo muito interessante, mostraram que é possível teletransportar um sistema de 2 qbits, $|\Phi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, usando como canal quântico um estado de 4 qbits mais 4 bits de informação clássica. No entanto, estes autores não construíram explicitamente este protocolo e não apresentaram uma generalização para N qbits. Além disso, eles também não caracterizaram detalhadamente que tipo de canal quântico precisamos para executar o protocolo.

Nesta Seção vamos construir explicitamente este protocolo e apresentar uma generalização para N qbits. Na construção do protocolo para 2 qbits, apresentamos um novo conjunto de 16 estados de Bell generalizados. Eles são um pouco diferentes daqueles criados por Gao *et al.* [33] para a realização de um protocolo probabilístico de teletransporte de 2 qbits. Mostramos também que as operações unitárias que Bob precisa realizar para completar o protocolo estão restritas a operações que podem ser implementadas individualmente em seus 2 qbits. Assim, portas lógicas difíceis de se implementar como o Não-Controlado (CNOT) não são necessárias para finalizar o protocolo.[7]

A maior motivação para definirmos estes 16 estados de Bell generalizados reside no fato de que, a partir deles, podemos facilmente construir uma "base mágica" generalizada. Mostramos que essa base mágica possui as mesmas propriedades interessantes do que a base mágica definida originalmente pela Ref. [14]. Com o auxílio dessa base mágica, generalizamos a concorrência criada por Wootters [99] e definimos o Emaranhamento de Teletransporte (E_T), o qual possui uma clara interpretação física em termos da eficiência que um sistema emaranhado de $2N$ qbits tem para teletransportar um estado de N qbits.

Vamos, agora, construir explicitamente o protocolo para teleportar quaisquer dois qbits [76], os quais podem ser sempre escritos como

$$|\phi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \tag{3.139}$$

onde a, b, c, e d são coeficientes complexos e supomos $|\phi\rangle$ normalizado. Os 16 estados de Bell generalizados [75], ou estados-G, para simplificar notação, são:

[7] O Não-Controlado é uma porta lógica que atua em 2 qbits. Considerando o primeiro qbit como o qbit de controle, ela produz o seguinte resultado: $|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$ e $|11\rangle \to |10\rangle$.

Grupo 1:

$$|g_1\rangle = \frac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right), \tag{3.140}$$

$$|g_2\rangle = \frac{1}{2}\left(|0000\rangle + |0101\rangle - |1010\rangle - |1111\rangle\right), \tag{3.141}$$

$$|g_3\rangle = \frac{1}{2}\left(|0000\rangle - |0101\rangle + |1010\rangle - |1111\rangle\right), \tag{3.142}$$

$$|g_4\rangle = \frac{1}{2}\left(|0000\rangle - |0101\rangle - |1010\rangle + |1111\rangle\right). \tag{3.143}$$

Grupo 2:

$$|g_5\rangle = \frac{1}{2}\left(|0001\rangle + |0100\rangle + |1011\rangle + |1110\rangle\right), \tag{3.144}$$

$$|g_6\rangle = \frac{1}{2}\left(|0001\rangle + |0100\rangle - |1011\rangle - |1110\rangle\right), \tag{3.145}$$

$$|g_7\rangle = \frac{1}{2}\left(|0001\rangle - |0100\rangle + |1011\rangle - |1110\rangle\right), \tag{3.146}$$

$$|g_8\rangle = \frac{1}{2}\left(|0001\rangle - |0100\rangle - |1011\rangle + |1110\rangle\right). \tag{3.147}$$

Grupo 3:

$$|g_9\rangle = \frac{1}{2}\left(|0010\rangle + |0111\rangle + |1000\rangle + |1101\rangle\right), \tag{3.148}$$

$$|g_{10}\rangle = \frac{1}{2}\left(|0010\rangle + |0111\rangle - |1000\rangle - |1101\rangle\right), \tag{3.149}$$

$$|g_{11}\rangle = \frac{1}{2}\left(|0010\rangle - |0111\rangle + |1000\rangle - |1101\rangle\right), \tag{3.150}$$

$$|g_{12}\rangle = \frac{1}{2}\left(|0010\rangle - |0111\rangle - |1000\rangle + |1101\rangle\right). \tag{3.151}$$

Grupo 4:

$$|g_{13}\rangle = \frac{1}{2}\left(|0011\rangle + |0110\rangle + |1001\rangle + |1100\rangle\right), \tag{3.152}$$

$$|g_{14}\rangle = \frac{1}{2}\left(|0011\rangle + |0110\rangle - |1001\rangle - |1100\rangle\right), \tag{3.153}$$

$$|g_{15}\rangle = \frac{1}{2}\left(|0011\rangle - |0110\rangle + |1001\rangle - |1100\rangle\right), \tag{3.154}$$

$$|g_{16}\rangle = \frac{1}{2}\left(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle\right). \tag{3.155}$$

Estes estados formam um base ortonormal, $\sum_{j=1}^{16} |g_j\rangle\langle g_j| = I$ e $\langle g_j|g_k\rangle = \delta_{jk}$, a qual chamamos de base de Bell generalizada [75], ou base-G.

Supomos também que Alice e Bob compartilham o estado $|g_1\rangle$ (qualquer outro

estado-G serviria). Logo, o estado inicial que descreve os qbits de Alice e Bob é

$$\begin{aligned}|\Phi\rangle &= |\phi\rangle \otimes |g_1\rangle \\ &= \frac{a}{2}\{|000000\rangle + |000101\rangle + |001010\rangle + |001111\rangle\} \\ &\quad + \frac{b}{2}\{|010000\rangle + |010101\rangle + |011010\rangle + |011111\rangle\} \\ &\quad + \frac{c}{2}\{|000000\rangle + |100101\rangle + |101010\rangle + |101111\rangle\} \\ &\quad + \frac{d}{2}\{|110000\rangle + |110101\rangle + |111010\rangle + |111111\rangle\}\end{aligned} \tag{3.156}$$

Aqui os primeiros quatro qbits pertencem a Alice e os restantes a Bob ($|AAAABB\rangle$, $A \rightarrow$ Alice e $B \rightarrow$ Bob). Usando as Eqs. (3.140-3.155) podemos escrever a Eq. (3.156) como

$$|\Phi\rangle = \frac{1}{4}\sum_{j=1}^{16} |g_j\rangle_A |\phi_j\rangle_B, \tag{3.157}$$

onde A e B são escritos para enfatizar quais qbits estão com Alice e Bob e os estados $|\phi_j\rangle$ estão definidos na Tabela 3.2.

Alice agora faz uma medida de Bell generalizada (medida-G) obtendo com iguais probabilidades um dos 16 estados-G. Por medida-G simbolizamos uma medida conjunta que Alice executa nos dois qbits a ser teleportado e nos dois qbits do estado-G compartilhado com Bob. Em seguida ela envia a Bob uma mensagem clássica de 4 bits informando qual estado-G ela obteve em sua medida. De posse dessa informação, Bob sabe qual operação unitária (Tabela 3.2) ele deve implementar em seus dois qbits para obter o estado teleportado, finalizando o protocolo.

Observando as 16 operações unitárias que Bob pode aplicar em seus dois qbits, vemos que todas podem ser escritas como $U = U_5 \otimes U_6$. Aqui 5 e 6 referem-se aos quinto e sexto qbits respectivamente, i. e., aos qbits de Bob. Isto mostra que precisamos apenas de operações de um qbit para implementar todas as 16 operações unitárias. Operações mais elaboradas, como a porta lógica CNOT, não são necessárias. Este fato possivelmente simplifica futuras realizações experimentais do protocolo.

Se usarmos canais quânticos formados por estados GHZ generalizados [75], i. e., $|GHZ\rangle = (1/\sqrt{2})\ (|0000\rangle + |1111\rangle)$, o protocolo não funciona. É impossível teleportar dois qbits arbitrários usando um estado GHZ. Apenas classes especiais de dois qbits tais como $b|01\rangle + c|10\rangle$ podem ser teleportadas [58].

As dificuldades técnicas que devem ser contornadas para experimentalmente realizar o protocolo não são nada triviais. Primeiro, Alice e Bob precisam ter uma fonte de estados-G. Segundo, Bob deve ser capaz de implementar as 16 operações locais, e Alice precisa de alguma forma realizar as medidas-G. De um certo modo, técnicas

Tabela 3.2: A primeira coluna mostra os estados $|\phi_j\rangle$. A terceira coluna mostra as transformações unitárias que Bob deve implementar em seus qbits, condicionado ao resultado da medida de Alice exposto na segunda coluna, para finalizar o protocolo.

$\|\phi_j\rangle$	Resultado de Alice	Operação de Bob
$\|\phi_1\rangle = \|\phi\rangle$	$\|g_1\rangle$	I
$\|\phi_2\rangle = \sigma_1^z\|\phi\rangle$	$\|g_2\rangle$	σ_1^z
$\|\phi_3\rangle = \sigma_2^z\|\phi\rangle$	$\|g_3\rangle$	σ_2^z
$\|\phi_4\rangle = \sigma_1^z\sigma_2^z\|\phi\rangle$	$\|g_4\rangle$	$\sigma_2^z\sigma_1^z$
$\|\phi_5\rangle = \sigma_2^x\|\phi\rangle$	$\|g_5\rangle$	σ_2^x
$\|\phi_6\rangle = \sigma_2^x\sigma_1^z\|\phi\rangle$	$\|g_6\rangle$	$\sigma_1^z\sigma_2^x$
$\|\phi_7\rangle = \sigma_2^x\sigma_2^z\|\phi\rangle$	$\|g_7\rangle$	$\sigma_2^z\sigma_2^x$
$\|\phi_8\rangle = \sigma_2^x\sigma_2^z\sigma_1^z\|\phi\rangle$	$\|g_8\rangle$	$\sigma_1^z\sigma_2^z\sigma_2^x$
$\|\phi_9\rangle = \sigma_1^x\|\phi\rangle$	$\|g_9\rangle$	σ_1^x
$\|\phi_{10}\rangle = \sigma_1^x\sigma_1^z\|\phi\rangle$	$\|g_{10}\rangle$	$\sigma_1^z\sigma_1^x$
$\|\phi_{11}\rangle = \sigma_1^x\sigma_2^z\|\phi\rangle$	$\|g_{11}\rangle$	$\sigma_2^z\sigma_1^x$
$\|\phi_{12}\rangle = \sigma_1^x\sigma_1^z\sigma_2^z\|\phi\rangle$	$\|g_{12}\rangle$	$\sigma_2^z\sigma_1^z\sigma_1^x$
$\|\phi_{13}\rangle = \sigma_1^x\sigma_2^x\|\phi\rangle$	$\|g_{13}\rangle$	$\sigma_2^x\sigma_1^x$
$\|\phi_{14}\rangle = \sigma_1^x\sigma_2^x\sigma_1^z\|\phi\rangle$	$\|g_{14}\rangle$	$\sigma_1^z\sigma_2^x\sigma_1^x$
$\|\phi_{15}\rangle = \sigma_1^x\sigma_2^x\sigma_2^z\|\phi\rangle$	$\|g_{15}\rangle$	$\sigma_2^z\sigma_2^x\sigma_1^x$
$\|\phi_{16}\rangle = \sigma_1^x\sigma_2^x\sigma_1^z\sigma_2^z\|\phi\rangle$	$\|g_{16}\rangle$	$\sigma_2^z\sigma_1^z\sigma_2^x\sigma_1^x$

experimentais tanto para a produção do canal quântico quanto para a realização das operações unitárias nos qbits de Bob já estão à disposição [64, 102]. Entretanto, ainda precisamos de maneiras eficientes para discriminar os 16 estados-G.

O protocolo anterior pode ser generalizado para teletransportar um estado de N qbits. Para isso, Alice precisa compartilhar um estado-G de $2N$ qbits. Em seguida ela executa um medida-G com os N qbits a serem teleportados e com metade do estado-G compartilhado com Bob. Depois ela envia uma mensagem de $2N$ bits clássicos a Bob informando o resultado da medida. Bob finaliza o protocolo executando no máximo $2N$ operações unitárias de um qbit para obter o estado teleportado. O número de operações unitárias que Bob deve implementar em seus N qbits está condicionado ao resultado da medida de Alice. O protocolo de teletransporte de N qbits pode ser assim formalmente esquematizado:

(1) Gera-se o estado-G semente $|s_0\rangle = (2^{-N/2})\sum_{j=0}^{M}|x_j\rangle_A\,|x_j\rangle_B$, onde $M = 2^N - 1$ e x_j é a representação binária do número j. No protocolo de dois qbits, $x_0 = 00$, $x_1 = 01$, $x_2 = 10$, e $x_3 = 11$. Zeros devem ser acrescentados para deixar todos x_j com o mesmo número de bits (N bits). Este estado-G é nosso canal quântico

e é composto de $2N$ qbits;

(2) Usando o estado-G semente é possível obter todos os outros estados-G operando localmente nos primeiros N qbits, $|s_j\rangle = \bigotimes_{k=1}^{N} (\sigma_k^z)^{j_{2k-1}} (\sigma_k^x)^{j_{2k}} |s_0\rangle$. Agora j_k representa o k-ésimo bit (da direita para a esquerda) do número $0 \leq j \leq 2^{2N} - 1$, o qual é escrito em notação binária e novamente zeros devem ser acrescentados para deixar todos os j's com o mesmo número de bits ($2N$ bits). O índice k indica em qual qbit as matrizes de Pauli σ^x e σ^z devem operar. Para o protocolo de dois qbits mostrado anteriormente, $|s_0\rangle = |g_1\rangle$, $|s_1\rangle = |g_2\rangle$, $|s_2\rangle = |g_9\rangle$, $|s_3\rangle = |g_{10}\rangle$, e assim por diante;

(3) Alice faz uma medida-G com os N qbits a ser teleportado e com seus N qbits do estado-G compartilhado com Bob. Ela, então, envia a Bob uma mensagem de $2N$ bits clássicos informando o resultado de sua medida;

(4) Com esta informação, Bob implementa a transformação unitária apropriada em seus N qbits. Estas operações são dadas por $U_j = \bigotimes_{k=1}^{N} (\sigma_k^z)^{j_{2k-1}} (\sigma_k^x)^{j_{2k}}$ e para o protocolo de dois qbits elas estão descritas na Tabela 3.2.

Vamos agora definir a base mágica generalizada $\{|e_j\rangle\}$ e uma base auxiliar $\{|f_j\rangle\}$, a qual nos ajudará nos cálculos mais à frente. Veja a Tabela 3.3. Em termos dos estados-F, um estado de dois qbits pode ser escrito como $|\Psi\rangle = \sum_{j=1}^{16} \alpha_j |f_j\rangle$. A partir desse estado definimos $|\Psi^*\rangle = \sum_{j=1}^{16} \alpha_j^* |f_j\rangle$, onde α_j^* significa o complexo conjugado de α_j. Usando essas definições, podemos apresentar a concorrência generalizada [97],

$$C(\Psi) = \left| \langle \Psi^* | \sigma_y^{\otimes 4} | \Psi \rangle \right|, \tag{3.158}$$

onde $\sigma_y^{\otimes 4} = \sigma_1^y \sigma_2^y \sigma_3^y \sigma_4^y$. Como $\sigma_y^{\otimes 4} \ |\Psi\rangle = \sum_{j=1}^{16} (-1)^{j+1} \ \alpha_j \ |f_j\rangle$,

$$C(\Psi) = \left| \sum_{j=1}^{16} (-1)^{j+1} \alpha_j^2 \right|. \tag{3.159}$$

Mas na base mágica $|\Psi\rangle = \sum_{j=1}^{16} \beta_j |e_j\rangle$. Então, usando a relação entre os estados-F e os estados mágicos dada na Tabela 3.3 podemos mostrar que $\alpha_j = \mathrm{i}^{(j+1)\oplus 2} \beta_j$, onde $a \oplus 2 = 0$ se a é par e 1 se a é ímpar. Isso implica,

$$C(\Psi) = \left| \sum_{j=1}^{16} \beta_j^2 \right|. \tag{3.160}$$

Usando a Eq. (3.160) podemos mostrar que a Eq. (3.158) satisfaz as mesmas propriedade que a concorrência originalmente definida por Wootters [99]. (1) Se todos os β_j's são reais então $C = 1$; (2) $0 \leq C \leq 1$; (3) na base mágica, $C = |\langle \Psi^* | \Psi \rangle|$; (4) todo estado de dois qbits com $C = 1$ pode ser escrito, a menos de uma fase

Tabela 3.3: A primeira coluna mostra os estados mágicos. A segunda coluna representa os estados-G e a terceira coluna os estados-F. Os três elementos de uma mesma linha devem ser lidos como $a = b = c$.

Estados mágicos	Estados-G	Estados-F
$\|e_1\rangle$	$\|g_1\rangle$	$\|f_1\rangle$
$\|e_2\rangle$	$\mathrm{i}\|g_2\rangle$	$\mathrm{i}\|f_2\rangle$
$\|e_3\rangle$	$\|g_4\rangle$	$\|f_3\rangle$
$\|e_4\rangle$	$\mathrm{i}\|g_3\rangle$	$\mathrm{i}\|f_4\rangle$
$\|e_5\rangle$	$\|g_6\rangle$	$\|f_5\rangle$
$\|e_6\rangle$	$\mathrm{i}\|g_5\rangle$	$\mathrm{i}\|f_6\rangle$
$\|e_7\rangle$	$\|g_7\rangle$	$\|f_7\rangle$
$\|e_8\rangle$	$\mathrm{i}\|g_8\rangle$	$\mathrm{i}\|f_8\rangle$
$\|e_9\rangle$	$\|g_{10}\rangle$	$\|f_9\rangle$
$\|e_{10}\rangle$	$\mathrm{i}\|g_9\rangle$	$\mathrm{i}\|f_{10}\rangle$
$\|e_{11}\rangle$	$\|g_{11}\rangle$	$\|f_{11}\rangle$
$\|e_{12}\rangle$	$\mathrm{i}\|g_{12}\rangle$	$\mathrm{i}\|f_{12}\rangle$
$\|e_{13}\rangle$	$\|g_{13}\rangle$	$\|f_{13}\rangle$
$\|e_{14}\rangle$	$\mathrm{i}\|g_{14}\rangle$	$\mathrm{i}\|f_{14}\rangle$
$\|e_{15}\rangle$	$\|g_{16}\rangle$	$\|f_{15}\rangle$
$\|e_{16}\rangle$	$\mathrm{i}\|g_{15}\rangle$	$\mathrm{i}\|f_{16}\rangle$

global, como uma combinação de estados mágicos com coeficientes reais; e (5) todos os estados mágicos possuem $C = 1$. Notando que $\sigma_y^{\otimes 4}$ é um operador que troca a direção do spin de todos os qbits, vemos que se $|\Psi\rangle$ é separável então $C = 0$.

A fim de quantificar a eficiência de um estado de quatro qbits para teleportar dois qbits, introduzimos o Emaranhamento de Teletransporte (E_T) [76]:

$$E_T(\Psi) = \frac{1}{16}\sum_{j=1}^{L} C(\Psi_j), \tag{3.161}$$

onde $|\Psi_j\rangle$ são todos os $L \leq 16$ estados ortogonais que podem ser obtidos de $|\Psi\rangle$ usando as 16 operações unitárias U_j listadas na terceira coluna da Tabela 3.2. Deve-se notar que as Eqs. (3.158) e (3.161) podem facilmente ser generalizadas para um estado de $2N$ qbits:

$$C(\Psi) = \left|\langle\Psi^*|\sigma_y^{\otimes 2N}|\Psi\rangle\right|, \tag{3.162}$$

$$E_T(\Psi) = \frac{1}{2^{2N}}\sum_{j=1}^{L} C(\Psi_j), \tag{3.163}$$

onde agora $|\Psi_j\rangle$ são os $L \leq 2^{2N}$ estados ortogonais obtidos a partir de $|\Psi\rangle$ usando as 2^{2N} operações unitárias $U_j = \bigotimes_{k=1}^{N} (\sigma_k^z)^{j_{2k-1}} (\sigma_k^x)^{j_{2k}}$. E_T satisfaz algumas propriedade interessantes: (1) Ele pode discriminar os estados generalizados W, GHZ e os estados-G, i. e. $E_T(W) < E_T(GHZ) < E_T(g_j)$; (2) Ele pode ser visto como uma medida da eficiência de $2N$ qbits para teleportar N qbits; (3) Todos os estados-G possuem $E_T = 1$; (4) Todos estados separáveis possuem $E_T = 0$.

Para ilustrarmos as propriedades acima, vamos nos concentrar no caso de quatro qbits. Seja o estado-G $|g_1\rangle$. Implementando a operação U_j obtemos 16 estados ortogonais (a base-G) com $C = 1$. Portanto, $E_T = 1$. Agora, estudando o estado GHZ generalizado $|GHZ^+\rangle = (1/\sqrt{2})(|0000\rangle + |1111\rangle)$, as 16 operações unitárias U_j produzem apenas oito estados ortogonais com $C = 1$,

$$|GHZ^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0000\rangle \pm |1111\rangle), \tag{3.164}$$

$$|G^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0100\rangle \pm |1011\rangle), \tag{3.165}$$

$$|H^{\pm}\rangle = \frac{1}{\sqrt{2}}(|1000\rangle \pm |0111\rangle), \tag{3.166}$$

$$|Z^{\pm}\rangle = \frac{1}{\sqrt{2}}(|1100\rangle \pm |0011\rangle). \tag{3.167}$$

Assim, $E_T = 1/2$. Repetindo o mesmo procedimento com o estado W generalizado $|W\rangle = (1/2)(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$ obtemos oito estados ortogonais com $C = 0$, i. e., $E_T = 0$. Podemos entender fisicamente o significado destes valores para E_T notando que usando os estados-G ($E_T = 1$) podemos deterministicamente teleportar qualquer estado de dois qbits. Usando, no entanto, os estados GHZ ($E_T = 1/2$), apenas algumas classes especiais de estados de dois qbits podem ser teleportados [58]. Para os estados W nem mesmo estas classes especiais podem ser deterministicamente teleportadas. E mais, podemos mostrar que o estado GHZ é capaz de teleportar deterministicamente um qbit e, por sua vez, o estado W realiza esta tarefa apenas prababilisticamente.

3.9 Codificação Superdensa Multipartite

No Cap. 1 mostramos que se Alice e Bob compartilham um estado de máximo emaranhamento ($(1/\sqrt{2})(|00\rangle + |11\rangle)$, por exemplo), Alice pode transmitir 2 bits de informação a Bob manipulando e enviando-lhe apenas um qbit [12].

Usando-se um estado GHZ tripartite ($(1/\sqrt{2})(|000\rangle + |111\rangle)$) pode-se mostrar que é possível transmitir 3 bits enviando apenas dois qbits [39, 23]. Comparando-se com a proposta original, na qual temos 2 bits de informação por qbit enviado, agora temos somente 1.5 bit de informação por qbit.

A seguir mostramos que uma pequena modificação no protocolo de teletransporte apresentado na seção anterior nos permite transmitir 4 bits de informação enviando-se apenas dois qbits.

Primeiramente, Alice e Bob devem compartilhar o estado $|g_1\rangle$, o mesmo usado no teletransporte de dois qbits:

$$|g_1\rangle = \frac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right). \tag{3.168}$$

No estado acima, os dois primeiros qbits estão com Alice e os outros dois com Bob ($|AABB\rangle$, $A \rightarrow$ Alice e $B \rightarrow$ Bob). Para conseguir transmitir sua mensagem de 4 bits, Alice deve ser capaz de localmente transformar o estado $|g_1\rangle$ em qualquer um dos estados $|g_i\rangle$. A Tabela 3.4 mostra como Alice operando localmente pode gerar os 16 estados-G.

Tabela 3.4: Aqui temos as 16 operações locais que Alice deve realizar em seus dois qbits para obter qualquer estado-G, os quais são utilizados para codificar a mensagem de 4 bits para Bob.

Grupo 1	Grupo 2
$\|g_1\rangle = I\|g_1\rangle$	$\|g_5\rangle = \sigma_2^x\|g_1\rangle$
$\|g_2\rangle = \sigma_1^z\|g_1\rangle$	$\|g_6\rangle = \sigma_1^z\sigma_2^x\|g_1\rangle$
$\|g_3\rangle = \sigma_2^z\|g_1\rangle$	$\|g_7\rangle = \sigma_2^z\sigma_2^x\|g_1\rangle$
$\|g_4\rangle = \sigma_2^z\sigma_1^z\|g_1\rangle$	$\|g_8\rangle = \sigma_2^z\sigma_1^z\sigma_2^x\|g_1\rangle$
Grupo 3	**Grupo 4**
$\|g_9\rangle = \sigma_1^x\|g_1\rangle$	$\|g_{13}\rangle = \sigma_2^x\sigma_1^x\|g_1\rangle$
$\|g_{10}\rangle = \sigma_1^z\sigma_1^x\|g_1\rangle$	$\|g_{14}\rangle = \sigma_1^z\sigma_2^x\sigma_1^x\|g_1\rangle$
$\|g_{11}\rangle = \sigma_2^z\sigma_1^x\|g_1\rangle$	$\|g_{15}\rangle = \sigma_2^z\sigma_2^x\sigma_1^x\|g_1\rangle$
$\|g_{12}\rangle = \sigma_2^z\sigma_1^z\sigma_1^x\|g_1\rangle$	$\|g_{16}\rangle = \sigma_2^z\sigma_1^z\sigma_2^x\sigma_1^x\|g_1\rangle$

Depois de escolher uma dessas 16 operações locais, Alice envia seus dois qbits para Bob. Com os quatro qbits, Bob realiza uma medida de Bell generalizada para determinar qual estado-G Alice lhe enviou. Assim, Bob lê a mensagem de 4 bits usando, por exemplo, a convenção (previamente discutida com Alice) exposta na Tabela 3.5.

As dificuldades técnicas para a realização desse protocolo são as mesmas apresentadas para o teletransporte de dois qbits: obtenção de fontes de estados-G, desenvolvimento de técnicas para a implementação das 16 operações locais e medidas generalizadas de Bell.

Para a codificação superdensa, também é interessante ver que o estado GHZ, $|GHZ\rangle = (1/\sqrt{2})(|0000\rangle + |1111\rangle)$, não pode ser usado para implementar o protocolo

Tabela 3.5: Temos aqui os 16 estados-G e suas codificações binárias, nas quais Alice e Bob concordam.

Estado	Convenção	Estado	Convenção
$\|g_1\rangle$	0000	$\|g_2\rangle$	0001
$\|g_3\rangle$	0010	$\|g_4\rangle$	0100
$\|g_5\rangle$	1000	$\|g_6\rangle$	0011
$\|g_7\rangle$	0110	$\|g_8\rangle$	1100
$\|g_9\rangle$	0101	$\|g_{10}\rangle$	1001
$\|g_{11}\rangle$	1010	$\|g_{12}\rangle$	0111
$\|g_{13}\rangle$	1011	$\|g_{14}\rangle$	1101
$\|g_{15}\rangle$	1110	$\|g_{16}\rangle$	1111

anterior se desejamos manter a mesma eficiência. Manipulando seus dois qbits, Alice pode produzir apenas os oito estados ortogonais abaixo:

$$|GHZ^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0000\rangle \pm |1111\rangle), \tag{3.169}$$

$$|G^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0100\rangle \pm |1011\rangle), \tag{3.170}$$

$$|H^{\pm}\rangle = \frac{1}{\sqrt{2}}(|1000\rangle \pm |0111\rangle), \tag{3.171}$$

$$|Z^{\pm}\rangle = \frac{1}{\sqrt{2}}(|1100\rangle \pm |0011\rangle). \tag{3.172}$$

Assim, usando um estado GHZ e manipulações em seus dois qbits apenas, Alice pode, no máximo, transmitir uma mensagem de 3 bits. Está é a justificativa de chamarmos os estados-G, algumas vezes, de estados de *máximo* emaranhamento, pois todos possuem $E_T = 1$ e são mais eficientes do que os estados GHZ para codificação superdensa e para teleportar dois qbits.

Este protocolo de codificação superdensa pode ser considerado ótimo. Por ótimo queremos dizer que sua capacidade de transmitir bits clássicos é igual ao limite de Holevo (*Holevo bound*) [21]. O limite de Holevo é a máxima capacidade de informação clássica que um sistema quântico de dimensão d pode transmitir: $H = \log_2 d$ bits. Como o estado $|g_j\rangle$ possui $d = 2^4$, $H = 4$ bits, exatamente o número de bits transmitidos pelo protocolo apresentado. Em geral, a capacidade de codificação superdensa χ, para um dado estado ρ^{AB} compartilhado entre A and B é dada por [21],

$$\chi(\rho^{AB}) = \log_2 d_A + S(\rho^B) - S(\rho^{AB}), \tag{3.173}$$

onde d_A é a dimensão do sistema de Alice, $\rho^B = Tr_A(\rho^{AB})$ é a matriz reduzida com relação ao subsistema A, ρ^{AB} é a matriz densidade do sistema global,

e $S(\sigma) = -Tr(\sigma \log_2 \sigma)$ é a entropia de von Neumann. Usando a Eq. (3.173) podemos novamente ver que o protocolo aqui apresentado atinge o limite de Holevo. Para $\rho^{AB} = |g_1\rangle\langle g_1|$ temos $d_A = 4$ e um cálculo rápido mostra que $S(\rho^B) = 2$ e $S(\rho^{AB}) = 0$. Por meio desses resultados, a Eq. (3.173) vale $\chi(|g_1\rangle) = 4$. Repetindo o mesmo cálculo para o estado GHZ obtemos $\chi(|GHZ\rangle) = 3$. Este último resultado nos diz que por mais engenhoso que possa ser um futuro protocolo de codificação superdensa usando os estados GHZ, ele nunca poderá ultrapassar a capacidade anteriormente calculada. Os estados-G, no entanto, saturam esta capacidade, atingindo o limite de Holevo.

Assim como generalizamos o protocolo de teletransporte de dois qbits para um número arbitrário de qbits, este protocolo pode, da mesma forma, ser generalizado.

(1) O estado de Bell generalizado $|g_1\rangle$ é escrito como $|s_0\rangle = (2^{-N/2}) \sum_{j=0}^{M} |x_j\rangle_A |x_j\rangle_B$, onde $M = 2^N - 1$ e x_j é a representação binária do número j. No protocolo de codificação superdensa de 4 bits, $x_0 = 00$, $x_1 = 01$, $x_2 = 10$, e $x_3 = 11$. Devemos acrescentar zeros a fim de deixar todos os x_j com a mesma quantidade de bits (N bits);

(2) A partir de $|s_0\rangle$ é possível obter todos os 2^{2N} estados de Bell generalizados agindo localmente nos primeiros N qbits, $|s_j\rangle = \bigotimes_{k=1}^{N} (\sigma_k^z)^{j_{2k-1}} (\sigma_k^x)^{j_{2k}} |s_0\rangle$. Agora j_k representa o k-ésimo bit (da direita para esquerda) do número $0 \leq j \leq 2^{2N} - 1$, o qual é escrito em notação binária e zeros são acrescentados quando necessário para que todos os j's tenham os mesmos números de bits ($2N$ bits). O subíndice k indica em qual qbit as matrizes de Pauli σ^x e σ^z devem atuar. Para o protocolo de 4 bits estas operações estão listadas na Tabela 3.4 e $|s_0\rangle = |g_1\rangle$, $|s_1\rangle = |g_2\rangle$, $|s_2\rangle = |g_9\rangle$, $|s_3\rangle = |g_{10}\rangle$, etc.

(3) Após implementar uma das 2^{2N} operações locais em seus qbits, Alice envia a Bob seus N qbits.

(4) Com o estado de $2N$ qbits, Bob faz uma medida de Bell generalizada para ler a mensagem de $2N$ bits.

3.10 O que são os estados-G

Agora vamos provar que o estado $|g_1\rangle$ é equivalente a um par de estados de Bell. Para evitar confusão, vamos reescrever o estado $|g_1\rangle$ especificando quais qbits pertencem a Alice e quais pertencem a Bob:

$$|g_1\rangle = \frac{1}{2}(|0_A 0_A 0_B 0_B\rangle + |0_A 1_A 0_B 1_B\rangle + |1_A 0_A 1_B 0_B\rangle + |1_A 1_A 1_B 1_B\rangle)\,. \qquad (3.174)$$

Trocando a ordem na qual escrevemos o segundo e terceiro qbits,

$$\begin{aligned} |g_1\rangle &= \frac{1}{2}(|0_A0_B0_A0_B\rangle+|0_A0_B1_A1_B\rangle+|1_A1_B0_A0_B\rangle+|1_A1_B1_A1_B\rangle) \\ &= \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)\frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle) \\ &= |\Phi^+\rangle_{AB}|\Phi^+\rangle_{AB}. \end{aligned} \tag{3.175}$$

Na verdade, repetindo o procedimento que nos levou a Eq. (3.175), todos os estados $|g_j\rangle$ podem ser escritos como um produto direto de dois estados de Bell. O resultado desses cálculos estão apresentados na Tabela 3.6.

Tabela 3.6: Aqui vemos os estados $|g_j\rangle$ e suas respectivas decomposições em dois estados de Bell.

Grupo 1	Grupo 2
$\|g_1\rangle = \|\Phi^+\rangle_{AB}\|\Phi^+\rangle_{AB}$	$\|g_5\rangle = \|\Phi^+\rangle_{AB}\|\Psi^+\rangle_{AB}$
$\|g_2\rangle = \|\Phi^-\rangle_{AB}\|\Phi^+\rangle_{AB}$	$\|g_6\rangle = \|\Phi^-\rangle_{AB}\|\Psi^+\rangle_{AB}$
$\|g_3\rangle = \|\Phi^+\rangle_{AB}\|\Phi^-\rangle_{AB}$	$\|g_7\rangle = \|\Phi^+\rangle_{AB}\|\Psi^-\rangle_{AB}$
$\|g_4\rangle = \|\Phi^-\rangle_{AB}\|\Phi^-\rangle_{AB}$	$\|g_8\rangle = \|\Phi^-\rangle_{AB}\|\Psi^-\rangle_{AB}$
Grupo 3	**Grupo 4**
$\|g_9\rangle = \|\Psi^+\rangle_{AB}\|\Phi^+\rangle_{AB}$	$\|g_{13}\rangle = \|\Psi^+\rangle_{AB}\|\Psi^+\rangle_{AB}$
$\|g_{10}\rangle = \|\Psi^-\rangle_{AB}\|\Phi^+\rangle_{AB}$	$\|g_{14}\rangle = \|\Psi^-\rangle_{AB}\|\Psi^+\rangle_{AB}$
$\|g_{11}\rangle = \|\Psi^+\rangle_{AB}\|\Phi^-\rangle_{AB}$	$\|g_{15}\rangle = \|\Psi^+\rangle_{AB}\|\Psi^-\rangle_{AB}$
$\|g_{12}\rangle = \|\Psi^-\rangle_{AB}\|\Phi^-\rangle_{AB}$	$\|g_{16}\rangle = \|\Psi^-\rangle_{AB}\|\Psi^-\rangle_{AB}$

Uma generalização da prova anterior mostra que o estado de $2N$ qbits $|s_0\rangle$, o qual é um canal quântico necessário para teleportar um estado arbitrário de N qbits [76], pode ser escrito como $|s_0\rangle = |\Phi^+\rangle_{AB}^{\otimes N}$. Este último resultado expressa a necessidade de N estados de Bell bipartites para teleportar um cadeia de N qbits. Veja Fig. 3.1.

Esta equivalência entre canais quânticos multipartites e canais EPR é um resultado interessante, para não dizer surpreendente. Primeiro, ela abre as portas para quantificarmos o emaranhamento de estados multipartites em termos dos estados de Bell para dois qbits. Tudo leva a crer que os estados de Bell são os canais quânticos elementares, a partir dos quais podemos representar todos os outros canais multipartites. Pelo menos para tarefas como codificação superdensa e teletransporte, mostramos que podemos entender canais multipartites dessa forma.

Segundo, é intrigante notar que para teleportar [76] um estado de dois qbits arbitrários,$|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ precisamos de dois estados de Bell e não 'verdadeiros' estados emaranhados multipartites como o estado $|GHZ\rangle = (1/\sqrt{2})(|0000\rangle + |1111\rangle)$. E mais intrigante ainda, um estado GHZ pode teleportar

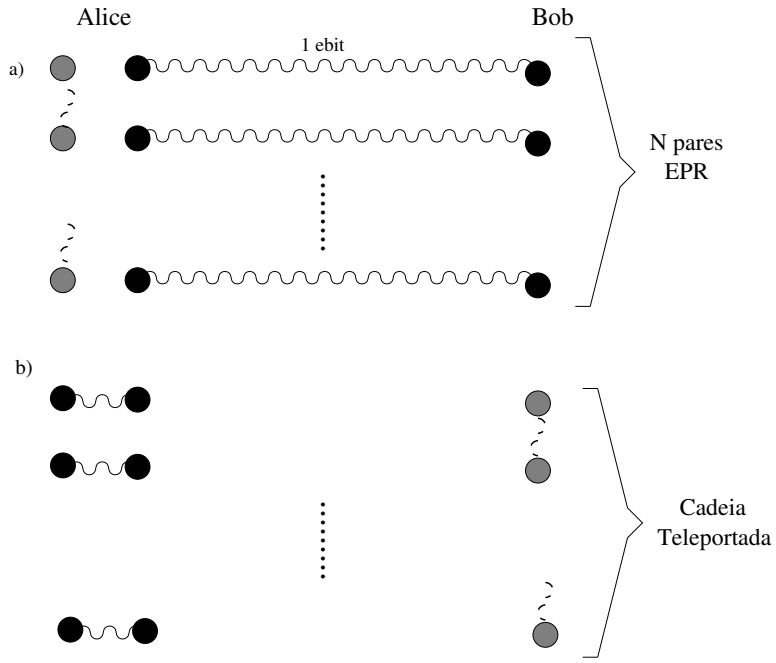


Figura 3.1: a) Situção inicial do protocolo. Temos N qbits a serem teleportados, onde todos podem estar emaranhados entre si ou não. Por isso a linha sinuosa-tracejada. b) Situação final do protocolo. Alice fez medidas de Bell em todos os pares de qbits que agora estão emaranhados e Bob já implementou as N operações unitárias em cada um de seus qbits.

apenas alguns estados de dois qbits mas nunca um estado arbitrário [76]. Extendendo esse raciocínio para muitos qbits, vemos que para teleportar uma cadeia de N constituintes precisamos 'apenas' de N pares de estados de Bell. Mesmo que todos os qbits da cadeia que queremos teleportar estejam emaranhados, podemos teleportá-la sem recorrer a nenhum canal quântico no qual tenhamos um estado globalmente emaranhado de N qbits. Basta 'paralelizar' N estados de Bell que obtemos o canal necessário para realizar essa tarefa.

Enfim, estes resultados mostram que temos muito para aprender sobre emaranhamento multipartite e que, talvez, explorando essa equivalência entre canais quânticos EPR e canais quânticos multipartites possamos avançar mais um pouco nesse fascinante assunto.

Parte II

Aplicações e Implicações

Capítulo 4

Aspectos do Princípio da Incerteza de Heisenberg

4.1 Introdução

Uma das mais importantes conseqüências da Mecânica Quântica (MQ) é um limite teórico imposto sobre a máxima precisão de medidas simultâneas em variáveis canonicamente conjugadas. Esta limitação, explicitamente apresentada por Werner Heisenberg [44], vai de encontro à idéia clássica de que podemos, pelo menos em princípio, reduzir as incertezas nas medidas *ad infinitum*. No mundo clássico, usando aparatos de medidas mais avançados, poderíamos reduzir tanto quanto desejássemos os erros nas medições de variáveis canonicamente conjugadas. Segundo a MQ, no entanto, existe uma lei fundamental na Natureza que nos impede de reduzir esses erros para além de um certo limiar.

Muitos experimentos checaram, usando uma grande variedade de pares de variáveis canonicamente conjugadas, a validade da Relação de Incerteza de Heisenberg (RIH). Ninguém nunca verificou uma violação dessa RI, expressa em forma de uma desigualdade que impõem limites inferiores ao produto das dispersões de pares de variáveis canônicas.

Contudo, recentemente, em medidas de coincidência de pares de partículas emaranhadas, Kim e Shih [56] sugeriram que poderíamos ter uma violação da RIH. A interpretação desse experimento é um tanto controversa. A Ref. [85] afirma que não há uma violação da RIH, mas nós achamos [70] que a RIH, pelo menos da forma como a conhecemos, não pode ser consistentemente aplicada para explicar os resultados experimentais em medidas de coincidência.

Neste capítulo derivamos uma RI válida em medidas de coincidência. Supomos que nosso sistema de N partículas idênticas e emaranhadas é descrito por um estado puro [70, 71]. Esta nova RI mostra as correlações quânticas entre as partículas que compõem o sistema e pode explicar o resultado experimental da Ref. [56], o qual foi

a maior motivação para a busca dessas RIs.

4.2 O Experimento de Kim e Shih

Inspirados num experimento imaginário (*Gedankenexperiment*) de Karl Popper [67], o qual pode ser visto como uma extensão dos argumentos de Einstein, Podolsky e Rosen [30], Kim e Shih realizaram o seguinte experimento [56].

Vários pares de fótons emaranhados *à la* EPR-Bohm são produzidos por Conversão Descendente Paramétrica Espontânea (*Spontaneous Parametric Down Conversion*). Para cada par, um fóton é enviado para Alice e o outro para Bob. Alice possui o detector D_1 e Bob o detector D_2. Veja Fig. 4.1.

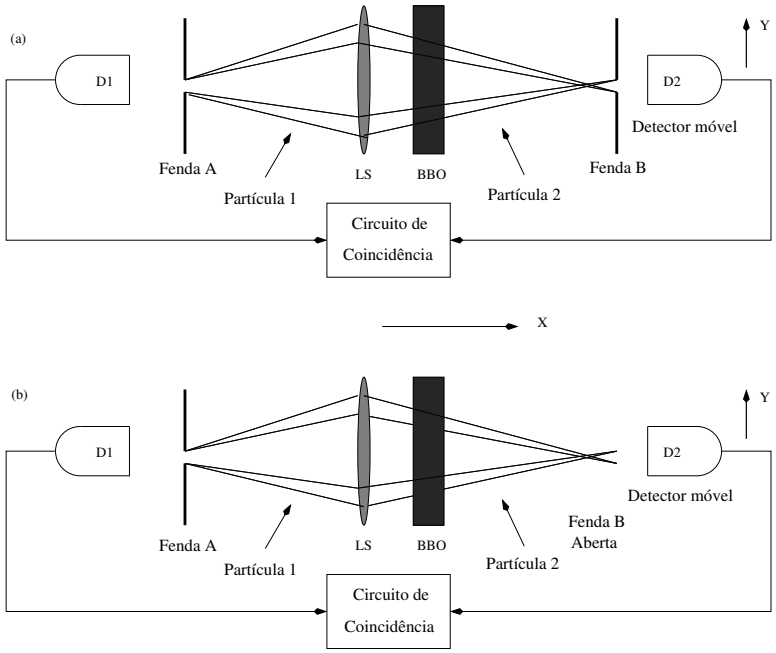


Figura 4.1: A parte (a) representa a montagem experimental onde ambas as fendas possuem a mesma largura. A parte (b) representa a configuração onde a fenda B é muito mais larga do que a fenda A. Um cristal de Borato de Bário Beta *(Beta Barium Borate)* recebe um feixe de laser e produz, via Conversão Descendente Paramétrica Espontânea, o par de fótons emaranhados. LS é a lente que produz a imagem fantasma *(ghost image)* [56] da fenda A e localiza o fóton 2 quando detectamos o fóton 1 na fenda A.

As medidas de Alice e Bob são condicionais no sentido de que a detecção do fóton 2, pelo detector D_2 que se move na direção y, é coincidente com a detecção em D_1 do fóton 1 após sua passagem pela fenda A. Kim e Shih realizam o experimento com duas montagens diferentes:

(a) Fenda A e fenda B possuem a mesma largura.

(b) Fenda B é muito mais larga do que a fenda A.

O primeiro caso não apresenta nenhuma surpresa pois ambas as partículas respeitam a RIH. A situação interessante aparece no caso (b). Para essa configuração os resultados experimentais nos dão $\Delta y_2 \Delta p_{y_2} < \hbar/2$, numa aparente violação da RIH.

4.3 Nova Relação de Incerteza

Para tentar explicar essa aparente violação da RIH, precisamos de uma nova RI que deixe explícito o fato de que temos um estado emaranhado e de que lidamos com partículas idênticas. Antes de passar à dedução da Relação de Incerteza Generalizada (RIG), precisamos definir formalmente o que entendemos por partículas idênticas e recordar a definição de emaranhamento para estado puro.

4.3.1 Partículas Idênticas

Sabemos que quando estudamos um sistema de N partículas idênticas devemos simetrizar o estado descrevendo esse conjunto de partículas, se lidamos com bósons, ou anti-simetrizar esse estado, caso lidamos com férmions. Devemos, também, usar *observáveis físicos* [25, 60]. Estes são definidos como sendo observáveis que comutam com todos os operadores de permutação de um conjunto de N partículas. Matematicamente, um observável físico deve satisfazer a seguinte relação de comutação:

$$[\mathcal{O}, P] = 0, \tag{4.1}$$

onde $\mathcal{O}$ é um observável físico e P é qualquer operador de permutação do sistema.

4.3.2 Estados Puros Emaranhados

O espaço de Hilbert $\mathcal{H}$ de um sistema de N partículas é o produto direto dos espaços de Hilbert $\mathcal{H}_i$ associados a cada partícula,

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_N = \bigotimes_{i=1}^{N} \mathcal{H}_i. \tag{4.2}$$

O estado mais geral $|\Psi\rangle$ descrevendo um sistema puro é dado por [25, 51]:

$$|\Psi\rangle = \sum_{i_1,\ldots,i_N} c_{i_1 \ldots i_N} |u_{i_1}\rangle_1 \otimes \ldots \otimes |u_{i_N}\rangle_N, \tag{4.3}$$

onde $c_{i_1 \ldots i_n}$ é o coeficiente de expansão do estado $|\Psi\rangle$ na base $\{|u_{i_1}\rangle_1 ; \ldots ; |u_{i_N}\rangle_N\}$. Aqui, um estado $|u_{i_n}\rangle_n$ indica que temos a partícula $n \leq N$ no estado $|u_{i_n}\rangle$.

Um sistema de N partículas é considerado emaranhado se não podemos escrever o estado $|\Psi\rangle$ como um produto de N estados, cada um pertecendo ao espaço de

Hilbert de uma das partículas que compõem o sistema. Em outras palavras, isso significa que temos um estado não separável,

$$|\Psi\rangle \neq |\psi_1\rangle \otimes \ldots \otimes |\psi_N\rangle \,. \tag{4.4}$$

Isso mostra que a Eq. (4.3) não pode ser escrita como:

$$|\Psi\rangle \neq \sum_{i_1} c_{i_1} |u_{i_1}\rangle_1 \otimes \ldots \otimes \sum_{i_N} c_{i_N} |u_{i_N}\rangle_N, \tag{4.5}$$

onde $c_{i_1}, \ldots, c_{i_N}$ são os coeficientes de expansão do estado não emaranhado $|\psi_1\rangle \otimes \ldots \otimes |\psi_N\rangle$ na base $\{|u_{i_1}\rangle_1 ; \ldots ; |u_{i_N}\rangle_N\}$.

4.3.3 Caso de N Partículas

Sabemos que as dispersões de quaisquer grandezas físicas representadas por dois operadores, A e B, satisfazem a desigualdade,

$$(\Delta A)^2 (\Delta B)^2 \geq \frac{|\,\langle [A,B] \rangle\,|^2}{4}, \tag{4.6}$$

onde ΔA e ΔB são os desvios quadrático médio dos observáveis A e B, calculados para um determinado estado quântico. Exigimos, agora, que para obter uma RI para um conjunto de N partículas idênticas e emaranhadas, devemos satisfazer as duas condições abaixo,

1. Usar apenas observáveis físicos.

2. Usar estados não separáveis.

Por meio destas duas hipóteses, as quais representam, da maneira mais simples, o fato de lidarmos com um sistema de N partículas idênticas e emaranhadas, obtemos uma RI mais geral do que a de Heisenberg. Na verdade, a RIH é o caso mais simples da RIG. Se temos apenas uma partícula ($N = 1$), recuperamos a RIH.

Comecemos a dedução da RIG definindo os observáveis físicos usados na Eq. (4.6). Atuando no espaço de estados $\mathcal{H}_i$ da partícula i encontramos os observáveis posição e momento, Q_i e P_i, respectivamente. Quando estudamos um sistema de N partículas, usamos os observáveis definidos como,[1]

$$Q_i = \mathcal{I}_1 \otimes \ldots \otimes Q_i \otimes \ldots \otimes \mathcal{I}_N, \tag{4.7}$$

$$P_i = \mathcal{I}_1 \otimes \ldots \otimes P_i \otimes \ldots \otimes \mathcal{I}_N, \tag{4.8}$$

onde $\mathcal{I}_i$ é o operador identidade que atua na partícula i. Facilmente vemos que estes operadores não comutam com alguns dos operadores de permutação definidos para

[1] De agora em diante, nos restringimos, por motivos de simplicidade, a sistemas unidimensionais.

um sistema de N constituintes. Precisamos, pois, criar um par de observáveis físicos para usarmos na dedução da RIG. O par mais simples de observável físico é,

$$Q = Q_1 + \ldots + Q_N, \tag{4.9}$$

$$P = P_1 + \ldots + P_N, \tag{4.10}$$

onde Q_i e P_i são dados pelas Eqs. (4.7) e (4.8). Assim, a Eq. (4.6) pode ser escrita como,

$$(\Delta Q)^2(\Delta P)^2 \geq \frac{|\langle [Q,P] \rangle|^2}{4}. \tag{4.11}$$

Mas o comutador de Q e P é,

$$[Q,P] = [Q_1,P_1] + \ldots + [Q_N,P_N] = iN\hbar. \tag{4.12}$$

Então, a Eq. (4.11) torna-se

$$(\Delta Q)^2(\Delta P)^2 \ \geq \ \frac{N^2\hbar^2}{4}. \tag{4.13}$$

Se definimos a Função Quântica de Covariância (FQC) para a posição e para o momento como [91],

$$C_Q(i,j) = \langle Q_i Q_j \rangle - \langle Q_i \rangle \langle Q_j \rangle, \tag{4.14}$$

$$C_P(i,j) = \langle P_i P_j \rangle - \langle P_i \rangle \langle P_j \rangle, \tag{4.15}$$

podemos reescrever a Eq. (4.13) da seguinte forma:

$$\sum_{i,j=1}^{N} C_Q(i,j) \sum_{i,j=1}^{N} C_P(i,j) \ \geq \ \frac{N^2\hbar^2}{4}. \tag{4.16}$$

Mas sabemos que $C_Q(i,i) = (\Delta Q_i)^2$ e que $C_P(i,i) = (\Delta P_i)^2$. Então, a Eq. (4.16) se torna:

$$\left(\sum_{i=1}^{N} (\Delta Q_i)^2 + \sum_{i \neq j=1}^{N} C_Q(i,j) \right) \times \left(\sum_{i=1}^{N} (\Delta P_i)^2 + \sum_{i \neq j=1}^{N} C_P(i,j) \right) \ \geq \ \frac{N^2\hbar^2}{4}. \tag{4.17}$$

Esta é a RIG que devemos usar quando trabalhamos com um sistema de N partículas idênticas e emaranhadas. Na expressão acima observamos dois termos para cada observável físico. Por exemplo, para o observável físico Q, $\sum_{i=1}^{N} (\Delta Q_i)^2$ é a soma dos quadrados das dispersões da posição para cada constituinte do sistema. O outro termo, $\sum_{i \neq j=1}^{N} C_Q(i,j)$, mostra as correlações quânticas entre todas as N partículas do sistema. Se pudéssemos fatorar o estado que descreve as N partículas, ele seria zero. Vale a pena notar que A. C. de la Torre, P. Catuogno e S. Ferrando [91] provaram que para estados puros as FQCs que envolvam operadores de mais de uma

partícula são nulas[2] se, e somente se, o sistema é separável. E, como emaranhamento para sistemas puros implica inseparabilidade, pelo menos uma dessas FQCs não se anula na Eq. (4.17) e de fato temos uma RI diferente daquela obtida para uma única partícula. Lembramos, porém, que se lidamos com estados mistos, podemos encontrar situações nas quais temos estados não emaranhados possuindo pelo menos um dessas FQCs diferente de zero.

4.3.4 Caso de Duas Partículas

Vamos, agora, nos restringir ao caso no qual temos apenas duas partículas. Assim, a Eq. (4.17) pode ser reescrita como:

$$\left[\frac{(\Delta Q_1)^2}{2}+\frac{(\Delta Q_2)^2}{2}+\left(\langle Q_1Q_2\rangle-\langle Q_1\rangle\langle Q_2\rangle\right)\right] \times\left[\frac{(\Delta P_1)^2}{2}+\frac{(\Delta P_2)^2}{2}+\left(\langle P_1P_2\rangle-\langle P_1\rangle\langle P_2\rangle\right)\right]\geq\frac{\hbar^2}{4}. \tag{4.18}$$

Usando a desigualdade de Schwarz,

$$\langle\varphi_1\mid\varphi_1\rangle\langle\varphi_2\mid\varphi_2\rangle\ \geq\ \langle\varphi_1\mid\varphi_2\rangle\langle\varphi_2\mid\varphi_1\rangle\,, \tag{4.19}$$

onde $|\varphi_1\rangle$ e $|\varphi_2\rangle$ são dois estados arbitrários, podemos simplificar mais a Eq. (4.18). Como a Eq. (4.19) é válida para qualquer estado, então, aplicando-a para os dois estados abaixo,

$$|\varphi_1\rangle\ =\ (Q_1\pm Q_2)\,|\psi\rangle\,, \tag{4.20}$$

$$|\varphi_2\rangle\ =\ |\psi\rangle\,, \tag{4.21}$$

onde $|\psi\rangle$ é o estado normalizado descrevendo o sistema de duas partículas em questão, obtemos:

$$\mid\langle Q_1Q_2\rangle-\langle Q_1\rangle\langle Q_2\rangle\mid\leq\ \frac{(\Delta Q_1)^2}{2}+\frac{(\Delta Q_2)^2}{2}. \tag{4.22}$$

O mesmo raciocínio aplicado ao observável momento fornece:

$$\mid\langle P_1P_2\rangle-\langle P_1\rangle\langle P_2\rangle\mid\leq\ \frac{(\Delta P_1)^2}{2}+\frac{(\Delta P_2)^2}{2}. \tag{4.23}$$

Analisando as Eqs. (4.22) e (4.23) vemos que o valor absoluto da FQC para a posição e para o momento é sempre menor do que a média das dispersões da posição e do momento das duas partículas. Logo, temos um limitante superior para a FQC. Substitutindo esse limite superior na Eq. (4.18) obtemos:

$$\left[(\Delta Q_1)^2+(\Delta Q_2)^2\right]\times\left[(\Delta P_1)^2+(\Delta P_2)^2\right]\geq\frac{\hbar^2}{4}. \tag{4.24}$$

[2]Supondo $i\neq j$ na definição da FQC.

Esta última expressão é a RI que devemos usar para um par de partículas idênticas e emaranhadas.

Um caso interessante surge quando produzimos um par de partículas idênticas e emaranhadas com mesma dispersão na posição e no momento. Por meio de *medidas coincidentes*, nas quais a detecção da partícula 1 é condicionada à detecção da partícula 2 [56, 70], podemos experimentalmente criar este cenário. Supondo a igualdade das dispersões, $\Delta Q_1 = \Delta Q_2$ e $\Delta P_1 = \Delta P_2$, a Eq. (4.24) torna-se:

$$\Delta Q_i \Delta P_i \geq \frac{\hbar}{4}, \tag{4.25}$$

onde $i = 1, 2$.

Aqui vemos que a RIG permite que o produto das dispersões seja duas vezes menor do que o permitido pela RIH. E claro, se esquecemos uma das partículas e medimos apenas ΔQ_i e ΔP_i para a outra, a RIH é satisfeita. Apenas quando temos partículas idênticas, emaranhamento e medidas coincidentes a Eq. (4.25) é válida.

4.3.5 Caso de Três Partículas

Para três partículas, a Eq. (4.17) pode ser escrita como:

$$\left(\sum_{i=1}^{3}(\Delta Q_i)^2 + \sum_{i\neq j=1}^{3} C_Q(i,j)\right) \times \left(\sum_{i=1}^{3}(\Delta P_i)^2 + \sum_{i\neq j=1}^{3} C_P(i,j)\right) \geq \frac{9\hbar^2}{4}. \tag{4.26}$$

Novamente podemos aplicar a desigualdade de Schwarz visando simplicar a expressão anterior. Substituimos, agora, os seguintes dois estados na Eq. (4.19):

$$|\varphi_1\rangle = (a_1 Q_1 + a_2 Q_2 + a_3 Q_3)\,|\psi\rangle\,, \tag{4.27}$$

$$|\varphi_2\rangle = |\psi\rangle\,, \tag{4.28}$$

onde $a_i = \pm 1, i = 1, 2, 3$. Assim, a desigualdade de Schwarz torna-se:

$$\left\langle (a_1 Q_1 + a_2 Q_2 + a_3 Q_3)^2 \right\rangle \geq \left\langle (a_1 Q_1 + a_2 Q_2 + a_3 Q_3) \right\rangle^2 \tag{4.29}$$

Manipulando a Eq. (4.29) e usando que $a_i^2 = 1$ obtemos:

$$\sum_{i=1}^{3}\left\langle Q_i^2\right\rangle + \sum_{i\neq j=1}^{3} a_i a_j \left\langle Q_i Q_j\right\rangle \geq \sum_{i=1}^{3}\left\langle Q_i\right\rangle^2 + \sum_{i\neq j=1}^{3} a_i a_j \left\langle Q_i\right\rangle\left\langle Q_j\right\rangle. \tag{4.30}$$

Mas $(\Delta Q_i)^2 = \left\langle Q_i^2\right\rangle - \left\langle Q_i\right\rangle^2$, fazendo com que a Eq. (4.30) se reduza a:

$$\sum_{i=1}^{3}(\Delta Q_i)^2 \geq -\sum_{i\neq j=1}^{3} a_i a_j C_Q(i,j). \tag{4.31}$$

Para $a_1 = 1$ e $a_2 = a_3 = -1$, a Eq. (4.31) é dada por,

$$\sum_{i=1}^{3} (\Delta Q_i)^2 \;\geq\; 2\left(C_Q(1,2) + C_Q(1,3) - C_Q(2,3)\right). \tag{4.32}$$

Para $a_2 = 1$ e $a_1 = a_3 = -1$, a Eq. (4.31) vale,

$$\sum_{i=1}^{3} (\Delta Q_i)^2 \;\geq\; 2\left(C_Q(1,2) - C_Q(1,3) + C_Q(2,3)\right). \tag{4.33}$$

Para $a_3 = 1$ e $a_1 = a_2 = -1$ temos,

$$\sum_{i=1}^{3} (\Delta Q_i)^2 \;\geq\; 2\left(-C_Q(1,2) + C_Q(1,3) + C_Q(2,3)\right). \tag{4.34}$$

Somando as Eqs. (4.32), (4.33) e (4.34) obtemos,

$$2\left(C_Q(1,2) + C_Q(1,3) + C_Q(2,3)\right) \;\leq\; 3\sum_{i=1}^{3} (\Delta Q_i)^2. \tag{4.35}$$

Agora, para $a_1 = a_2 = a_3 = 1$, a Eq. (4.31) torna-se,

$$2\left(C_Q(1,2) + C_Q(1,3) + C_Q(2,3)\right) \;\geq\; -\sum_{i=1}^{3} (\Delta Q_i)^2. \tag{4.36}$$

Combinando as Eqs. (4.35) e (4.36) chegamos à seguinte expressão:

$$-\sum_{i=1}^{3} (\Delta Q_i)^2 \;\leq\; \sum_{i\neq j=1}^{3} C_Q(i,j) \;\leq\; 3\sum_{i=1}^{3} (\Delta Q_i)^2. \tag{4.37}$$

Um procedimento similar nos leva a um resultado equivalente para o momento:

$$-\sum_{i=1}^{3} (\Delta P_i)^2 \;\leq\; \sum_{i\neq j=1}^{3} C_P(i,j) \;\leq\; 3\sum_{i=1}^{3} (\Delta P_i)^2. \tag{4.38}$$

Substituindo as Eqs. (4.37) e (4.38) na Eq. (4.26) obtemos,

$$\left(\sum_{i=1}^{3} (\Delta Q_i)^2\right)\left(\sum_{i=1}^{3} (\Delta P_i)^2\right) \;\geq\; \frac{9\hbar^2}{64}. \tag{4.39}$$

Esta é a RIG que devemos usar quando estudamos três partículas idênticas e emaranhadas. Novamente obtemos uma situação interessante quando todas as três partículas são preparadas com as mesmas dispersões na posição e no momento. Isto é,

$$\Delta Q_1 = \Delta Q_2 = \Delta Q_3, \tag{4.40}$$

$$\Delta P_1 = \Delta P_2 = \Delta P_3, \tag{4.41}$$

Assim, a Eq. (4.39) vale,

$$\Delta Q_i \Delta P_i \geq \frac{\hbar}{8}, \tag{4.42}$$

onde $i = 1, 2, 3$.

Agora temos um limite inferior para o produto das dispersões quatro vezes menor do que o fornecido pela RIH. As condições dadas pelas Eqs (4.40) e (4.41) podem ser alcançadas por meio de medidas tricoincidentes feitas em sistemas tripartites emaranhados de partículas idênticas. Se ignoramos duas partículas e nos concentramos em apenas uma, a RIH continua válida e a Eq. (4.42) não pode mais ser aplicada.

4.4 Discussão

Os resultados acima não devem ser considerados uma violação do princípio de incerteza de Heisenberg. Continuamos não podendo medir simultaneamente a posição e o momento (ou qualquer par de observáveis que não comutam entre si) de uma partícula. O que de fato mostramos foi que, se preparamos apropriadamente um sistema de partículas idênticas e usamos circuitos de coincidência para detectar todos os seus constituintes, podemos obter $\Delta Q_1 \Delta P_1 < \frac{\hbar}{2}$. Em nenhum momento de nossa dedução usamos hipóteses alheias à MQ padrão.

Em outras palavras, a MQ não proíbe que $\Delta Q_1 \Delta P_1 < \frac{\hbar}{2}$ para os casos nos quais lidamos com medidas coincidentes em partículas idênticas e emaranhadas. Todas as outras deduções anteriores de relações de incerteza foram feitas considerando-se apenas uma partícula isolada. Aqui, reforçamos que nem sempre resultados válidos para uma partícula isolada podem ser diretamente generalizados para duas ou mais partículas emaranhadas. Ou melhor, nem sempre o que é válido para uma partícula pode ser trivialmente extendido para sistemas com várias partículas submetidas a determinadas condições experimentais.

Para finalizar, vale a pena dizer que existe um resultado experimental confirmando a possibilidade de termos o produto das dispersões da posição e do momento menor do que o limite imposto pela RIH. Este resultado experimental [56] foi a maior motivação para alcançarmos os resultados apresentados neste capítulo: Queríamos encontrar uma explicação teórica para os resultados da Ref. [56] invocando apenas o fato de o experimento se utilizar de medidas coincidentes e de pares de fótons idênticos e emaranhados.

Capítulo 5

Caos e Emaranhamento

5.1 Introdução

Nos capítulos anteriores enfatizamos aspectos bem gerais no estudo do emaranhamento quântico. Foi dada maior atenção ao entendimento formal do que seria um estado emaranhado, tanto qualitativa como quantitativamente. A partir deste capítulo passamos a abordar problemas mais práticos, i. e., problemas que serão enfrentados na construção de um possível computador quântico.

Um dos passos cruciais na construção de um computador quântico se dá na escolha de qual sistema físico será usado na sua confecção. Existem inúmeras propostas já apresentadas, onde podemos destacar implementações via ressonância magnética nuclear (RMN), íons aprisionados e cavidades quânticas. Mas seria interessante estudar as possibilidades de construção de um computador quântico usando-se dispositivos em estado sólido. Melhor ainda seria a construção de um computador quântico usando-se dispositivos semicondutores já usados nos computadores atuais, haja vista o enorme domínio técnico que alcançamos na manipulação de dispositivos baseados no silício.

Neste capítulo estudamos a Hamiltoniana de Heisenberg, a qual modela a interação entre os spins de alguns sólidos [27, 28, 81] e que pode vir a ser uma possível implementação de um computador quântico.

Investigamos como defeitos numa cadeia unidimensional afeta o emaranhamento de um sistema descrito pelo modelo de Heisenberg bem como a relação entre emaranhamento, caos e localização [78]. No capítulo seguinte estudamos um sistema de dois qbits descritos pelo modelo de Heisenberg, no qual os qbits estão em equilíbrio térmico com um resrvatório a temperatura T [74]. O entendimento de como o emaranhamento se comporta a temperaturas finitas é extremamente importante pois nos permite estimar até que temperatura nosso processador quântico continua funcionando (emaranhado).

5.2 Caos, Localização e Emaranhamento

Como o emaranhamento de pares de qbits está relacionado com caos quântico e localização? Para responder essa questão parcialmente precisamos de um modelo. Um modelo de interesse prático consiste de uma cadeia unidimensional de spins 1/2, onde um determinado spin interage apenas com seus vizinhos mais próximos. Cada spin na cadeia corresponde a um qbit e as interações entre os spins podem ser usadas para implementar portas lógicas de dois qbits, ou seja, por meio dessas interações podemos construir um computador quântico elementar.

Neste sistema chamamos de defeito o sítio (local onde se encontra o qbit) cujo espaçamento de nível energético (nível de Zeeman) difere dos espaçamentos de nível energético dos outros sítios. Isso é alcançado aplicando-se um campo magnético externo na direção z nesse sítio diferente de todos os campos aplicados nos outros sítios. Um sistema desordenado é caracterizado pela presença de um ou mais defeitos.

A cadeia de spin aqui utilizada é perfeita para se analisar a relação entre emaranhamento, caos e localização, pois ela possui distintas regiões de interesse [79]. Podemos, pois, acompanhar o comportamento do emaranhamento quando transitamos das regiões caóticas para as não caóticas.

5.3 O Modelo de Heisenberg

A Hamiltoniana que descreve esse sistema de spins é

$$H = \sum_{n=1}^{L} \frac{h_n}{2}\sigma_n^z + \sum_{n=1}^{L-1} \frac{J_Z}{4}\sigma_n^z\sigma_{n+1}^z + \sum_{n=1}^{L-1} \frac{J_{XY}}{4}(\sigma_n^x\sigma_{n+1}^x + \sigma_n^y\sigma_{n+1}^y). \qquad (5.1)$$

Consideramos apenas interações de primeiros vizinhos, $\hbar = 1$, e σ^x, σ^y, e σ^z são as matrizes de Pauli. Cada sítio n está sujeito a um campo magnético externo na direção z, produzindo uma separação de h_n nos níveis energéticos do qbit n. Existem L sítios e lidamos com uma cadeia aberta. O sistema é isotrópico (anisotrópico) quando a constante de acoplamento J_Z das interações de Ising $\sigma_n^z\sigma_{n+1}^z$ for igual à (diferente da) constante de acoplamento J_{XY} da interação tipo XY: $\sigma_n^x\sigma_{n+1}^x + \sigma_n^y\sigma_{n+1}^y$. Este último termo é responsável por delocalizar o sistema, uma vez que ele propaga as excitações pela cadeia. Ele também é conhecido como termo de *hopping*.

5.4 Caos Quântico

Sabe-se que a distribuição dos espaçamentos dos níveis de energia de um sistema integrável é Poissoniana, $P_P(s) = \exp(-s)$, e a de um sistema caótico obedece a uma distribuição de Wigner-Dyson $P_{WD}(s) = (\pi s/2)\exp(-\pi s^2/4)$ [43]. $P(s)$ é a probabilidade de encontrarmos a diferença de energia entre dois níveis como sendo

ds. Supõe-se que $\int P(s)\mathrm{d}s = 1$ (normalização) e que $\langle s\rangle = \int sP(s)\mathrm{d}s = 1$ (média igual a um). Essa vai ser a definição de caos quântico adotada aqui.

Na ausência de defeitos, i. e., quando temos uma cadeia ideal, o sistema é integrável, possui espaçamento de níveis Poissoniano e podemos encontrar expressões analíticas para seus autovalores e autovetores usando-se o ansatz de Bethe [1, 16, 55, 101]. A partir do momento em que ligamos campos magnéticos aleatórios nos vários sítios da cadeia e aumentamos progressivamente suas intensidades, o sistema transita da região de integrabilidade para a de caoticidade, onde obtemos uma distribuição de Wigner-Dyson para os espaçamentos de níveis de energia. Nesta região, não há método analítico que nos permita encontrar os autovalores e autovetores do sistema. Aumentando-se ainda mais a intensidade do campo magnético, a localização torna-se relevante e obtemos de novo uma distribuição de Poisson.

5.5 Localização

Para quantificar a localização/delocalização usamos uma grandeza conhecida como número de componentes principais (*number of principal components*): N_{pc}. Escrevendo-se os autovetores $|\psi_j\rangle$ da Hamiltoniana acima como superposições dos registros quânticos $|\phi_i\rangle$, i.e. $|\psi_j\rangle = \sum_{i=1,N} a_i^j |\phi_i\rangle$, onde N é o número total de autovetores, o N_{pc} para o autovetor j é definido como [103],

$$N_{pc}^j = \frac{1}{\sum_{i=1}^{N} \left|a_i^j\right|^4}. \tag{5.2}$$

Um registro quântico $|\phi_i\rangle = |\alpha_1, ..., \alpha_L\rangle$ é um estado no qual $\alpha_k = 0, 1$ indica um spin para baixo ou para cima,[1] respectivamente, e L é o número total de sítios. Um sistema delocalizado possui alto N_{pc}, enquanto um sistema fortemente localizado possui N_{pc} muito perto de 1.

5.6 Medida de Emaranhamento Utilizada

Para se estudar quantitativamente o emaranhamento entre pares de qbits vamos usar a concorrência C [99], cuja interpretação física e relevância na quantificação do emaranhamento bipartite foram discutidas no Cap. 3. Recordando, a concorrência é dada por

$$C_{12} = \max\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4, 0\}, \tag{5.3}$$

[1] Apenas neste capítulo usamos a notação tradicional, onde $|0\rangle = (0, 1)^T$ representa o estado fundamental e $|1\rangle = (1, 0)^T$ o estado excitado. Para todos os outros capítulos, conforme convencionado no ínicio da tese, usamos a notação da comunidade de teoria quântica de informação, $|0\rangle = (1, 0)^T$ e $|1\rangle = (0, 1)^T$, onde T é a operação de transposição.

onde $\lambda_1, \lambda_2, \lambda_3$, e λ_4 são as raízes quadradas dos autovalores, em ordem decrescente, da matriz $R = \rho_{12}\tilde{\rho}_{12}$, ρ_{12} é a matriz densidade que descreve os dois qbits de interesse na cadeia de spins e $\tilde{\rho}_{12}$ é

$$\tilde{\rho}_{12} = (\sigma_y \otimes \sigma_y)\, \rho_{12}^{*}\, (\sigma_y \otimes \sigma_y)\,. \tag{5.4}$$

O símbolo ρ^* representa o complexo conjugado da matrix ρ quando escrita na base $\{|11\rangle, |10\rangle, |01\rangle, |00\rangle\}$.

5.7 Resultados Analíticos para Dois Qbits

Para uma cadeia isotrópica de dois sítios a Hamiltoniana (5.1) pode ser escrita como

$$H = \frac{1}{2}\left(h_1\sigma_1^z + h_2\sigma_2^z\right) + \frac{J}{4}\left(\sigma_1^z\sigma_2^z + \sigma_1^y\sigma_2^y + \sigma_1^x\sigma_2^x\right). \tag{5.5}$$

Uma característica interessante desse sistema isotrópico é que $[H, \sigma_1^z + \sigma_2^z] = 0$, i. e., o momento angular total na direção z é conservado. Isso nos diz que estados com números diferentes de excitações não se acoplam. Isso fica evidente se olharmos para a representação matricial de H:

$$H = \begin{pmatrix} \frac{\Sigma}{2} + \frac{J}{4} & 0 & 0 & 0 \\ 0 & \frac{\Delta}{2} - \frac{J}{4} & \frac{J}{2} & 0 \\ 0 & \frac{J}{2} & -\frac{\Delta}{2} - \frac{J}{4} & 0 \\ 0 & 0 & 0 & -\frac{\Sigma}{2} + \frac{J}{4} \end{pmatrix}, \tag{5.6}$$

onde $\Sigma = h_1 + h_2$ e $\Delta = h_1 - h_2$. A Hamiltoniana acima é diagonal por blocos. Assim $|11\rangle$ e $|00\rangle$ são autovetores não emaranhados de H. Como estamos interessados no emaranhamento, restringimo-nos aos outros dois autovetores, os quais são obtidos diagonalizando-se a matriz bloco 2×2 acima. Estes autovetores com seus respectivos autovalores são:

$$|E_\pm\rangle = \frac{J\,|10\rangle - \left(\Delta \mp \sqrt{J^2 + \Delta^2}\right)|01\rangle}{\sqrt{2\left(J^2 + \Delta^2\right) \mp 2\Delta\sqrt{J^2 + \Delta^2}}}, \tag{5.7}$$

$$E_\pm = -\frac{J}{4} \pm \frac{\sqrt{J^2 + \Delta^2}}{2}. \tag{5.8}$$

A concorrência dos autovetores $|E_\pm\rangle$ é

$$C_\pm = \frac{1}{\sqrt{1 + \Delta^2/J^2}}. \tag{5.9}$$

A Eq. (5.9) claramente mostra que $C_\pm$ é função decrescente de Δ e crescente da constante de acoplamento J. Quando $\Delta = 0$ (qbits com mesmo espaçamento energético)

obtemos estados de máximo emaranhamento independentemente se estamos no regime de acoplamento fraco ou forte. Para quaisquer outros valores de Δ não alcançamos mais estados de máximo emaranhamento, mostrando que o aparecimento de um defeito ($h_1 \neq h_2$) reduz a quantidade de emaranhamento. Mas mesmo se $\Delta \neq 0$, tomando $J \gg \Delta$ podemos obter altos valores para a concorrência. Ou seja, no regime de acoplamento forte podemos ter alto teor de emaranhamento.

Aplicando a Eq. (5.2) aos autovetores $|E_\pm\rangle$ obtemos a seguinte expressão para o N_{pc}:

$$N_{pc}^{\pm} = \frac{1}{1 - C_{\pm}^2/2}. \tag{5.10}$$

A Eq. (5.10) mostra que o N_{pc} para estes estados é uma função crescente da concorrência, implicando, pelo menos para este caso simples de dois qbits, que delocalização é favorável ao emaranhamento. Quando $C_\pm = 1$ (máximo emaranhamento), $N_{pc}^{\pm} = 2$ e quando $C_\pm = 0$ (sem emaranhamento) temos $N_{pc}^{\pm} = 1$ (sistema altamente localizado). Entretanto, não devemos generalizar essa relação entre delocalização e emaranhamento, pois nem sempre ela é válida. Isto ficará mais claro na próxima seção, ao lidarmos com cadeias maiores. No entanto, vale a pena observar o seguinte exemplo. O estado $|\psi\rangle = \sqrt{1/4}\,(|11\rangle + |10\rangle + |01\rangle + |00\rangle)$, é altamente delocalizado ($N_{pc} = 4$) mas separável ($C_\psi = 0$), retratando que nem sempre delocalização implica emaranhamento.

5.8 Resultados Numéricos para L Qbits

5.8.1 Dois Defeitos

Motivados pela seção anterior, vamos checar se dois qbits com os mesmos espaçamentos de níves energéticos, mas agora numa cadeia com várias excitações, i. e. vários qbits no estado $|1\rangle$, estão fortemente emaranhados [78]. Supomos que esses dois qbits possuem níveis de espaçamento $h + d$, enquanto todos os outros qbits da cadeia possem níveis de espaçamento h.

Desligando a interação de Ising, i.e., se $J_Z = 0$ na Eq. (5.1) e se $d \gg J_{XY}$, os dois qbits estão, de fato, maximamente emaranhados (exceto se um dos qbits está na borda da cadeia, onde efeitos de borda diminuem o emaranhamento). Podemos ver isso na parte superior esquerda da Fig. 5.1, onde círculos indicam que os dois qbits escolhidos são os primeiros vizinhos $(n, n+1)$, quadrados os segundos vizinhos $(n, n+2)$ e triângulos os terceiros vizinhos $(n, n+3)$. Obtemos a concorrência traçando sobre todos os qbits que não são de interesse e, a partir da matriz reduzida dos dois qbits, calculando C conforme explicado anteriormente. Na Fig. 5.1 mostramos a concorrência máxima dentre todas as 924 concorrências dos autovetores de uma cadeia composta por 12 qbits e 6 excitações. Notamos que quando $J_Z = 0$, mesmo

com muitas excitações, a situação se assemelha ao caso de uma excitação [80], onde apenas o termo de *hopping* está presente.

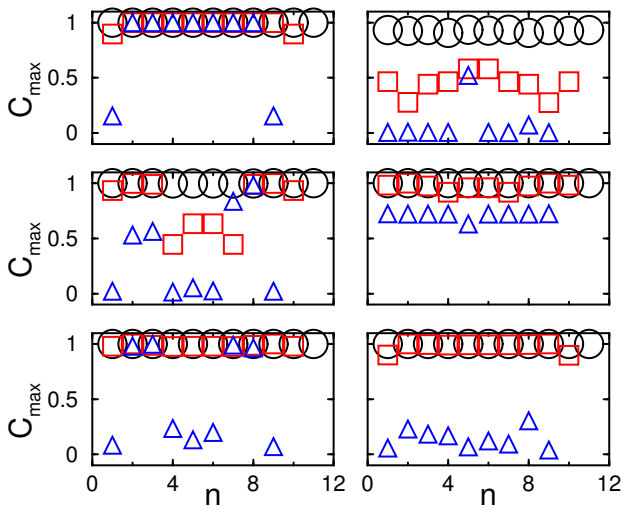


Figura 5.1: Aqui mostramos a máxima concorrência para vários pares de qbits que possuem o mesmo espaçamento de nível energético. Círculos indicam os pares de primeiros vizinhos $(n, n+1)$, quadrados os pares de segundos vizinhos $(n, n+2)$ e triângulos os pares de terceiros vizinhos $(n, n+3)$. Usamos $d = 100$ e $J_{XY} = 1$. Parte superior à esquerda: $J_Z = 0$, parte superior à direita: $J_Z = J_{XY}$, parte do meio à esquerda: $J_Z = 10J_{XY}$, parte do meio à direita: $J_Z = 100J_{XY}$, parte inferior à esquerda: $J_Z = 159J_{XY}$ e parte inferior à direita: $J_Z = 327J_{XY}$.

No entanto, quando a interação de Ising se faz presente, os resultados mudam consideravelmente. Efeitos de muitos corpos passam a desempenhar um papel importante. Para o caso de uma cadeia isotrópica ($J_Z = J_{XY} = J$), conforme se pode ver na parte superior à direita da Fig. 5.1, somente os primeiros vizinhos continuam com altos valores para a concorrência. Para um caso particular de anisotropia ($J_Z > J_{XY}$), por outro lado, temos valores consideráveis para a concorrência até mesmo para segundos vizinhos, como exposto na parte do meio da Fig. 5.1. A anisotropia também causa efeitos inesperados para os terceiros vizinhos. Para o caso especial no qual $J_Z = d = 100J_{XY}$, visto na parte do meio à direita da Fig. 5.1, temos altos valores para suas concorrências, fato que não ocorre quando temos ao mesmo tempo sistema altamente anisotrópico e $J_Z \neq d$. Nesta situação, a concorrência de alguns pares se aproxima muito de 1 e, para outros, ela se torna extremamente baixa, como vemos na parte inferior da Fig. 5.1. Apesar de não ser fácil entender todos esses resultados, uma coisa fica clara. A presença do termo de Ising ($\sigma_n^z \sigma_{n+1}^z$) muda completamente o comportamento da concorrência para segundos e terceiros vizinhos [77].

5.8.2 Vários Defeitos

Agora vamos estudar como o caos e a localização podem afetar o emaranhamento de pares de qbits quando temos muitas excitações presentes na cadeia [78]. Dependendo do tipo de defeito encontrado na cadeia, o sistema pode se tornar caótico. Para determinar se nosso sistema é caótico ou não, calculamos a sua distribuição de espaçamento dos níveis energéticos. Mais adiante detalhamos esse ponto. Agora vale lembrar que assim como para o caso de dois qbits, a componente z do spin total do sistema $\sum_{n=1}^{L} S_n^z$ é conservada. Logo, como estados com diferentes números de excitações não se acoplam, trabalhamos apenas com setores da Hamiltoniana que possuem um mesmo número de excitações. E como estamos interessados prioritariamente em estudar a relação entre caos e emaranhamento nesse sistema de spins, analisamos apenas o setor com o maior número de excitações, i. e. o setor com $L/2$ excitações. Este é o setor onde o aspecto caótico de uma cadeia de spin é mais manifesto [34]. Por limitações de poder de cálculo numérico, nos restringimos a uma cadeia com $L = 12$ sítios e 6 excitações, onde lidamos com um total de $12!/(6!\,6!) = 924$ estados.

Supomos uma cadeia isotrópica ($J_Z = J_{XY} = J$) onde $J = 1$. Aplicamos campos magnéticos externos aleatórios aos qbits. Estes campos apontam na direção z e são dados por $h_n = h + d_n$, onde os d_n's são números aleatórios não correlacionados que satisfazem uma distribuição Gaussiana: $\langle d_n \rangle = 0$ e $\langle d_n d_m \rangle = d^2 \delta_{n,m}$.

Dependendo da integrabilidade (não caoticidade) e localização do sistema, podemos identificar diferentes regiões, as quais estão representadas na Fig. 5.2.

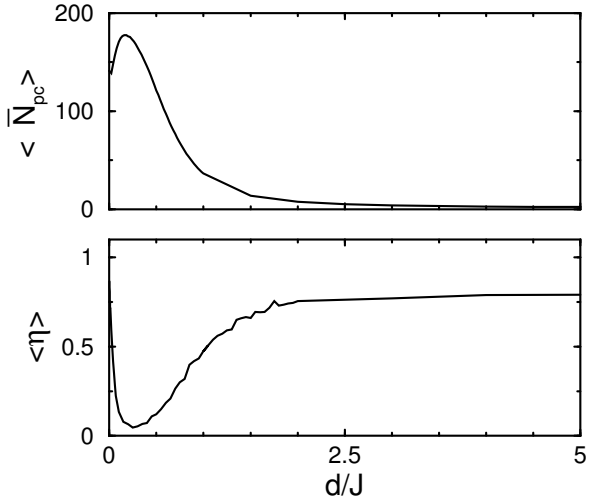


Figura 5.2: Em cima: Dependência de $\langle \overline{N_{pc}} \rangle$ por d/J. A barra representa a média sobre os 924 autovetores para cada d/J e $\langle\ \rangle$ representa a próxima média sobre 20 sequências diferentes de números aleatórios. Em baixo: Dependência de $\langle \eta \rangle$ sobre d/J. De novo, $\langle\ \rangle$ indica média sobre 20 sequências diferentes de 12 números aleatórios Gaussianos. $J = 1$.

Calculamos a média do número de componentes principais $\overline{N_{pc}}$ para os 924 autovetores em função de d. Para isso, utilizamos 12 números Gaussianos aleatórios, os quais eram os níveis de espaçamento dos qbits. Esse procedimento foi repetido para 20 sequências diferentes de 12 números. Ou seja, tivemos 20 experimentos numéricos. No topo da Fig. 5.2 mostramos $\langle\overline{N_{pc}}\rangle$, onde $\langle\,\rangle$ corresponde a média sobre 20 diferentes sequências. Paramos em 20 sequências pois, comparando algumas simulações onde usamos mais sequências, os resultados não se alteraram substancialmente. Na parte inferior da Fig. 5.2 apresentamos a quantidade usada aqui para caracterizar quão caótico está nosso sistema. Este parâmetro é definido como $\eta = \int_0^{s_0}[P(s) - P_{WD}(s)]\mathrm{d}s / \int_0^{s_0}[P_P(s) - P_{WD}(s)]\mathrm{d}s$, onde $s_0 = 0.4729...$ é o ponto de interseção entre $P_P(s)$ e $P_{WD}(s)$ [34, 52] e $P(s)$ é a distribuição do espaçamento dos níveis de energia do sistema em estudo. Um sistema regular possui $\eta = 1$ e um sistema caótico possui $\eta = 0$. Aqui novamente $\langle\,\rangle$ indica a média sobre 20 sequências de números aleatórios.

Quando $d = 0$ o sistema é integrável, mas delocalizado. Temos uma distribuição de Poisson ($\eta \sim 1$), mas alto $\langle\overline{N_{pc}}\rangle$. Aumentando d o sistema se torna caótico e ainda mais delocalizado. Para $0 < d < 0.2$, nos aproximamos de uma distribuição de Wigner-Dyson (η tende a 0) e $\langle\overline{N_{pc}}\rangle$ se torna ainda maior. No entanto, se continuamos a aumentar d, a distribuição de níveis de energia se aproxima novamente de uma distribuição de Poisson e $\langle\overline{N_{pc}}\rangle$ diminui. Esta região de transição corresponde a $0.2 < d < 2$. Assim que d se torna muito maior que a energia de interação J, o sistema passa a estar fortemente localizado, sua distribuição é novamente Poissoniana e $\langle\overline{N_{pc}}\rangle \to 1$.

Nós comparamos $\langle\overline{N}_{pc}\rangle$ e $\langle\eta\rangle$ com a concorrência para pares de qbits de primeiros vizinhos (Fig. 5.3), segundos vizinhos (alto da Fig. 5.4), e terceiros vizinhos (parte inferior da Fig. 5.4). Para cada par, calculamos a concorrência máxima $C_{\max}$ entre os 924 autovalores. Depois tomamos as médias sobre as 20 diferentes sequências de números aleatórios. Calculamos também a concorrência média $\overline{C}$ para cada par escolhido. Novamente tomamos a média de $\overline{C}$ sobre as 20 sequências de números aleatórios. As concorrências médias para todos os pares apresentam comportamentos semelhantes. Devido a isso, e ao fato de que esse valor é muito pequeno para vizinhos distantes, mostramos apenas a concorrência média para os primeiros vizinhos (parte inferior da Fig. 5.3).

Por meio das Figs. 5.2, 5.3, e 5.4 podemos analisar o que acontece com o emaranhamento nas distintas regiões em que nossa cadeia de spins se encontra.

Comecemos pela parte inferior da Fig. 5.3. Comparando as concorrências médias $\langle\overline{C}\rangle$ para $d = 0$ e $0 < d < 0.2$, que é a região onde o caos e delocalização aumentam, vemos que as concorrências decrescem um pouco. Isto sugere que para tais sistemas, com interações de primeiros vizinhos, o caos contribui para o decréscimo do emaranhamento bipartite médio entre os qbits. Na região de transição, $0.2 < d < 2$,

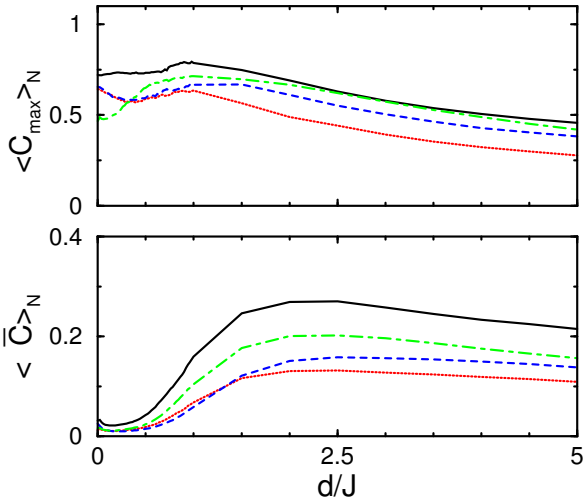


Figura 5.3: Em cima temos a dependência de $\langle C_{\max}\rangle$ por d/J e em baixo temos $\langle\overline{C}\rangle$ para alguns primeiros vizinhos (N). Em ambos os gráficos: curva preta/sólida representa o par de qbits 1-2, vermelha/pontilhada o par 3-4, azul/tracejada o par 6-7, e verde/pontilhada-tracejada os qbits 10-11.

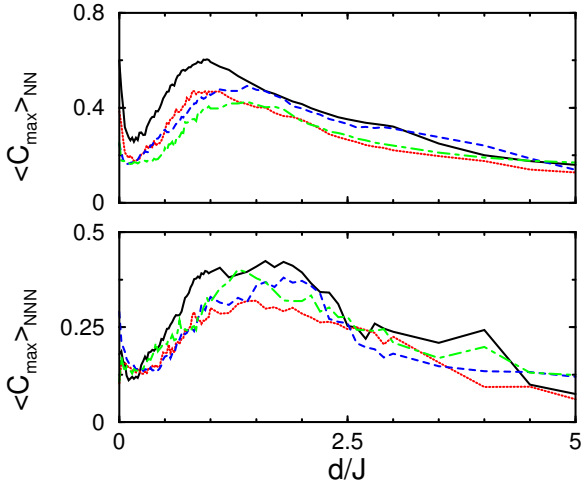


Figura 5.4: Superior: Concorrência máxima para segundos vizinhos (NN). Curva preta/sólida mostra o par 1-3, vermelha/pontilhada os qbits 2-4, azul/tracejada o par 3-5, e verde/pontilhada-tracejada o par 4-6. Inferior: Concorrência máxima para terceiros vizinhos (NNN). Curva preta/sólida nos dá o par 2-5, vermelha/pontilhada os qbits 4-7, azul/tracejada o par 5-8, e verde/pontilhada-tracejada os qbits 7-10.

região onde o sistema se torna menos caótico e mais localizado, vemos um rápido aumento das concorrências. Isto é muito interessante pois, a despeito de o sistema estar em processo de localização, as concorrências médias aumentam. Finalmente, para $d > 2$, região onde o sistema está fortemente localizado e regular (não-caótico), as concorrências médias decrescem, como era de se esperar. O efeito da localização na concorrência média, portanto, depende de quão longe estamos da região caótica.

Assim, a localização aumenta o emaranhamento se o sistema se move da região de não integrabilidade para a de integrabilidade, mas diminui o emaranhamento se o sistema já está altamente localizado.

O topo da Fig. 5.3 mostra que na região de caos ($d \sim 0.2$) a concorrência máxima para primeiros vizinhos é maior do que a $\langle C_{max} \rangle$ para os segundos e terceiros vizinhos (Fig. 5.4). Isto pode ser entendido se notarmos que para vizinhos diretamente acoplados (primeiros vizinhos), os efeitos do caos não são tão drásticos e eles preservam as concorrências máximas razoavelmente elevadas. Mas novamente verificamos que o caos diminui o emaranhamento de quaisquer dois qbits. Também vemos que na região onde a localização está se tornando forte ($d > 2$) ainda temos valores razoáveis para a $\langle C_{max} \rangle$ dos primeiros vizinhos. Esse resultado contrasta com o comportamento da $\langle C_{max} \rangle$ para os segundos e terceiros vizinhos, onde vemos uma diminuição mais rápida da $\langle C_{max} \rangle$.

Para finalizar, esses resultados também sugerem que a interação entre dois qbits contrabalanceia a destruição de seu emaranhamento devido ao caos e localização. Esta interpretação é reforçada se notarmos que a Hamiltoniana aqui considerada possui apenas interações de primeiros vizinhos e, como mostramos numericamente, primeiros vizinhos possuem mais emaranhamento se comparados a segundos e terceiros vizinhos, os quais, por sua vez, são mais susceptíveis aos efeitos do caos e localização.

Capítulo 6

Emaranhamento Térmico e Magnético

6.1 Introdução

A descoberta da existência de emaranhamento em uma cadeia de spin unidimensional, quando esta se encontra em equilíbrio térmico com um reservatório a temperatura T, foi feita independentemente por M. A. Nielsen [62] e por M. C. Arnesen *et al.* [3]. Nielsen estudou a cadeia de spin mais simples possível, uma cadeia de dois qbits, obtendo resultados analíticos que mostravam a existência de emaranhamento quando estes dois qbits estavam termalizados. Além disso, ele mostrou que por meio de um campo magnético externo, podia-se, até uma determinada temperatura, aumentar o grau de emaranhamento do sistema. Arnesen *et al.*, por sua vez, estudaram numericamente cadeias de spin compostas por até 10 qbits, obtendo resultados semelhantes.

No entanto, tanto Nielsen quanto Arnesen *et al.* usaram uma Hamiltoniana muito simples para modelar a interação entre os spins. Isso motivou muitos autores a estudarem modelos mais rebuscados, nos quais cada qbit estava submetido a um campo magnético diferente e nos quais as interações spin-spin podiam ser anisotrópicas [54, 94, 90, 42].

Neste capítulo lidamos com uma cadeia de spin sem campo magnético externo. Supomos apenas interação de primeiros vizinhos. A Hamiltoniana que descreve o sistema é:

$$H = \sum_{i=1}^{N-1} \left(\frac{J_x}{4} \sigma_x^i \sigma_x^{i+1} + \frac{J_y}{4} \sigma_y^i \sigma_y^{i+1} + \frac{J_z}{4} \sigma_z^i \sigma_z^{i+1} \right), \tag{6.1}$$

onde vamos nos restringir a dois qbits ($N = 2$), J_x, J_y, J_z são as constantes de acoplamento, e $\sigma_x, \sigma_y, \sigma_z$ as matrizes de Pauli. Usamos $\hbar = 1$.

A seguir apresentamos uma expressão analítica para a concorrência do estado térmico descrito pela Hamiltoniana (6.1) e um estudo inédito detalhado para o modelo anisotrópico XYZ [74]. Mostramos que existem regiões para os modelos XY e XYZ onde a concorrência *cresce* ao aumentarmos a anisotropia do sistema. Este comportamento é uma nova característica do emaranhamento térmico sem campo magnético externo, já que Wang [94] e Kamta e Starace [54] estudaram regiões onde a concorrência decresce com a anisotropia. Nestas regiões a anisotropia também *aumenta* a temperatura crítica T_c além da qual a concorrência é zero. Revisamos, também, os resultados obtidos pelas Refs. [54, 90, 94] para o modelo XY ($J_z = 0$) e para o modelo XXX ($J_x = J_y = J_z$), os quais são casos particulares da nossa solução analítica para a cadeia XYZ. Finalizamos o capítulo mostrando numericamente que, ao contrário dos casos onde há um campo magnético externo [3, 62], não existe nenhum conjunto de constantes de acoplamento que propicie um aumento da concorrência aumentando-se a temperatura T do sistema.

6.2 Modelo XYZ: Uma Visão Geral

Para melhor estudar o modelo XYZ, reescrevemos a Hamiltoniana (6.1) da seguinte forma:

$$H = \frac{J_z}{4}\sigma_z^1\sigma_z^2 + \frac{\Sigma+\Delta}{8}\sigma_x^1\sigma_x^2 + \frac{\Sigma-\Delta}{8}\sigma_y^1\sigma_y^2, \tag{6.2}$$

onde $\Delta = J_x - J_y$ e $\Sigma = J_x + J_y$. Os quatro autovetores dessa Hamiltoniana são os quatro estados de Bell (estados maximamente emaranhados):

$$\begin{aligned} H\left|\Phi^{\pm}\right\rangle &= \lambda_{\Phi^{\pm}}\left|\Phi^{\pm}\right\rangle, \\ H\left|\Psi^{\pm}\right\rangle &= \lambda_{\Psi^{\pm}}\left|\Psi^{\pm}\right\rangle, \end{aligned}$$

onde,

$$\begin{aligned} \left|\Phi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ \left|\Psi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \\ \lambda_{\Phi^{\pm}} &= \frac{J_z \pm \Delta}{4}, \\ \lambda_{\Psi^{\pm}} &= \frac{-J_z \pm \Sigma}{4}. \end{aligned}$$

Usamos o parâmetro $\delta = \Delta/\Sigma$ para quantificar a anisotropia do sistema. Quando $\delta = 0$ e $J_z = 0$ temos o modelo XY isotrópico e quando $\delta = \pm 1$ e $J_z = 0$ recuperamos o modelo de Ising.

A matriz densidade que descreve um sistema em equilíbrio térmico com um reservatório a temperatura T é $\rho = \exp(-H/kT)/Z$ (ensemble canônico), onde

$Z = \mathrm{Tr}\{\exp(-H/kT)\}$ é a função de partição e k é a constante de Boltzmann. A Hamiltoniana (6.2) nos dá o seguinte estado térmico escrito na base padrão (*standard basis*):

$$\rho = \frac{1}{Z}\begin{pmatrix} e^{-\alpha}\cosh(\beta) & 0 & 0 & -e^{-\alpha}\sinh(\beta) \\ 0 & e^{\alpha}\cosh(\gamma) & -e^{\alpha}\sinh(\gamma) & 0 \\ 0 & -e^{\alpha}\sinh(\gamma) & e^{\alpha}\cosh(\gamma) & 0 \\ -e^{-\alpha}\sinh(\beta) & 0 & 0 & e^{-\alpha}\cosh(\beta) \end{pmatrix}, \tag{6.3}$$

onde

$$\alpha = \frac{J_z}{4kT}, \qquad \beta = \frac{\Delta}{4kT}, \qquad \gamma = \frac{\Sigma}{4kT},$$

e

$$Z = 2\left(\exp(-\alpha)\cosh(\beta) + \exp(\alpha)\cosh(\gamma)\right).$$

Para obtermos a concorrência, precisamos das raízes quadradas dos quatro autovalores da matriz $R = \rho\tilde{\rho}$, onde $\tilde{\rho} = \sigma_y^{\otimes 2}\rho^*\sigma_y^{\otimes 2}$. Estes autovalores são dados por

$$\lambda_I^{\pm} = \frac{e^{-\alpha}}{Z}\left(\cosh(\beta) \pm \sinh(\beta)\right), \tag{6.4}$$

$$\lambda_{II}^{\pm} = \frac{e^{\alpha}}{Z}\left(\cosh(\gamma) \pm \sinh(\gamma)\right). \tag{6.5}$$

Não é trivial colocar em ordem decrescente $\lambda_I^{\pm}$ e $\lambda_{II}^{\pm}$, pois precisamos dos valores de α, β, e γ para ordená-los corretamente. Contudo, a concorrência de ρ pode ser analiticamente escrita da seguinte forma:

$$C = \begin{cases} \max\{0,\, C_1\}, & \text{se } 2\alpha > |\beta| - |\gamma|, \\ \max\{0,\, C_2\}, & \text{se } 2\alpha \leq |\beta| - |\gamma|, \end{cases} \tag{6.6}$$

onde

$$C_1 = \frac{e^{\alpha}\sinh(|\gamma|) - e^{-\alpha}\cosh(\beta)}{e^{\alpha}\cosh(\gamma) + e^{-\alpha}\cosh(\beta)}, \tag{6.7}$$

$$C_2 = \frac{e^{-\alpha}\sinh(|\beta|) - e^{\alpha}\cosh(\gamma)}{e^{\alpha}\cosh(\gamma) + e^{-\alpha}\cosh(\beta)}. \tag{6.8}$$

Antes de estudarmos em detalhes a Eq. (6.6) para valores arbitrários de J_x, J_y, e J_z, vamos estudar alguns casos particulares interessantes.

6.3 Modelo de Ising

No modelo de Ising $J_x = J_y = 0$ [94]. Isto implica $\beta = \gamma = 0$. Substituindo esse resultado na Eq. (6.6) obtemos:

$$C = \max\left\{0, \frac{-e^{-|\alpha|}}{e^{|\alpha|} + e^{-|\alpha|}}\right\} = 0. \tag{6.9}$$

Podemos entender porque o modelo de Ising termalizado não possui emaranhamento para qualquer T olhando para a matriz densidade (6.3). Quando $\beta = \gamma = 0$ ela é diagonal na base padrão, o que representa ausência de correlações. Este resultado já era esperado pois, apesar de ρ ter quatro estados maximamente emaranhados como autovetores, $|\Phi^{\pm}\rangle$ e $|\Psi^{\pm}\rangle$ são degenerados, fazendo com que sempre tenhamos emaranhamento nulo.

6.4 Modelo XY

Quando $J_z = 0$ lidamos com o modelo XY, o qual é chamado isotrópico se $J_x = J_y = J$ e anisotrópico se $J_x \neq J_y$. Analisamos separadamente os dois casos.

6.4.1 Caso Isotrópico

No modelo XY isotrópico $\alpha = \beta = 0$ e $\gamma = J/(2kT)$. Então a Eq. (6.6) fica:

$$C = \max\left\{0, \frac{\sinh\left(\frac{|J|}{2kT}\right) - 1}{\cosh\left(\frac{J}{2kT}\right) + 1}\right\}. \tag{6.10}$$

Analisando a Eq. (6.10) vemos que para temperaturas muito baixas a concorrência é próxima de 1 e que ela decresce monotonicamente com o aumento da temperatura até atingir uma temperatura crítica T_c, a qual é solução de $\sinh(|J|/(2kT_c)) = 1$. Vemos também que sistemas com altas constantes de acoplamento (J grande) possuem uma concorrência maior para um dado T do que aqueles sistemas com acoplamento fraco. Além do mais, a concorrência é a mesma se trabalhamos com sistemas ferro ($J < 0$) ou antiferromagnéticos ($J > 0$).

6.4.2 Caso Anisotrópico

Impondo $J_z = 0$ na Eq. (6.6) obtemos a seguinte expressão para a concorrência do modelo XY anisotrópico:

$$C = \max\left\{0, \frac{\sinh(|\gamma|) - \cosh(\beta)}{\cosh(\gamma) + \cosh(\beta)}\right\}, \quad \text{se } |\delta| < 1, \tag{6.11}$$

$$C = \max\left\{0, \frac{\sinh(|\beta|) - \cosh(\gamma)}{\cosh(\gamma) + \cosh(\beta)}\right\}, \quad \text{se } |\delta| \geq 1. \tag{6.12}$$

As Eqs. (6.11) e (6.12) nos mostram duas regiões de anisotropia. A primeira, $|\delta| < 1$, foi estudada por Wang [94] e por Kamta e Starace [54]. Eles mostraram que, aumentando-se a anisotropia $|\delta|$, a concorrência diminuia para uma dada temperatura T e que quando $|\delta| = 1$ a concorrência é zero para todo T (Modelo de Ising). No entanto, na segunda região, $|\delta| > 1$, vemos que a concorrência *aumenta* ao se aumentar a anisotropia δ e que a temperatura crítica T_c também aumenta com a

anisotropia. Em ambas as regiões a concorrência é função monotonicamente decrescente da temperatura. As Figs. 6.1 e 6.2 ilustram este comportamento.

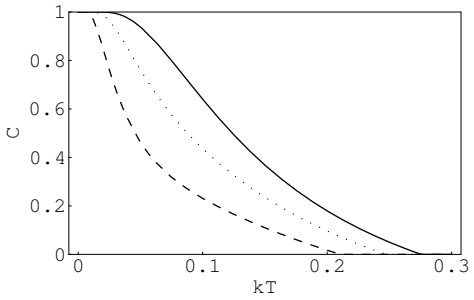


Figura 6.1: Dependência da concorrência C para o modelo XY em função da temperatura absoluta kT. A curva sólida representa $\delta = 0.3$, a pontilhada $\delta = 0.6$, e a tracejada $\delta = 0.8$. Vemos claramente que quanto maior δ menor C. Usamos $\Sigma = 1$.

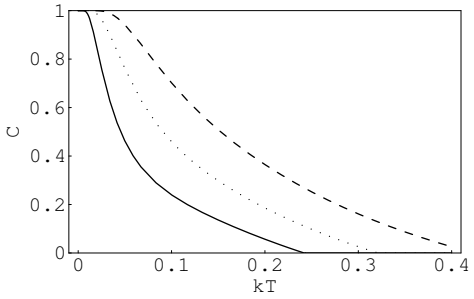


Figura 6.2: Dependência da concorrência C para o modelo XY com a temperatura. A curva sólida representa $\delta = 1.2$, a pontilhada $\delta = 1.4$, e a tracejada $\delta = 1.7$. Agora vemos que quanto maior δ *maior* é C. Usamos $\Sigma = 1$.

É interessante observar que as condições para $|\delta|$ dadas nas Eqs. (6.11) e (6.12) são equivalentes a $J_x J_y > 0$ e $J_x J_y \leq 0$ respectivamente. Isto quer dizer que a anisotropia aumenta a concorrência se J_x e J_y possuem sinais diferentes.

6.5 Modelo XXX

Quando $J_x = J_y = J_z = J$ temos o modelo XXX [3]. Dessa forma, $\beta = 0$ e $\gamma = 2\alpha$. A Eq. (6.6) nos dá $C = 0$ se $J \leq 0$ e

$$C = \max\left\{0,\, \frac{1 - 3e^{-4\alpha}}{1 + 3e^{-4\alpha}}\right\},\ \text{se } J > 0, \tag{6.13}$$

É interessante notar que, ao contrário do modelo XY isotrópico [94], a concorrência para o modelo ferromagnético XXX é sempre zero [3]. Podemos entender este fato se atentarmos para os autovalores do modelo XXX. Para $J < 0$ temos uma degenerescência no estado fundamental, o qual é formado pelos constituintes do tripleto. Logo,

$$\rho(T=0) = \frac{1}{3}\left(\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left|\Phi^-\right\rangle\left\langle\Phi^-\right|\right),$$

que é um estado não emaranhado. E aumentando-se a temperatura, o singleto se mistura com os elementos do tripleto num novo estado não emaranhado. No entanto, quando $J > 0$, o estado fundamental é formado apenas pelo singleto, um estado maximamente emaranhado, e obtemos $C = 1$. Ao se aumentar a temperatura, diminui-se o emaranhamento pois misturamos os componentes do tripleto com o singleto. Veja a Fig. 6.3.

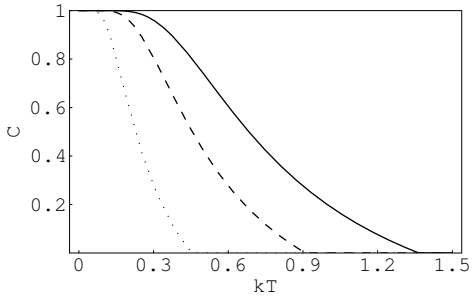


Figura 6.3: Dependência da concorrência C com a temperatura absoluta kT para três valores de constantes de acoplamento J do modelo XXX. A linha sólida representa $J = 1.5$, a tracejada $J = 1$, e a pontilhada $J = 0.5$.

6.6 Modelo XXZ

Se $J_z \neq J$ e $J_x = J_y = J$ temos o modelo XXZ. Agora $\beta = 0$ e a Eq. (6.6) nos dá $C = 0$ se $2\alpha \leq -|\gamma|$ e

$$C = \max\left\{0,\ \frac{e^{2\alpha}\sinh(|\gamma|) - 1}{e^{2\alpha}\cosh(\gamma) + 1}\right\},\ \text{se } 2\alpha > -|\gamma|. \tag{6.14}$$

Novamente podemos entender porque para $2\alpha \leq -|\gamma|$ não há emaranhamento, mesmo quando $T = 0$, estudando o estado fundamental. Nesta região, $J_z < 0$ e $|\Phi^{\pm}\rangle$ são os estados fundamentais degenerados. Portanto,

$$\rho(T=0) = \frac{1}{2}\left(\left|\Phi^{+}\right\rangle\left\langle\Phi^{+}\right| + \left|\Phi^{-}\right\rangle\left\langle\Phi^{-}\right|\right) = \frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right),$$

o qual é claramente um estado separável. Aumentando-se T, misturamos $|\Psi^{\pm}\rangle$ com $|\Phi^{\pm}\rangle$, produzindo um estado não emaranhado. Por outro lado, quando $2\alpha > -|\gamma|$ o estado fundamental é o singleto, um estado de máximo emaranhamento. Aumentando-se a temperatura misturamos os componentes do tripleto com o singleto, diminuindo, pois, a concorrência. Veja a Fig. 6.4.

Vale a pena notar que observamos numericamente que quando $J_z > 0$, o emaranhamento é função crescente de J_z. Observamos também que para qualquer sinal de J, um aumento de seu módulo sempre acarreta um aumento no emaranhamento. Estes dois resultados podem ser entendidos analisando-se os autovalores do sistema: aumentando-se o valor de $|J|$ ou de J_z, aumentamos a proporção de singletos (J

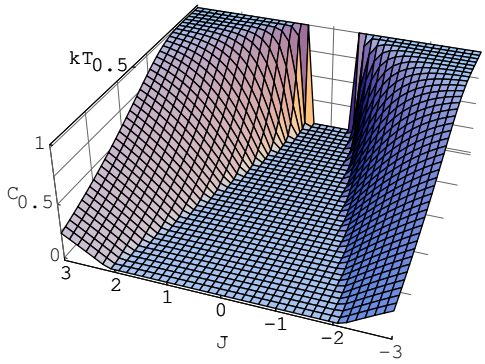


Figura 6.4: A concorrência C como função da temperatura absoluta kT e de J. Usamos $J_z = -0.5$. Fica claro que existe uma região onde $C = 0$ para qualquer T.

positivo) ou a proporção de $|\Psi^+\rangle$ (J negativo) no estado térmico. Estes dois fatos são responsáveis por um aumento da concorrência.

6.7 Estado Térmico XYZ: Estudo Detalhado

Agora vamos estudar em detalhes o modelo XYZ. J_x, J_y, e J_z são arbitrários e devemos estudar a Eq. (6.6) na sua forma mais geral. Primeiro observamos uma situação interessante. Sempre que $2\alpha = |\beta| - |\gamma|$ temos concorrência nula, mesmo em $T = 0$. Esta condição é equivalente a $2J_z = |\Delta| - |\Sigma|$, implicando que sistemas com constantes de acoplamento perto desta região não são úteis na geração de emaranhamento. As Figs. 6.5, 6.6 e 6.8, 6.9 destacam este comportamento. A Eq. (6.6) mostra que

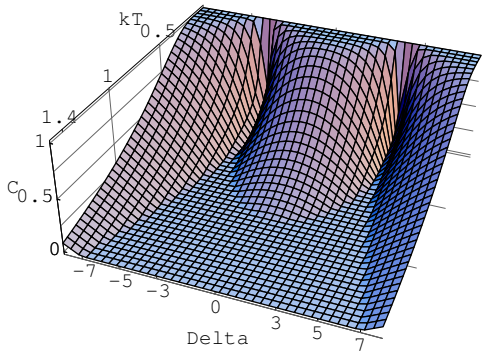


Figura 6.5: C como função de Δ e de kT. Vemos que há regiões onde um aumento da anisotropia *aumenta* C e que C é função monotonicamente decrescente de kT. $\Sigma = 2$ e $J_z = 1$.

para J_z fixo existem regiões onde se aumentando a anisotropia δ, *aumenta-se* a concorrência. Na região onde $2\alpha < |\beta| - |\gamma|$, quanto maior a anisotropia mais o sistema fica emaranhado. No entanto, na região onde $2\alpha > |\beta| - |\gamma|$, a qual se reduz às regiões estudadas por Wang e Kamta se tomamos $J_z = 0$, a anisotropia diminui o grau de emaranhamento. As Figs. 6.5 e 6.6 ilustram este fato.

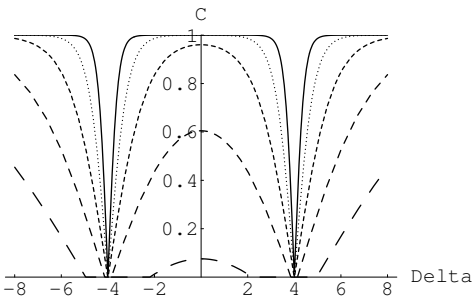


Figura 6.6: C como função de Δ para vários valores de kT. A linha sólida representa $kT = 0.05$, pontilhada $kT = 0.1$, tracejada curta $kT = 0.2$, tracejada $kT = 0.4$, e tracejada longa $kT = 0.8$. Vemos claramente que para $|\Delta| > 4$, i. e. $2\alpha < |\beta| - |\gamma|$, quanto maior a anisotropia (maior $|\Delta|$) mais emaranhado fica o sistema. $\Sigma = 2$ e $J_z = 1$.

Podemos melhor entender o comportamento de C ao variarmos Δ estudando as proporções ou probabilidades P, no estado térmico ρ, dos quatro autovetores da Hamiltoniana XYZ.

$$P_{\Phi^\pm} = Tr\left\{\left|\Phi^\pm\right\rangle\left\langle\Phi^\pm\right|\rho\right\} = \frac{\exp\left(-\lambda_{\Phi^\pm}/kT\right)}{Z}, \tag{6.15}$$

$$P_{\Psi^\pm} = Tr\left\{\left|\Psi^\pm\right\rangle\left\langle\Psi^\pm\right|\rho\right\} = \frac{\exp\left(-\lambda_{\Psi^\pm}/kT\right)}{Z}. \tag{6.16}$$

Quando $2\alpha = |\beta| - |\gamma|$ o estado térmico é uma mistura estatística onde temos em iguais proporções $|\Phi^\pm\rangle$ (Φ^- para $\beta > 0$ e Φ^+ para $\beta < 0$) e $|\Psi^-\rangle$ mais uma pequena porcentagem do estado $|\Psi^+\rangle$. Nessa situação, a matriz densidade que descreve o sistema é $\rho = (1/2 - \epsilon/2)\left(\left|\Phi^\pm\right\rangle\left\langle\Phi^\pm\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|\right) + \epsilon\left|\Psi^+\right\rangle\left\langle\Psi^+\right|$, onde $\epsilon \ll 1$. Esta matriz é separável se $\epsilon \leq 1/2$, o que explica porque nesta região onde $2\alpha = |\beta| - |\gamma|$ não temos emaranhamento. Veja Fig. 6.7.

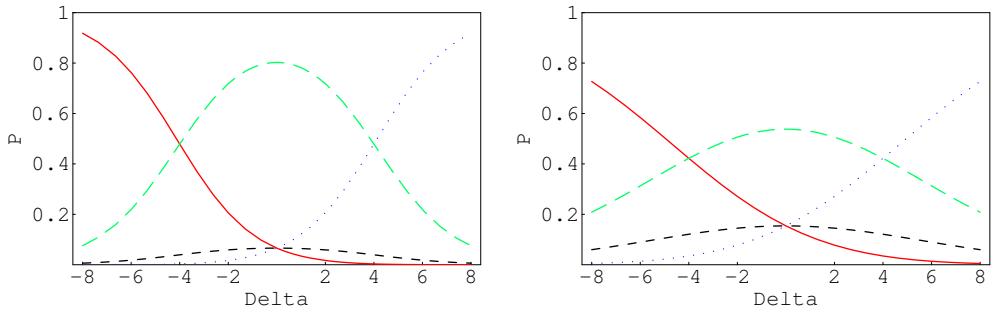


Figura 6.7: Distribuições de probabilidades P dos autovetores da Hamiltoniana XYZ no estado térmico como função de Δ. A curva sólida/vermelha fornece P para $|\Phi^+\rangle$, pontilhada/azul para $|\Phi^-\rangle$, tracejada curta/preta para $|\Psi^+\rangle$, e tracejada longa/verde para $|\Psi^-\rangle$. Para altos valores de $|\Delta|$ e $|\Delta| \approx 0$ apenas um estado de máximo emaranhamento domina, justificando porque temos alta concorrência nesta região. E mais, aumentando-se a temperatura, vemos que perto de $\Delta = 0$ os três constituintes do tripleto se misturam com o singleto, diminuindo C. Para $|\Delta|$ grande esta mistura só ocorre para altas temperaturas. $J_z = 1$ e $\Sigma = 2$. Esquerda: $kT = 0.4$. Direita: $kT = 0.8$.

Podemos também entender porque para $2\alpha < |\beta| - |\gamma|$ a anisotropia aumenta o emaranhamento estudando as Eqs. (6.15) e (6.16). Nesta região, um aumento na anisotropia (alto Δ) produz um estado térmico quase que completamente dominado por um estado de máximo emaranhamento, acarretando um aumento de C. Por outro lado, se estamos na região onde $2\alpha > |\beta| - |\gamma|$, um aumento na anisotropia produz uma mistura estatística de dois estados de máximo emaranhamento, causando um decréscimo em C. No limite onde $2\alpha = |\beta| - |\gamma|$ temos uma mistura destes dois estados em iguais proporções, deixando $C = 0$. Veja Fig. 6.7.

Fixando J_x, J_y, e variando J_z vemos que a concorrência cresce se tomamos valores de J_z maiores ou menores que $(|\Delta| - |\Sigma|)/2$. Há, porém, um valor de J_z além do qual C não cresce mais. Este comportamento é mais drástico se estamos na região onde $2\alpha > |\beta| - |\gamma|$. Lá, somente para $kT \approx 0$ obtemos $C \approx 1$. Para qualquer outro valor de kT, aumentando-se J_z faz-se com que $C \to C_{max}$, onde $C_{max} < 1$. E mais, quanto maior kT menor é o valor de C_{max}. Se estamos na região onde $2\alpha < |\beta| - |\gamma|$, diminuindo J_z nós ainda podemos obter assintoticamente $C = 1$ para $kT > 0$. Veja as Figs. 6.8 e 6.9.

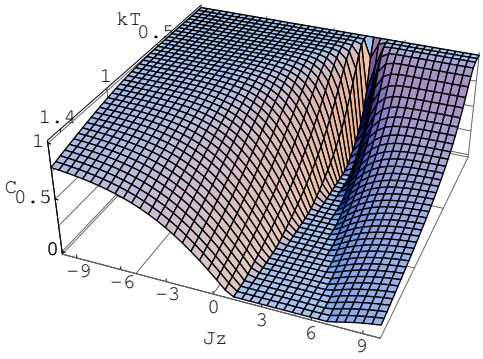


Figura 6.8: Dependência de C como função de J_z e kT. Afastando-se de $J_z = 3$, i. e. $(|\Delta| - |\Sigma|)/2$, obtemos maiores valores para C, a qual é uma função decrescente de kT. $\Delta = 7$ e $\Sigma = 1$.

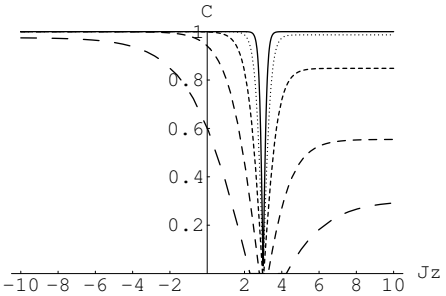


Figura 6.9: C em função de J_z para diferentes valores de kT. Para a curva sólida $kT = 0.05$, pontilhada $kT = 0.1$, tracejada curta $kT = 0.2$, tracejada $kT = 0.4$, e tracejada longa $kT = 0.8$. Na região onde $2\alpha > |\beta| - |\gamma|$ aumentando-se J_z obtemos $C \approx 1$ apenas para $kT \approx 0$. $\Delta = 7$ e $\Sigma = 1$.

Podemos novamente entender fisicamente o comportamento de C como função de J_z estudando as distribuições de probabilidades P, no estado térmico, dos quatro autovetores da Hamiltoniana XYZ. Vemos que ao nos afastarmos de $J_z = (|\Delta| - |\Sigma|)/2$ um dos estados de máximo emaranhamento começa a dominar, explicando porque C cresce. Mas somente na região onde $2\alpha < |\beta| - |\gamma|$ existem para $kT > 0$ valores de $|J_z|$ além dos quais a probabilidade P é zero para os outros três estados de Bell, e por isso $C = 1$. Se estamos na região onde $2\alpha > |\beta| - |\gamma|$ obtemos para altos valores de J_z uma contribuição razoável de outro estado de máximo emaranhamento ($|\Psi^+\rangle$), justificando porque $C < 1$ nesta região. Veja a Fig. 6.10.

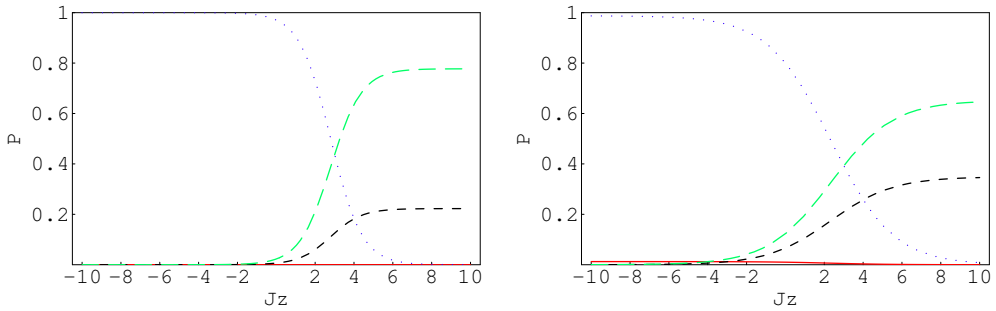


Figura 6.10: Distribuições de probabilidades P dos autovetores da Hamiltoniana XYZ no estado térmico como função de J_z. A curva sólida/vermelha fornece P para $|\Phi^+\rangle$, pontilhada/azul $|\Phi^-\rangle$, tracejada curta/preta $|\Psi^+\rangle$, e tracejada longa/verde $|\Psi^-\rangle$. Afastando-se de $J_z = 3$ um dos estados de máximo emaranhamento começa a dominar, explicando porque C cresce. $\Delta = 7$ e $\Sigma = 1$. Esquerda: $kT = 0.4$. Direita: $kT = 0.8$.

Terminamos nosso estudo da cadeia XYZ apontando que procuramos numericamente por um conjunto de constantes de acoplamento que poderia resultar em $\partial C/\partial(kT) > 0$. Se tal conjunto existisse teríamos encontrado uma região na qual aumentando-se a temperatura, aumentaríamos também o emaranhamento, sem o auxílio de campos magnéticos externos. Testamos o sinal de $\partial C/\partial(kT)$ para todas as combinações de J_x, J_y, e J_z, variando-os de -2 a 2 em incrementos de 0.01 e de -50 a 50 em incrementos de 0.5. Não encontramos nenhum conjunto de constantes onde $\partial C/\partial(kT) > 0$. Isto sugere que devemos ter sim um campo magnético externo para alcançarmos uma derivada positiva.

Parte III

Discussão e Conclusão

Capítulo 7

Conclusão

O estudo dos aspectos qualitativos e quantitativos do emaranhamento constitui uma das três grandes frentes de pesquisa da recém criada Teoria Quântica da Informação. Junto com a Computação Quântica e a Comunicação Quântica, o Emaranhamento Quântico passou a ser um assunto muito investigado no final da década de 1990 e início do século XXI. Na verdade, estas três grandes áreas se interpenetram e essa divisão é um tanto arbitrária.

Ainda hoje, apesar de um número cada vez maior de pesquisadores interessados no assunto, temos muitas perguntas sem respostas ou apenas parcialmente respondidas. Estes problemas em aberto vão desde aspectos fundamentais e conceituais em Mecânica Quântica até a aspectos práticos, como a viabilidade de se construir determinados dispositivos de comunicação e computação quântica.

Nesta tese nos concentramos numa destas frentes, o Emaranhamento Quântico. Estudamos aspectos formais do emaranhamento bem como suas implicações. Nos dedicamos ao emaranhamento bipartite e tocamos de leve o emaranhamento multipartite.

Mais especificamente, no Cap. 2, construímos um modelo no qual é possível decidir se duas partículas estão emaranhadas observando-se apenas uma delas. Medindo-se a dispersão do momento e, em seguida, a dispersão da posição em tempos diferentes de uma das partículas, podemos afirmar se lidamos com um par de partículas Gaussianas emaranhadas. Mostramos, também, que esse mesmo procedimento nos dá o grau de emaranhamento do sistema. Esse modelo simples sugere que existem situações nas quais apenas uma parte de um sistema composto pode conter todas as informações relevantes sobre o emaranhamento do sistema. Obviamente, este método só se aplica quando sabemos *a priori* se temos estados puros. Sem essa informação, ele não é válido. E mais, imaginamos improvável sua generalização para estados arbitrários, haja vista que a partir de uma determinada matriz reduzida sempre podemos construir estados mistos separáveis e estados puros emaranhados.

No entanto, este resultado sugere algo interessante e pouco explorado no estudo

do emaranhamento. Observando atentamente o funcionamento do protocolo anterior, vemos que seu sucesso está na medida das dispersões da posição para *vários* instantes de tempo. Isto quer dizer que, talvez, a evolução temporal de um estado possa nos auxiliar na determinação de seu grau de emaranhamento. A dinâmica de um sistema pode vir a se tornar uma importante ferramenta no estudo do emaranhamento. Entretanto, queremos deixar claro que isso se trata de uma conjectura. Pode ser que o resultado obtido para esse modelo, onde a evolução temporal é importante na determinação de seu grau de emaranhamento, seja apenas uma coincidência. Mas temos, de qualquer forma, um problema em aberto: até que ponto a dinâmica de um sistema pode nos auxiliar na determinação de seu grau de emaranhamento?

No capítulo seguinte, ao estudar o emaranhamento de formação (EoF) para estados descritos por variáveis canônicas, calculamos dois limites inferiores para o EoF válidos para quaisquer estados Gaussianos de dois modos. Utilizamos caminhos diferentes para chegar em cada um dos limites inferiores.

O primeiro limite inferior foi deduzido empregando-se um procedimento que simetriza um estado Gaussiano de dois modos usando-se apenas operações locais e comunicação clássica (LOCC). Assim, tomando um estado arbitrário Gaussiano, primeiramente o simetrizamos e, depois, lembrando que o emaranhamento de um sistema nunca aumenta via LOCC, calculamos o limite inferior do EoF a partir da expressão válida para estados Gaussianos simétricos.

O segundo limite inferior é um corolário de um teorema sobre estados Gaussianos mistos simétricos. Este teorema pode ser entendido como uma generalização do seguinte resultado já demonstrado para estados puros: dados dois estados puros de dois modos com a mesma quantidade de emaranhamento, onde um deles é um estado comprimido, este sempre terá o maior grau de não-localidade EPR. O teorema por nós demonstrado diz que, para as mesmas hipóteses do teorema anterior, relaxando apenas a exigência de lidarmos com estado puro, os estados Gaussianos simétricos mistos são aqueles com a maior não-localidade EPR. E, como podemos mostrar que o grau de emaranhamento está relacionado com o aspecto não-local de um estado misto, podemos determinar um limite inferior para o seu EoF. Apesar de os limites inferiores deduzidos no Cap. 3 nos ajudarem a entender o comportamento do emaranhamento para estados Gaussianos arbitrários, ainda falta esclarecer se existe ou não uma expressão analítica para o valor exato do EoF para estados Gaussianos não simétricos. E, caso ela exista, qual é esta expressão?

Também no Cap. 3 mostramos como Alice pode, deterministicamente e com máxima fidelidade, teleportar um estado arbitrário de dois qbits. Este mesmo protocolo foi generalizado para teleportar um cadeia de N qbits. O canal quântico compartilhado por Alice e Bob para a realização do protocolo de teletransporte também pode ser usado para realizar codificação superdensa. Mostramos que o protocolo de codificação superdensa atinge o limite de Holevo, i. e., a máxima capacidade de

transmissão de informação permitida para um dado estado quântico. Provamos, em seguida, que o canal quântico usado no teletransporte de N qbits é equivalente a N estados de Bell trabalhando em paralelo.

Apresentamos também uma maneira de quantificar a eficiência que $2N$ qbits possuem para teleportar N qbits. Chamamos esta eficiência de Emaranhamento de Teletransporte (E_T). O E_T é uma medida de emaranhamento para sistemas multipartites, possuindo uma fácil implementação e um forte apelo físico. Devemos ressaltar, entretanto, que o E_T só está definido para um número par de qbits. Uma generalização desse resultado para um número ímpar de qbits e, por que não, para estados mistos será um passo muito importante na quantificação de emaranhamento multipartite.

A partir do Cap. 4 passamos a estudar algumas consequências do emaranhamento. Mostramos que as relações de incerteza para partículas idênticas emaranhadas são mais gerais do que aquelas apresentadas por Heisenberg. Esta nova relação pôde explicar resultados experimentais que, aparentemente, violavam as relações de incerteza de Heisenberg para uma única partícula.

No Cap. 5 estudamos como o emaranhamento está relacionado com o caos e localização em cadeias de spin de uma dimensão. O modelo utilizado neste estudo foi uma cadeia isotrópica, onde os spins interagiam apenas com seus primeiros vizinhos. Os spins eram submetidos a campos magnéticos externos aleatórios. Dependendo da intensidade destes campos, conseguíamos deixar o sistema caótico ou integrável. Mostramos que o caos é responsável por um decréscimo no emaranhamento bipartite entre os primeiros, segundos e terceiros vizinhos. Observamos também que os primeiros vizinhos são menos sensíveis ao caos, estando razoavelmente emaranhados num ambiente caótico.

Exploramos também a relação entre emaranhamento e localização. Verificamos que na região de forte localização, onde o sistema é integrável, o emaranhamento decresce com a localização. Contudo, na região de transição entre caos e integrabilidade (ausência de caos), observamos um aumento do emaranhamento entre os spins conforme o sistema se tornava mais localizado.

No Cap. 6 estudamos o emaranhamento térmico entre dois qbits descritos pelo modelo de Heisenberg XYZ. Nesta análise, não tínhamos campos magnéticos externos atuando nos qbits. Apresentamos uma expressão analítica para o emaranhamento desse sistema, a qual se reduz a resultados já conhecidos para os modelos XY e XXX. Mostramos que existem regiões de anistropia nas constantes de acoplamento onde quanto maior a anisotropia mais emaranhado é o estado térmico para uma dada temperatura T. Nestas regiões, a temperatura crítica, além da qual o emaranhamento é nulo, também aumenta com o aumento da anisotropia. Fizemos uma busca numérica tentando encontrar combinações de constantes de acoplamento onde um aumento na temperatura causasse um aumento no emaranhamento. Não fomos

bem sucedidos nesta busca, sugerindo que precisamos sempre de campos magnéticos externos para que este tipo de fenômeno ocorra.

Finalmente, vale a pena mencionar que há muito por se fazer para que possamos entender de fato o comportamento do emaranhamento térmico em uma cadeia de spin. Estamos preparando um estudo analítico para o modelo XYZ com campo magnético externo e já temos um algoritmo codificado, em fase de testes, que nos permitirá estudar numericamente cadeias maiores, com ou sem campo magnético. Seria interessante também estudar, tanto analitica quanto numericamente, cadeias de spins com interações de longo alcance utilizando-se de alguma medida de emaranhamento global.

Apêndice A

Medidas em Mecânica Quântica

Modernamente podemos apresentar o postulado da medida em Mecânica Quântica da seguinte forma [63]:

Postulado 1 *Uma medida quântica é descrita por um conjunto* $\{M_m\}$ *de operadores de medida, os quais atuam no espaço de Hilbert do sistema observado. A cada possível resultado da medida associamos um índice* m*. A probabilidade* $p(m)$ *de obtermos o resultado rotulado por* m *para um estado descrito por* $|\Psi\rangle$ *é*

$$p(m) = \langle\Psi|M_m^\dagger M_m|\Psi\rangle.$$

Após a medida o novo estado que descreve o sistema é

$$|\Psi\rangle \longrightarrow \frac{M_m|\Psi\rangle}{\sqrt{\langle\Psi|M_m^\dagger M_m|\Psi\rangle}}.$$

Para que $p(m)$ possa ser interpretado como probabilidades, os operadores M_m devem satisfazer as seguintes propriedades:

$$\begin{aligned} M_m^\dagger M_m &\geq 0, \\ \sum_m M_m^\dagger M_m &= \mathcal{I}. \end{aligned}$$

A primeira relação implica probabilidades positivas e a segunda garante que a soma de todos os $p(m)$ seja 1.

Por meio desta definição, a medida projetiva de von Neumann é vista como um caso muito particular de medida quântica. Quando $M_m M_{m'} = \delta_{m,m'} M_m$, i. e., M_m é um projetor, lidamos com medidas projetivas. Agora, uma medida valorada por operadores positivos (POVM) ocorre quando temos operadores $E_m = M_m^\dagger M_m \geq 0$ tais que

$$p(m) = \langle\Psi|E_m|\Psi\rangle \quad \text{e} \quad \textstyle\sum_m E_m = \mathcal{I}.$$

Os operadores E_m são os *elementos do POVM* associados ao resultado da possível medida. O conjunto completo $\{E_m\}$ é conhecido como POVM. A partir dos elementos do POVM podemos construir operadores de medida M_m. Para isso basta tomarmos $M_m = \sqrt{E_m}$. Dessa forma M_m satisfaz todas as propriedades de um operador de medida.

Um POVM também é conhecido por medida borrada (*fuzzy measurement*). O termo *fuzzy* é usado para realçar que não projetamos necessariamente o estado do sistema após a medida. Fisicamente podemos entender as medidas *fuzzy* como sendo menos invasivas do que as medidas projetivas. Numa visão simplista, neste tipo de medida obtemos alguma informação do sistema sem, no entanto, eliminarmos completamente a evolução unitária inerente ao sistema observado. Um exemplo muito interessante de aplicação de medidas *fuzzy* se dá durante a transição entre dois estados quânticos ortogonais [59]. Podemos acompanhar o processo de transição de um elétron, por exemplo, entre dois níveis de energia. Este acompanhamento seria impossível se nos atêssemos apenas a medidas projetivas de von Neumann.

Para finalizar esse Apêndice, vamos ilustrar o conceito de POVM através de um exemplo bem simples [63]. Suponhamos que Alice envie a Bob um qbit descrito por $|\psi_1\rangle = |0\rangle$ ou por $|\psi_2\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$. O objetivo de Bob é descobrir qual estado Alice enviou. Como estes estados não são ortogonais, Bob não poderia distingui-los utilizando-se apenas de medidas projetivas de von Neumann. Agora, se Bob faz uso do POVM descrito pelos elementos

$$\begin{aligned} E_1 &= \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|, \\ E_2 &= \frac{\sqrt{2}}{1+\sqrt{2}}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|) \quad \text{e} \\ E_3 &= \mathcal{I} - E_1 - E_2, \end{aligned}$$

ele poderá, às vezes, distinguir perfeitamente entre $|\psi_1\rangle$ e $|\psi_2\rangle$.

Se Bob recebe o estado $|\psi_1\rangle$, então $p(1) = 0, p(2) \neq 0$ e $p(3) \neq 0$. Por outro lado, recebendo $|\psi_2\rangle$ temos que $p(1) \neq 0, p(2) = 0$ e $p(3) \neq 0$. Dessa forma, se Bob obter E_1 ele tem certeza de que Alice enviou $|\psi_2\rangle$. Caso ele obtenha E_2, Bob está certo de que seu estado é $|\psi_1\rangle$. Contudo, sempre que ele medir E_3, nada poderá afirmar. Este é o preço que se paga para poder distinguir estados não ortogonais. Nem sempre o protocolo funcionará.

Apêndice B

Teorema da Não-Clonagem.

Suponhamos que exista uma máquina que clone estados quânticos arbitrários. Ela recebe o estado a ser clonado, implementa uma transformação unitária U e devolve dois estados idênticos. Dessa forma, para dois estados *distintos* de entrada $|\phi_1\rangle$ e $|\phi_2\rangle$ temos

$$U(|\phi_1\rangle \otimes |\psi\rangle) = |\phi_1\rangle \otimes |\phi_1\rangle, \tag{B.1}$$

$$U(|\phi_2\rangle \otimes |\psi\rangle) = |\phi_2\rangle \otimes |\phi_2\rangle, \tag{B.2}$$

onde $|\psi\rangle$ é o estado inicial auxiliar fornecido pela máquina de clonagem. Calculando o produto escalar entre as Eqs. (B.1) e (B.2),

$$\begin{aligned} \langle\phi_1|\phi_2\rangle\langle\psi|\psi\rangle &= \langle\phi_1|\phi_2\rangle\langle\phi_1|\phi_2\rangle, \\ \langle\phi_1|\phi_2\rangle &= \langle\phi_1|\phi_2\rangle\langle\phi_1|\phi_2\rangle. \end{aligned} \tag{B.3}$$

Há apenas duas possibilidades. Se $\langle\phi_1|\phi_2\rangle \neq 0$, então necessariamente $\langle\phi_1|\phi_2\rangle = 1$, i. e., $|\phi_1\rangle = |\phi_2\rangle$, o que contradiz a hipótese. Se $\langle\phi_1|\phi_2\rangle = 0$, então $|\phi_1\rangle$ e $|\phi_2\rangle$ são estados ortogonais. Dessa forma, podemos apenas clonar estados ortogonais, não existindo uma máquina quântica que clone estados arbitrários. E mais, o fato de podermos clonar estados ortogonais está de acordo com a possibilidade de clonar estados clássicos, pois obviamente estados clássicos distintos são ortogonais.

Apêndice C

Teorema de Bell

Tomemos um sistema composto particionado em dois subsistemas, os quais se encontram com Alice e Bob. Ambos possuem aparatos capazes de medir as variáveis A e B. Estas variáveis podem assumir apenas dois valores: ± 1.

Alice e Bob podem ajustar da maneira que lhes convier as configurações de seus instrumentos de medida. Para spins-1/2 estas configurações correspondem a possíveis orientações de um campo magnético não homogêneo. Para medidas de polarização de fótons, elas correspondem às orientações dos polarizadores. Chamemos de $\mathbf{a}$ a orientação do aparato de medida com Alice e de $\mathbf{b}$ a orientação do aparato com Bob.

Vamos supor que o resultado de qualquer medida depende das possíveis orientações (parâmetros controláveis) e de um número qualquer de parâmetros incontroláveis, seja porque não desenvolvemos técnicas experimentais para controlá-los ou seja porque a Natureza proíbe seu controle. Representamos coletivamente estes parâmetros por λ. Dessa forma, podemos especificar os resultados das medidas feitas por Alice e por Bob pelas funções abaixo, as quais podem assumir apenas os valores ± 1:

$$A(\mathbf{a}, \mathbf{b}, \lambda) = \pm 1, \quad B(\mathbf{a}, \mathbf{b}, \lambda) = \pm 1. \tag{C.1}$$

Agora, lançando mão da hipótese de *localidade*, o resultado da medida feita por Alice não pode depender da orientação escolhida por Bob. O mesmo tipo de raciocínio se aplica aos resultados obtidos por Bob. Assim sendo,

$$A(\mathbf{a}, \mathbf{b}, \lambda) \longrightarrow A(\mathbf{a}, \lambda), \quad B(\mathbf{a}, \mathbf{b}, \lambda) \longrightarrow B(\mathbf{b}, \lambda). \tag{C.2}$$

Para obtermos predições quantitativas desta hipótese de localidade, precisamos estudar as correlações entre os resultados das medidas de Alice e de Bob. Para cada par de partículas produzido, λ pode assumir qualquer valor. Definimos, pois, a função de correlação abaixo,

$$P(a, b) = \int A(\mathbf{a}, \lambda) B(\mathbf{b}, \lambda) \rho(\lambda) \mathrm{d}\lambda, \tag{C.3}$$

onde $\rho(\lambda)$ é uma distribuição de probabilidade que representa os possíveis valores para o parâmetro incontrolável λ. Por ser distribuição de probabilidade, $\rho(\lambda) \geq 0$ e $\int \rho(\lambda)\mathrm{d}\lambda = 1$. Não supomos nenhuma função específica para $\rho(\lambda)$. Uma possível teoria de variável oculta nos forneceria a regra de como calcular $\rho(\lambda)$.

Consideremos um cenário onde Alice realiza suas medidas em duas possíveis orientações, $\mathbf{a}$ e $\mathbf{a}'$, escolhendo aleatoriamente para cada medida uma dessas duas orientações. Bob também procede da mesma forma, orientando seu aparelho de medida ora na direção $\mathbf{b}$ e ora na direção $\mathbf{b}'$. Dessa forma, temos quatro funções de correlação, as quais devem satisfazer a desigualdade abaixo[1]

$$\begin{aligned}
P(\mathbf{a},\mathbf{b}) - P(\mathbf{a},\mathbf{b}') &= \int A(\mathbf{a},\lambda)B(\mathbf{b},\lambda)\rho(\lambda)\mathrm{d}\lambda - \int A(\mathbf{a},\lambda)B(\mathbf{b}',\lambda)\rho(\lambda)\mathrm{d}\lambda \\
&= \int A(\mathbf{a},\lambda)B(\mathbf{b},\lambda)\rho(\lambda)\mathrm{d}\lambda - \int A(\mathbf{a},\lambda)B(\mathbf{b}',\lambda)\rho(\lambda)\mathrm{d}\lambda \\
&\quad - \int A(\mathbf{a},\lambda)B(\mathbf{b},\lambda)A(\mathbf{a}',\lambda)B(\mathbf{b}',\lambda)\rho(\lambda)\mathrm{d}\lambda \\
&\quad + \int A(\mathbf{a},\lambda)B(\mathbf{b},\lambda)A(\mathbf{a}',\lambda)B(\mathbf{b}',\lambda)\rho(\lambda)\mathrm{d}\lambda \\
&= \int A(\mathbf{a},\lambda)B(\mathbf{b},\lambda)[1 - A(\mathbf{a}',\lambda)B(\mathbf{b}',\lambda)]\rho(\lambda)\mathrm{d}\lambda \\
&\quad - \int A(\mathbf{a},\lambda)B(\mathbf{b}',\lambda)[1 - A(\mathbf{a}',\lambda)B(\mathbf{b},\lambda)]\rho(\lambda)\mathrm{d}\lambda.
\end{aligned}$$

Agora, como as funções A e B são no máximo iguais a unidade, quaisquer produtos dessas funções também atingem no máximo a unidade. Dessa forma, um limitante superior para o módulo do lado esquerdo da equação anterior é

$$\begin{aligned}
|P(\mathbf{a},\mathbf{b}) - P(\mathbf{a},\mathbf{b}')| &\leq \int [1 - A(\mathbf{a}',\lambda)B(\mathbf{b}',\lambda)]\rho(\lambda)\mathrm{d}\lambda \\
&\quad + \int [1 - A(\mathbf{a}',\lambda)B(\mathbf{b},\lambda)]\rho(\lambda)\mathrm{d}\lambda. \\
&\leq 2 - P(\mathbf{a}',\mathbf{b}') - P(\mathbf{a}',\mathbf{b}).
\end{aligned}$$

Rearranjando a expressão anterior,

$$S = |P(\mathbf{a},\mathbf{b}) - P(\mathbf{a},\mathbf{b}')| + P(\mathbf{a}',\mathbf{b}') + P(\mathbf{a}',\mathbf{b}) \leq 2. \tag{C.4}$$

Assim, se um sistema composto viola a desigualdade acima, $S > 2$, dizemos que ele não satisfaz a hipótese de localidade de Bell.

[1] A demonstração que se segue é fortemente baseada na apresentada pela Ref. [6], diferindo daquela originalmente feita por Bell [9].

Apêndice D

Decomposição de Schmidt

A decomposição de Schmidt é uma ferramenta muito útil no estudo das propriedades de emaranhamento de sistemas bipartites. Apresentamos essa decomposição através do teorema abaixo.

Teorema 14 *Seja $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ um estado puro composto por dois subsistemas A e B. Então existem estados ortonormais $|u_i\rangle_A$ para o sistema A e $|v_i\rangle_B$ para o sistema B tais que*

$$|\Psi\rangle = \sum_{i=1}^{n} \sqrt{p_i}|u_i\rangle_A|v_i\rangle_B, \tag{D.1}$$

onde $n = min\{dim\mathcal{H}_A, dim\mathcal{H}_B\}$, $\sqrt{p_i}$ são números reais não negativos, conhecidos como coeficientes de Schmidt, e $\sum_i p_i = 1$.

Prova:
Sem perder em generalidade, seja $\dim\mathcal{H}_A \leq \dim\mathcal{H}_B$. Dessa forma, $\{|u_i\rangle_A\}$ é uma base ortonormal de $\mathcal{H}_A$. Podemos, pois, escrever $|\Psi\rangle$ da seguinte forma, onde $\{|z_k\rangle_B\}$ é uma base ortonormal qualquer de $\mathcal{H}_B$.

$$|\Psi\rangle = \sum_{i=1}^{\dim\mathcal{H}_A} \sum_{k=1}^{\dim\mathcal{H}_B} a_{ik}|u_i\rangle_A|z_k\rangle_B = \sum_{i=1}^{n} |u_i\rangle_A|\tilde{v}_i\rangle_B, \tag{D.2}$$

onde $|\tilde{v}_i\rangle_B = \sum_k a_{ik}|z_k\rangle_B$. Vale a pena observar que, pelo menos por enquanto, não podemos dizer se $\{|\tilde{v}_i\rangle_B\}$ são ortonormais.

Vamos supor que $\{|u_i\rangle_A\}$ foi escolhido de tal forma a deixar $\rho_A = \mathrm{Tr}_B(\rho)$ diagonal. Aqui, $\rho = |\Psi\rangle\langle\Psi|$. Isto é, queremos

$$\rho_A = \sum_{i=1}^{n} p_i|u_i\rangle_A\,{}_A\langle u_i|. \tag{D.3}$$

Como ρ_A é matriz densidade, p_i é não negativo e $\sum_i p_i = 1$. Mas podemos calcular ρ_A diretamente de ρ, o qual pode ser escrito como

$$\begin{aligned} \rho &= |\Psi\rangle\langle\Psi| = \left(\sum_{i=1}^{n} |u_i\rangle_A |\tilde{v}_i\rangle_B\right)\left(\sum_{i'=1}^{n} {}_A\langle u_{i'}|\,{}_B\langle\tilde{v}_{i'}|\right) \\ &= \sum_{i,i'=1}^{n} |u_i\rangle_A\,{}_A\langle u_{i'}| \otimes |\tilde{v}_i\rangle_B\,{}_B\langle\tilde{v}_{i'}|. \end{aligned} \tag{D.4}$$

Calculando ρ_A por meio da Eq. (D.4) obtemos

$$\rho_A = \sum_{i,i'}^{n} {}_B\langle\tilde{v}_{i'}|\tilde{v}_i\rangle_B\,|u_i\rangle_A\,{}_A\langle u_{i'}|. \tag{D.5}$$

Comparando as Eqs. (D.3) e (D.5) e lembrando que por construção ρ_A é diagonal quando escrita na base $\{|u_i\rangle_A\}$, necessariamente devemos ter

$${}_B\langle\tilde{v}_{i'}|\tilde{v}_i\rangle_B = p_i\delta_{ii'}. \tag{D.6}$$

Esta última condição nos mostra que $\{|\tilde{v}_i\rangle_B\}$ forma um conjunto de estados ortogonais. Para encontrar estados ortonormais, e mostrarmos a decomposição de Schmidt, basta definir o estado abaixo a partir de $|\tilde{v}_i\rangle_B$,

$$|\tilde{v}_i\rangle_B = \sqrt{p_i}|v_i\rangle_B. \tag{D.7}$$

Assim, substituindo a Eq. (D.7) em (D.2) temos a decomposição de Schmidt,

$$|\Psi\rangle = \sum_{i=1}^{n} \sqrt{p_i}|u_i\rangle_A|v_i\rangle_B. \qquad \square \tag{D.8}$$

Um exemplo interessante de aplicação da decomposição de Schmidt pode ser visto quando lidamos com dois qbits. Pelo teorema de Schmidt um estado de dois qbits pode ser escrito como

$$|\Psi\rangle = \sqrt{p_1}|u_1\rangle|v_1\rangle + \sqrt{p_2}|u_2\rangle|v_2\rangle. \tag{D.9}$$

Na expressão acima, e onde não houver possibilidade de confusão, não escreveremos mais os subíndices A e B. Implementando em $|\Psi\rangle$ a transformação unitária local $U = U_A \otimes U_B$, onde,

$$U_A = |0\rangle\langle u_1| + |1\rangle\langle u_2|, \tag{D.10}$$

$$U_B = |1\rangle\langle v_1| + |0\rangle\langle v_2|, \tag{D.11}$$

obtemos,

$$|\Phi\rangle = U|\Psi\rangle = c_1|01\rangle + c_2|10\rangle, \tag{D.12}$$

sendo $c_i = \sqrt{p_i}$. Ou seja, todo estado de dois qbits pode ser escrito, via transformações unitárias locais, como $|\Phi\rangle$. E como transformações unitárias locais preservam o grau de emaranhamento do sistema, todo estado emaranhado de dois qbits possui dois coeficientes de Schmidt diferentes de zero. Se um dos coeficientes de Schmidt for nulo, temos estado separável. Colocando de outra forma, acabamos de mostrar um critério de separabilidade para estados puros bipartites, o qual se baseia no estudo de seus coeficientes de Schmidt.

Apêndice E

Concavidade de $\Delta(\rho)$

Precisamos provar que $\Delta(\rho) \geq \sum_j p_j \Delta(\phi_j)$, onde $\rho = \sum_j p_j \left|\phi_j\right\rangle \left\langle\phi_j\right|$. Usando a definição de $\Delta(\rho)$ obtemos para ρ e para $\sum_j p_j \Delta(\phi_j)$ as seguintes expressões:

$$\begin{aligned}\Delta(\rho) &= \min\left\{1, \frac{1}{2}\left[\sum_j p_j \left(\left\langle X^2\right\rangle_{\phi_j} + \left\langle P^2\right\rangle_{\phi_j}\right) - \left(\sum_j p_j \left\langle X\right\rangle_{\phi_j}\right)^2 \right.\right. \\ &\quad \left.\left. - \left(\sum_j p_j \left\langle P\right\rangle_{\phi_j}\right)^2\right]\right\}, \qquad \text{(E.1)}\end{aligned}$$

$$\begin{aligned}\sum_j p_j \Delta(\phi_j) &= \sum_j p_j \min\left\{1, \frac{1}{2}\left[\left\langle X^2\right\rangle_{\phi_j} + \left\langle P^2\right\rangle_{\phi_j} - \left\langle X\right\rangle^2_{\phi_j} - \left\langle P\right\rangle^2_{\phi_j}\right]\right\} \qquad \text{(E.2)} \\ &\leq \frac{1}{2}\sum_j p_j \left[\left\langle X^2\right\rangle_{\phi_j} + \left\langle P^2\right\rangle_{\phi_j} - \left\langle X\right\rangle^2_{\phi_j} - \left\langle P\right\rangle^2_{\phi_j}\right], \qquad \text{(E.3)}\end{aligned}$$

onde $X = X_1 - X_2$ e $P = P_1 + P_2$. A desigualdade é consequência do fato de que podemos ter pelo menos um $\left\langle X^2\right\rangle_{\phi_j} + \left\langle P^2\right\rangle_{\phi_j} - \left\langle X\right\rangle^2_{\phi_j} - \left\langle P\right\rangle^2_{\phi_j} > 2$. Olhando para a Eq. (E.2) vemos que ela não é maior do que 1. Logo, se a Eq. (E.1) é igual a 1 temos $\Delta(\rho) \geq \sum_j p_j \Delta(\phi_j)$. Mas se ela é menor do que 1, $\Delta(\rho) \geq \sum_j p_j \Delta(\phi_j)$ se a seguinte desigualdade é satisfeita:

$$\left(\sum_j p_j \left\langle X\right\rangle_{\phi_j}\right)^2 + \left(\sum_j p_j \left\langle P\right\rangle_{\phi_j}\right)^2 \leq \sum_j p_j \left[\left\langle X\right\rangle^2_{\phi_j} + \left\langle P\right\rangle^2_{\phi_j}\right]. \qquad \text{(E.4)}$$

Usando a desigualdade de Cauchy-Schwarz [26] para um observável R obtemos $\sum_j p_j \left\langle R\right\rangle^2_{\phi_j} \geq \left(\sum_j p_j \left\langle R\right\rangle_{\phi_j}\right)^2$. Portanto, a Eq. (E.4) é sempre satisfeita. □

Referências Bibliográficas

[1] F. C. Alcaraz, M. N. Barber, & M. T. Batchelor, *Ann. of Phys. (N. Y.)* **182**, 280 (1988).

[2] G. Arfken, *Mathematical Methods for Physicists* (Academic Press, Orlando, 1985), Cap. 8.

[3] M. C. Arnesen, S. Bose, & V. Vedral, *Phys. Rev. Lett.* **87**, 017901 (2001).

[4] A. Aspect, P. Grangier, & G. Roger, *Phys. Rev. Lett.* **47**, 460 (1981).

[5] A. Aspect, P. Grangier, & G. Roger, *Phys. Rev. Lett.* **49**, 91 (1982).

[6] L. E. Ballentine, *Quantum Mechanics* (World Scienfific, Singapore, 1998), p. 234-238.

[7] J. N. Bandyopadhyay & A. Lakshminarayan, *Phys. Rev. Lett.* **89**, 060402 (2002).

[8] S. M. Barnett & P. L. Knight, *J. Mod. Opt.* **34**, 841 (1987).

[9] J. S. Bell, *Physica* **1**, 195 (1964).

[10] C.H. Bennett & G. Brassard *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, Bangalore, Índia, Dezembro 1984, p. 175.

[11] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, & W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).

[12] C. H. Bennett & S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).

[13] C. H. Bennett, H. J. Bernstein, S. Popescu, & B. Schumacher, *Phys. Rev. A* **53**, 2046 (1996).

[14] C. H. Bennett, D. P. DiVincenzo, J. Smolin, & W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).

[15] C. H. Bennett, G. Brassard, S. Popescu, R. Schumacher, J. Smolin, & W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).

[16] H. A. Bethe, *Z. Phys.* **71**, 205 (1931).

[17] D. Bohm, *Quantum Theory* (Dover Publications, Mineola, 1989), p. 614-615.

[18] N. Bohr, *Phys. Rev.* **48**, 696 (1935).

[19] D. Bouwmeester, A. K. Ekert, & A. Zeilinger (Eds.), *The Physics of Quantum Information* (Springer-Verlag, Berlin, 2000).

[20] S. L. Braunstein & P. van Loock, *eprint quant-ph/0410100.* (A ser publicado em *Rev. Mod. Phys.*)

[21] D. Bruss, G. M. D'Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), & U. Sen, *Phys. Rev. Lett.* **93**, 210501 (2004).

[22] C. M. Caves, I. H. Deutsch, & R. B.-Kohout, *J. Opt. B: Quantum Semiclass. Opt.* **6**, S801 (2004).

[23] J. L. Cereceda, *eprint quant-ph/0105096.*

[24] J. F. Clauser, M. A. Horne, A. Shimony, & R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).

[25] C. Cohen-Tannoudji, B. Diu, & F. Laloë, *Quantum Mechanics* **Vols. 1 and 2** (Hermann and John Wiley & Sons, Paris, 1977).

[26] L.-M. Duan, G. Giedke, J. I. Cirac, & P. Zoller, *Phys. Rev. Lett.* **84**, 2722 (2000).

[27] M. I. Dykman & P. M. Platzman, *Fortschr. Phys* **48**, 9 (2000).

[28] M. I. Dykman & L. F. Santos, *J. Phys. A* **36**, L561 (2003).

[29] R. E. Edwards, *Functional analysis, theory and application* (Holt, Rinehart and Winston, New York, 1965).

[30] A. Einstein, B. Podolsky, & N. Rosen, *Phys. Rev.* **47**, 777 (1935).

[31] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

[32] B-G. Englert & K. Wódkiewicz, *Phys. Rev. A* **65**, 054303 (2002).

[33] T. Gao, Z.-X. Wang, & F.-l. Yan, *Chin. Phys. Lett.* **20**, 2094 (2003).

[34] B. Georgeot & D. L. Shepelyansky, *Phys. Rev. E* **62**, 3504 (2000).

[35] G. Giedke, L-M. Duan, I. Cirac, & P. Zoller, *Quantum Inf. and Comp.* **1**, 79 (2001).

[36] G. Giedke, M. M. Wolf, O. Krüger, R. F. Werner, & J. I. Cirac, *Phys. Rev. Lett.* **91**, 107901 (2003).

[37] N. Gisin, *Phys. Lett. A* **154**, 201 (1991).

[38] N. Gisin, *Phys. Lett. A* **210**, 151 (1996).

[39] V. N. Gorbachev, A. I. Trubilko, A. I. Zhiliba, & E. S. Yakovleva, *eprint quant-ph/0011124*.

[40] D. M. Greenberger, M. A. Horne, A. Shimony, & A. Zeilinger, *Am. J. Phys.* **58**, 1131 (1990).

[41] L. K. Grover, *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, Maio 1996, p. 212 (quant-ph/9605043).

[42] S-J. Gu, H-Q. Lin, & Y-Q. Li, *Phys. Rev. A* **68**, 042330 (2003).

[43] T. Guhr, A. Müller-Groeling, & H.A. Weidenmüller, *Phys. Rep.* **299**, 189 (1998).

[44] W. Heisenberg, *Z. Phys.*, **43**, 172 (1927).

[45] R. A. Horn & C. R. Johnson, *Matrix Analysis* (Cambridge University Press, New York, 1985).

[46] R. Horodecki, P. Horodecki, & M. Horodecki, *Phys. Lett. A* **200**, 340 (1995).

[47] M. Horodecki, P. Horodecki, & R. Horodecki, *Phys. Lett. A* **223**, 1 (1996).

[48] P. Horodecki, *Phys. Lett. A* **232**, 333 (1997).

[49] M. Horodecki, P. Horodecki, & R. Horodecki, *Phys. Rev. Lett.* **84**, 2014 (2000).

[50] L. P. Hughston, R. Jozsa, & W. K. Wootters, *Phys. Lett. A* **183**, 14 (1993).

[51] C. J. Isham, *Lectures on Quantum Theory* (Imperial College Press, London, 1995), p. 168.

[52] P. Jacquod & D. L. Shepelyansky, *Phys. Rev. Lett.* **79**, 1837 (1997).

[53] A. Jamiołkowski, *Rep. Math. Phys.* **3**, 275 (1972).

[54] G. L. Kamta & A. F. Starace, *Phys. Rev. Lett.* **88**, 107901 (2002).

[55] M. Karbach & G. Müller, *e-print cond-mat/9809162*.

[56] Y. H. Kim & Y Shih, *Found. Phys.*, **29**, 1849 (1999).

[57] J. Lee, H. Min, & S. D. Oh, *Phys. Rev. A* **66**, 052318 (2002).

[58] H. W. Lee, *Phys. Rev. A* **64**, 014302 (2001) e referências lá contidas.

[59] M. B. Mensky, *Quantum Measurements and Decoherence* (Kluwer Academic Publishers, Dordrecht, 2000). Cap. 1, Sec. 1.3.

[60] A. M. L. Messiah & O. W. Greenberg, *Phys. Rev.*, **136**, B248 (1964).

[61] P. A. Miller & S. Sarkar, *Phys. Rev. E* **60**, 1542 (1999).

[62] M. A. Nielsen, Tese de Doutoramento, University of New Mexico, 1998 (quant-ph/0011036).

[63] M. A. Nielsen & I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[64] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs, & A. Zeilinger, *Phys. Rev. Lett.* **86**, 4435 (2001).

[65] A. Peres, *Phys. Rev. Lett.* **77**, 1413 (1996).

[66] S. Popescu & D. Rohrlich, *Phys. Lett. A* **166**, 293 (1992).

[67] K. R. Popper, *Quantum Theory and the Schism in Physics* (Hutchinson, London, 1982).

[68] J. Preskill, *Lectures notes for Physics 229: Quantum Information and Computation* (California Institute of Technology, 1998). Cap. 4, Sec. 2.

[69] E. M. Rains, *Phys. Rev. A* **60**, 179 (1999).

[70] G. Rigolin, *Found. Phys. Lett.* **15**, 293 (2002).

[71] G. Rigolin, *eprint quant-ph/0105057.*

[72] G. Rigolin & C. O. Escobar, *eprint quant-ph/0206044.*

[73] G. Rigolin & C. O. Escobar, *Phys. Rev. A* **69**, 012307 (2004).

[74] G. Rigolin, *Int. J. Quant. Inf.* **2**, 393 (2004).

[75] G. Rigolin, *eprint quant-ph/0407193.*

[76] G. Rigolin, *Phys. Rev. A* **71**, 032303 (2005).

[77] L. F. Santos & G. Rigolin, *Phys. Rev. A* **71**, 032321 (2005).

[78] L. F. Santos, G. Rigolin, & C. O. Escobar, *Phys. Rev. A* **69**, 042304 (2004).

[79] L. F. Santos, *J. Phys. A: Math. Gen.* **37**, 4723 (2004).

[80] L. F. Santos, *Phys. Rev. A* **67**, 062306 (2003).

[81] L. F. Santos & M. I. Dykman, *Phys. Rev. B* **68**, 214410 (2003).

[82] E. Schrödinger, *Proc. Camb. Phil. Soc.* **31**, 555 (1935).

[83] B. L. Schumaker & C. M. Caves, *Phys. Rev. A* **31**, 3093 (1985).

[84] P. W. Shor, *SIAM J. Sci. Statist. Comput.* **26**, 1484 (1997) (quant--ph/9508027).

[85] A. J. Short, *Found. Phys.*, **14**, 275 (2001).

[86] R. Simon, E. C. G. Sudarshan, & N. Mukunda *Phys. Rev. A* **36**, 3868 (1987).

[87] R. Simon, N. Mukunda, & B. Dutta, *Phys. Rev. A* **49**, 1567 (1994).

[88] R. Simon, *Phys. Rev. Lett.* **84**, 2726 (2000).

[89] E. Strømer, *Acta. Math.* **110**, 233 (1963).

[90] Y. Sun, Y. Chen, & H. Chen, *Phys. Rev. A* **68**, 044301 (2003).

[91] A. C. de la Torre, P. Catuogno, & S. Ferrando, *Found. Phys. Lett.* **2**, 235 (1989).

[92] V. Vedral, M. B. Plenio, M. A. Rippin, & P. L. Knight, *Phys. Rev. Lett.* **78**, 2275 (1997).

[93] V. Vedral, M. B. Plenio, K. Jacobs, & P. L. Knight, *Phys. Rev. A* **56**, 4452 (1997).

[94] X. Wang, *Phys. Rev. A* **64**, 012313 (2001).

[95] R. F. Werner, *Phys. Rev. A* **40**, 4277 (1989).

[96] J. Williamson, *Am. J. Math.* **58**, 141 (1936).

[97] A. Wong & N. Christensen, *Phys. Rev. A* **63**, 044301 (2001).

[98] W. K. Wootters & W. H. Zurek, *Nature* **299** 802 (1982); D. Dieks, *Phys. Lett. A* **92** 271 (1982).

[99] W. K. Wootters, *Phys. Rev. Lett.* **80**, 2245 (1998).

[100] S. L. Woronowicz, *Rep. Math. Phys.* **10**, 165 (1976).

[101] C. N. Yang & C. P. Yang, *Phys. Rev.* **150**, 321, 327 (1966).

[102] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, & J.-W. Pan, *Nature* **430**, 54 (2004).

[103] V. Zelevinsky, M. Horoi, & B. A. Brown, *Phys. Lett. B* **350**, 141 (1995).