Emaranhamento: dos Gatos de Schrödinger à Álgebra Multilinear [1]

Marcelo de O. Terra Cunha
Departamento de Matemática - UFMG

18 de Outubro de 2004

[1]Texto referente ao minicurso a ser apresentado na II Bienal da SBM - Salvador, 25 a 29/10/2004

Introdução

O Emaranhamento

A Mecânica Quântica teve uma gestação de cerca de 25 anos, desde o primeiro trabalho de Plank, em 1900, até assumir uma forma axiomática na década de 20. Nesse período de gestação merecem destaque especial os nome de Einstein, de Broglie, Schrödinger, Bohr e Sommerfeld. Na axiomatização, que pode ser considerado o nascimento da teoria, os destaques são Bohr, Heisenberg, Jordan, Pauli e Dirac.

Seguiram-se dez anos que podem ser considerados a infância da teoria: havia muitos problemas a serem resolvidos e um novo arcabouço teórico a ser utilizado. O crescimento e o sucesso da teoria foram espantosos. Para se ter uma idéia, alguns dos Prêmios Nobel da época: Plank (18), Einstein (21), Bohr (22), de Broglie (29), Heisenberg (32) e Dirac e Schrödinger (33). O estudo da física atômica, molecular, nuclear, da matéria condensada, dos gases, da interação com a radiação foram revolucionadas pela Mecânica Quântica, com todas essas áreas tendo trabalhos seminais neste época.

Em 1935 podemos dizer que a Teoria Quântica chega à adolescência. Einstein, Podolski e Rosen apresentam seu famoso "paradoxo" em um trabalho que pergunta[8]: "Pode a Mecânica Quântica ser considerada uma teoria completa?". Na opinião dos autores, *não*. Inspirado neste trabalho, Schrödinger cria sua famosa metáfora do *gato*, ao qual também deveria se aplicar a Mecânica Quântica. Porém, lembra Schrödinger, não temos qualquer registro de observação de algo que possa ser interpretado como um gato em uma *superposição* de estado "vivo" e "morto". Com a leitura do texto, deve se tornar claro para o leitor a que se refere o termo "superposição," em particular deve se entender que não se trata simplesmente de um gato 50% vivo e 50% morto, para o que podemos fazer uma descrição clássica.

Essa revolta "adolescente" gerou muita discussão (o que é natural), bem como algumas feridas. A maior parte da comunidade física passou a se dedicar a aplicar a mecânica quântica aos problemas, sem se dedicar por demais às questões levantadas por alguns de seus fundadores; enquanto uma pequena parcela passou a se dedicar demais a essas questões, por vezes sem se aprofundar o suficiente na própria mecânica quântica. Curiosamente, o trabalho de Bohm[11] parece ter aumentado tal separação. A situação muda quando Bell[12], já na década de 60, consegue colocar esta discussão (que dependia mais de opiniões que de critérios científicos) em termos quantitativos, criando as chamadas *desigualdades de Bell*, que teorias resultantes de alguns de nossos "preconceitos" clássicos deveriam obedecer, mas a mecânica quântica viola.

Este não foi um fim para a discussão, mas ao menos permitiu trazer de volta ao debate as diferentes concepções de teoria e realidade. A década de 80 trouxe para o laboratório a questão da *não-localidade*, viva ainda hoje, pois cada experimento de "violação de desigualdades de Bell" é seguido por alguns contra-argumentos sobre situações não completamente controladas e que podem afetar os resultados.

Mas foi também no último quarto do século XX que a revolta adolescente deu lugar a uma maturidade da meia-idade. Ao invés de se questionar se a teoria possui não-localidade, se isso é desejável sob diversos pontos de vista... a questão se tornou: será que esta não-localidade pode ser útil? Será que alguma tarefa pode ser melhor realizada usando as características da mecânica quântica do que com os métodos clássicos? Assim, o *emaranhamento*, termo criado por Schrödinger para descrever o estado das partículas de Einstein, Podolski e Rosen, passava de vilão a mocinho.

Atualmente já se sabe que a mecânica quântica pode sim ser utilizada de maneira vantajosa em diversas tarefas de processamento da informação. Assim surgiu a Teoria Quântica da Informação. O emaranhamento é personagem central nesta teoria, mas como bom personagem, ainda guarda mistérios. Não existe ainda uma teoria completa sobre o emaranhamento!

O intuito deste minicurso é apresentar para a comunidade matemática (e interessada em matemática) que a questão do emaranhamento é um problema em álgebra multilinear. Que não é preciso o conhecimento profundo de mecânica quântica para participar da busca pela compreensão deste conceito. E que, por se tratar de um problema razoavelmente recente, com origem na teoria quântica da informação, tem sido proeminentemente abordado por físicos e cientistas de computação, quando matemáticos possuem um grande potencial de contribuição na área.

O Texto

O capítulo que se segue é, de fato, a versão atual (18 de outubro de 2004) do primeiro capítulo de minha Tese de Doutorado, a ser defendida nos próximos meses. Este capítulo tem por intuito apresentar e fixar os conceitos envolvidos no problema da caracterização do emaranhamento. O objetivo central foi apresentar e discutir os conceitos com a profundidade desejada a uma Tese, mas tendo em mente que o leitor tanto podia ser um físico, quanto alguém que não conhecesse mecânica quântica. O minicurso poderá ser visto como uma via de acesso rápido a este texto, enquanto o texto se propõe a ser a via de acesso rápido ao problema. Embora pudesse ser desejável um texto "mais didático", incluindo exercícios, por exemplo, essa nunca foi a intenção, neste caso. Nas três primeira secções, o pouco que há de original são os comentários e a forma de apresentação. Já a última secção é, na presente versão, inteiramente destinada a descrever uma contribuição original, desenvolvida na UFMG, em colaboração com dois estudantes: Daniel Cavalcanti e Leandro Cioletti. Acima de tudo, este texto é um convite à pesquisa no assunto. Sejam todos bem-vindos!

Conteúdo

Capítulo 1

Emaranhamento e sua Caracterização

Neste capítulo apresentamos a noção de emaranhamento de estados quânticos. A secção 1.1 fixa os conceitos centrais da teoria quântica, e deve permitir ao leitor não familiarizado com esta ter acesso ao resto do texto. Não substitui, é claro, o estudo aprofundado do assunto. O problema relativamente mais simples de caracterizar o emaranhamento de estados puros é tratado na secção 1.2. Para sistemas bipartites, a decomposição de Schmidt é a ferramenta central. Medidas entrópicas do emaranhamento são apresentadas. O importante caso de dois qubits é discutido e os problemas relativos a dimensões mais altas são apontados. Sistemas com mais de duas partes exibem correlações ainda mais interessantes. Em particular, mostra-se que para três qubits existem *diferentes emaranhamentos*. A secção 1.3 trata do emaranhamento de estados mistos, um problema ainda mais rico. A noção de separabilidade é apresentada e alguns critérios são discutidos. O emaranhamento de formação é também apresentado, bem como o conceito de destilação do emaranhamento de um estado quântico. Particular atenção é dada ao processo de *tomografia quântica*, pelo qual é possível "medir" (*i.e.*: caracterizar completamente) o estado de um sistema. A fórmula de Wootters para o cálculo do emaranhamento de formação de sistemas de dois qubits é apresentada e as dificuldades de generalização deste resultado são discutidas. Alguns resultados interessantes sobre sistemas multipartites são apresentados e comentados, bem como alguns outros quantificadores são apresentados: entropia relativa de emaranhamento, robustez e emaranhamento testemunhado. A secção 1.4 se destina a contribuições originais apresentadas, ou em produção. Na presente versão, apresentamos o problema de determinar tomograficamente o estado puro de três qubits, com a restrição a medições em pares.

1.1 Noções Gerais

1.1.1 Testes, Estados e Probabilidades

Vamos adotar, ao longo deste texto, algumas definições do livro de Asher Peres[1]. Para este autor, o conceito de *teste quântico* é essencial: é ele que nos permite

caracterizar o *estado* de um sistema[1]. Um teste quântico é caracterizado por uma intervenção no sistema, para a qual um conjunto de respostas é permitido[2]. Se o mesmo teste for aplicado novamente, a mesma resposta deverá ser obtida. Um teste B é dito *compatível* com um teste A se a aplicação do teste B entre duas repetições do teste A não destrói a propriedade de repetição do resultado, descrita anteriormente, ou seja, a resposta ao segundo teste A é a mesma que do primeiro.

Para o leitor desacostumado, essa definição de *compatibilidade* pode parecer estranha. O conceito de *teste* também pode ser aplicado em física clássica: é assim que *ganhamos informação* sobre os sistemas. Mas o conceito de compatibilidade não é necessário classicamente, pois todos os testes clássicos são compatíveis. A cada novo teste, ganhamos *mais* informação sobre o sistema, sem nunca perdê-la por meio de testes[3]. Quanticamente, existem testes *incompatíveis*! Neste caso, a realização de um teste B entre duas realizações de um mesmo teste A permite que as duas realizações apresentem respostas distintas a e a'.

Um conjunto de testes mutuamente compatíveis $\{A_i\}$ é dito *completo* quando nenhum outro teste, essencialmente diferente dos A_i, pode ser acrescido a este conjunto, mantendo a compatibilidade. Esta definição não é fechada em si mesma, mas muito mais uma definição daquilo que está sendo considerado como o *sistema quântico* de interesse, ou seja, quais variáveis (graus de liberdade) estão sendo estudadas. Sem nenhuma vergonha de ser redundante, Peres define [1, p.24]

> *"A quantum system is whatever admits a closed dynamical description within quantum theory."*

Estamos agora em condições de definir uma *preparação*. Novamente usando palavras do autor [1, p.31]

> *"The simplest method for producing quantum systems in a given state is to subject them to a complete test, and to discard all the systems that did not yield the desired outcome."*

O estado que emerge de uma preparação como descrita por Peres é chamado um *estado puro*. A característica básica de um estado puro é a existência de uma certa quantidade de testes (*e.g.*: aqueles do conjunto completo escolhido para a preparação) para os quais ele dá uma resposta *com* 100% *de probabilidade*. Para outros testes (não compatíveis com o conjunto usado na preparação), o melhor que a mecânica quântica pode fazer é prever probabilidades para os possíveis resultados. Mais uma vez, nas palavras de Peres [1, p.13]:

---

[1] Note que esse caminho, bastante consistente, não é o usualmente adotado. É comum que os autores comecem com hipóteses do tipo: "seja o estado quântico descrito por...", enquanto Peres discute o conceito de estado.

[2] O termo *teste* é usado pelo autor em lugar de *medição* ou *medida*. Duas vantagens nesta escolha: deixar o chamado *problema da medição* para seu devido momento, evitando ciclicidade nas discussões e permitindo uma definição mais ampla para o conceito de medição; e evitar problemas com o significado matemático - totalmente distinto - da palavra *medida*.

[3] Podemos perder informação se houver interações sobre as quais não tenhamos suficiente controle, mas fazer novas perguntas a um sistema clássico não o fará "mudar a resposta" de uma pergunta anterior.

> "*In a strict sense, quantum theory is a set of rules allowing the computation of* **probabilities** *for the outcomes of tests which follow specified preparations.*"

1.1.2 Interferência, Espaços Vetoriais e Notação

Outra característica marcante da teoria quântica é o fenômeno de interferência. Em suas famosas *Lectures*, Feynman[2] inicia sua apresentação da mecânica quântica pelo experimento de fenda dupla, que em sua opinião contém *o único* mistério da mecânica quântica[4]. Este fenômeno de interferência no cálculo das *probabilidades* é que sugere o uso de *amplitudes de probabilidades*, números complexos, cujos módulos ao quadrado são as probabilidades. Se há duas (ou mais) possibilidades *indistingüíveis*[5] de se obter um resultado em um teste, as amplitudes de probabilidades de cada alternativa devem ser somadas. Essa idéia simples, mas revolucionária, descreve o fenômeno de interferência, e aponta para o chamado *Princípio de Superposição*, segundo o qual os estados puros de um sistema quântico formam um espaço vetorial sobre $\mathbb{C}$, o corpo dos números complexos[6].

Como as amplitudes são números complexos, mas apenas seus módulos são experimentalmente relevantes, dois vetores $\vec{\psi}$ e $\vec{\phi}$ tais que $\vec{\psi} = e^{i\theta}\vec{\phi}$ descrevem estados idênticos, no sentido que os testes quânticos são incapazes de distingüi-los. Além disso, a soma das probabilidades de possibilidades excludentes deve ser 1. Munindo o espaço de estados de um produto escalar hermitiano tal que as possíveis alternativas de cada teste sejam representadas por vetores ortogonais, somos levados a considerar apenas vetores unitários. Essas duas considerações mostram que, de fato, o conjunto dos estados puros é a *projetivização* do espaço (vetorial) de estados anteriormente apresentado.

Vamos adotar a notação mais usual em textos sobre mecânica quântica: a *notação de Dirac*. Esta notação é bastante conveniente quando se trabalha em um espaço vetorial complexo, V, munido de produto escalar hermitiano. Os vetores são denotados por $|\psi\rangle$, e usualmente referidos como *kets*. Todo espaço vetorial possui seu *dual*, formado pelos *funcionais* $f : \mathsf{V} \to \mathbb{C}$, lineares[4]. O dual, denotado V^*, é também um espaço vetorial sobre $\mathbb{C}$. Se $\dim \mathsf{V} = n$, então $\dim \mathsf{V}^* = n$, e portanto V e V^* são isomorfos. Mas apenas quando V é munido de um produto escalar (hermitiano, quando o espaço é complexo) é que existe um *isomorfismo canônico*. Para entender este resultado, basta lembrar que dado um vetor $|v\rangle$ e uma base arbitrária $\{|u_i\rangle\}$ para V, o problema de obter o coeficiente v_i na decomposição $|v\rangle = \sum_j v_j |u_j\rangle$ depende de todos os elementos da base, ou seja, se conhecemos apenas o vetor $|v\rangle$ e o elemento $|u_j\rangle$ da base, não é possível obter v_j; mas a situação muda de figura se V for dotado de produto escalar, e fizermos a exigência de a base $\{|u_i\rangle\}$ ser ortogonal: neste caso o coeficiente v_j depende apenas do vetor $|v\rangle$ e do elemento da base $|u_j\rangle$.

O funcional linear que associa a $|v\rangle$ o coeficiente v_j de sua decomposição é chamado o dual de $|u_j\rangle$. Na notação de Dirac, este funcional é denotado

[4] "*We choose to examine a phenomenon which is impossible,* absolutely *impossible, to explain in any classical way, and which has in it the heart of quantum mechanics. In reality, it contains the* only *mystery.*"[2, p.1-1]

[5] A questão da indistingüibilidade é central na teoria quântica, mas não será abordada aqui.

[6] Existem várias tentativas não convencionais de generalizar a teoria quântica para algo não linear. Ver, por exemplo, [3, cap.22].

$\langle u_j|$. Funcionais lineares são chamados *bras*. O produto escalar (anti-linear na primeira componente) $(|\phi\rangle, |\psi\rangle)$ ganha a notação simplificada $\langle\phi \mid \psi\rangle$, que é a justificativa dos termos mneomônicos *bra* e *ket*: juntos, nesta ordem, eles fazem um *braket*.

Se $\mathbf{A}$ é um operador linear sobre V, a matriz que representa este operador com respeito à base ortonormal[7] $\{|u_i\rangle\}$ é $(\langle u_i| \mathbf{A} |u_j\rangle)_{ij}$. Por este motivo, termos como $\langle\phi| \mathbf{O} |\psi\rangle$ são geralmente referidos como *elementos de matriz*. Os *testes*, discutidos anteriormentes, são associados a operadores hermitianos (*i.e.*: auto-adjuntos) sobre o espaço de estados.

Um operador bastante importante é dado por $|\psi\rangle\langle\psi|$, o operador de *projeção ortogonal* sobre (o espaço unidimensional gerado por) $|\psi\rangle$. Para qualquer base $\{|u_i\rangle\}$, vale a resolução da identidade $\mathbf{1} = \sum_j |u_j\rangle\langle u_j|$.

1.2 Emaranhamento de Estados Puros

"*What is entanglement?*
There are many possible answers, maybe as many as there are researchers in this field." Dagmar Bruß

Não é simples definir emaranhamento em palavras. Ao longo deste trabalho vários aspectos serão apresentados e enfatizados, tentando passar a maneira como o autor entende o conceito. É certo que o emaranhamento é uma propriedade de sistemas quânticos *compostos*, no sentido de possuir vários subsistemas. Assim, pode haver emaranhamento entre dois átomos, entre dois *spins*, entre a polarização de dois *fótons*, etc... Mais que isso, conforme a discussão sobre *sistemas quânticos* (1.1.1), é sempre necessário definir aquilo que está sendo descrito quanticamente: pode parecer estranho falar em emaranhamento para um único átomo, mas pode haver emaranhamento entre diferentes graus de liberdade de um mesmo átomo (*e.g.*: o *momentum* de um átomo pode se emaranhar com seu *spin* pela interação com um campo magnético; de fato é essa a essência do experimento de Stern-Gerlach). Salvo menção em contrário, não estaremos preocupados com qual sistema físico será descrito, e sim com a estrutura matemática decorrente de tal descrição.

1.2.1 Sistemas Bipartites

O caso mais simples de sistema quântico onde pode haver emaranhamento é o de um sistema bipartite. Por influência da Teoria da Informação, chamaremos cada *parte* por um nome: *Ana* e *Bernardo*[8]. Se Ana consegue descrever a sua parte do sistema por um estado puro $|a\rangle$, enquanto Bernardo descreve sua parte por $|b\rangle$, temos uma descrição do sistema global por um estado puro, que denotaremos $|a, b\rangle$. O Princípio de Superposição implica que o espaço de estados E para o sistema global é o *produto tensorial* dos espaços de estados das partes: $\mathsf{E} = \mathsf{E}_A \otimes \mathsf{E}_B$. Uma maneira operacional de construir E é escolher bases $\{|a_i\rangle\}$ de E_A e $\{|b_j\rangle\}$ de E_B e definir E como o espaço vetorial gerado pelos vetores ortonormais $\{|a_i, b_j\rangle\}$. Com essa construção é imediato que a dimensão de E é o produto das dimensões dos fatores E_A e E_B.

[7] Salvo menção em contrário, o termo base será usado com o significado base ortonormal ao longo deste trabalho.

[8] Nos textos de língua inglesa, os personagens usuais são *Alice* e *Bob*.

Estamos agora em condições de apresentar uma primeira definição de emaranhamento. Seja E um espaço vetorial com estrutura de produto tensorial: $\mathsf{E} = \mathsf{E}_A \otimes \mathsf{E}_B$. Um vetor $|\Psi\rangle \in \mathsf{E}$ é dito *fatorável* se $|\Psi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$. Se tal decomposição não for possível, $|\Psi\rangle$ é dito *emaranhado*[9]. Uma maneira mais física de ver tal definição é dizer que um estado puro do sistema global é fatorável quando cada parte pode ser descrita por um estado puro.

Qualquer intervenção realizada em apenas uma das partes é dita uma *operação local*. A justificativa para tal nomenclatura é que podemos pensar em casos onde Ana e Bernardo estejam afastados espacialmente; mas é importante frisar que isso não é uma exigência geral. Através de "canais clássicos" de comunicação (telefone, correio eletrônico, publicação em jornal...), Ana e Bernardo podem "combinar" uma seqüência de operações locais. Uma seqüência assim pode envolver testes em uma das partes, com posterior manipulação da outra parte de uma forma que dependa dos resultados de testes anteriores, novas manipulações em ambas as partes... o que quer que seja, sem envolver um "canal quântico", ou seja, sem permitir a interação direta das partes, ou ainda a interação de ambas com outros sistemas quânticos. Processos assim são chamados *operações locais com comunicação clássica*, com a sigla em inglês LOCC. É uma premissa geralmente aceita que LOCC não pode gerar emaranhamento. Pode sim gerar correlações, mas de uma maneira que pode ser descrita classicamente. Voltaremos a este tema na subsecção 1.3.3.

A Decomposição de Schmidt

Antes de discutirmos exemplos específicos, vamos apresentar uma ferramenta essencial para o estudo do emaranhamento em estados puros de sistemas bipartites: a *decomposição de Schmidt*.

Seja W um espaço vetorial com estrutura de produto tensorial: $\mathsf{W} = \mathsf{U} \otimes \mathsf{V}$. Sejam $\dim \mathsf{U} = m$ e $\dim \mathsf{V} = n$, e sem perda de generalidade consideremos $m \leq n$. Para cada vetor unitário $|\Psi\rangle \in \mathsf{W}$ existem bases ortonormais $\{|u_i\rangle\}$ de U e $\{|v_j\rangle\}$ de V tais que

$$|\Psi\rangle = \sum_{k=1}^{m} \lambda_k |u_k\rangle \otimes |v_k\rangle \,, \tag{1.1}$$

onde $\lambda_k > 0$ e $\sum \lambda_k^2 = 1$.

Três demonstrações distintas podem ser encontradas nas referências [1, 5, 6]. Os coeficientes λ_k são chamados *coeficientes de Schmidt* e as bases $\{|u_i\rangle\}$ e $\{|v_j\rangle\}$ são *bases de Schmidt* para o vetor $|\Psi\rangle$. O número de coeficientes de Schmidt necessários para descrever um estado puro, chamado *número de Schmidt*, é uma forma de quantificar o emaranhamento[10][7] presente no estado puro $|\Psi\rangle$. Claramente, um estado puro é fatorável se, e somente se, seu número de Schmidt é 1. Por outro lado, o número de Schmidt de qualquer vetor de W está limitado superiormente por m, a dimensão da menor parte. Genericamente, a menos de escolhas de fases, a decomposição de Schmidt (1.1) é única. As exceções, que

[9] Matematicamente também são usados os termos *decomponível* em lugar de fatorado, e *não-decomponível* em lugar de emaranhado. Embora matematicamente precisos, não usaremos tais termos aqui.

[10] Uma forma um pouco grosseira, pois semi-contínua inferiormente. Critérios gerais para quantificadores de emaranhamento serão apresentados e discutidos na subsecção 1.3.2.

aparecem quando há igualdade entre dois ou mais coeficientes de Schmidt, são, porém, casos de particular importância (*e.g.*: o estado de Einstein-Podolski-Rosen-Bohm (EPRB)[8, 9], que será discutido mais adiante).

Como discutido, operações locais devem ser desimportantes no que se refere a emaranhamento. Operações locais podem levar qualquer base de Schmidt em outra base ortonormal. Assim, as propriedades de emaranhamento para um estado puro de um sistema bipartite estão inteiramente contidas no conjunto dos seus coeficientes de Schmidt (chamado *espectro de Schmidt*). Uma ordem parcial pode ser definida no conjunto dos vetores unitários de W, levando em conta seus espectros de Schmidt. Para isso, vamos ordenar os coeficientes de Schmidt em ordem decrescente, e definir:

$$\Psi \preceq \Phi \Leftrightarrow \sum_{k=1}^{r} \lambda_i^2 (\Psi) \geq \sum_{k=1}^{r} \lambda_i^2 (\Phi), \forall r. \tag{1.2}$$

Se $\Psi \preceq \Phi$, então $|\Psi\rangle$ é menos emaranhado que $|\Phi\rangle$, no sentido que LOCC podem levar $|\Phi\rangle$ a $|\Psi\rangle$. Em particular, estados fatoráveis são menos emaranhados (segundo esta relação de ordem) que quaisquer outros estados. É importante frisar que existem estados não comparáveis, como por exemplo aqueles que possuem os seguintes espectros de Schmidt: $\left\{\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right\}$ e $\left\{\frac{\sqrt{3}}{2}, \frac{1}{2\sqrt{2}}, \frac{1}{2\sqrt{2}}\right\}$.

Dois Qubits: um pouco de história

O menor espaço vetorial que admite estrutura não-trivial de produto tensorial tem dimensão 4: $\mathbb{C}^4 \cong \mathbb{C}^2 \otimes \mathbb{C}^2$. Por influência da Teoria de Informação, tornou-se usual designar um sistema quântico cujo espaço de estados é bidimensional por *qubit*, corruptela de *quantum bit*, ou seja, o análogo quântico de um registrador binário, a unidade básica de informação usualmente considerada. Para mais detalhes, ver, por exemplo, a ref. [5]. Vamos adotar a notação usual para qubits, onde o espaço de estados é gerado por $\{|0\rangle, |1\rangle\}$. Assim, a base produto para o espaço de dois qubits é dada por $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Mesmo com um espaço de estados razoavelmente simples, o emaranhamento já se mostra importante neste sistema. Uma simplificação do estado utilizado por Einstein, Podolski e Rosen em seu famoso trabalho de 1935[8] foi discutido por Bohm em seu livro de mecânica quântica[9]. Na notação de qubits, este estado é dado por

$$|EPRB\rangle = \frac{1}{\sqrt{2}} \{|01\rangle - |10\rangle\}. \tag{1.3}$$

Com relação à ordem parcial 1.2, este estado é *maximamente emaranhado*. Como o número de Schmidt para este sistema não pode ser superior a 2, segue que a ordem parcial 1.2 é completa neste exemplo, *i.e.*: dados dois estados $|\Psi\rangle$ e $|\Phi\rangle$, ou $\Psi \preceq \Phi$, ou $\Phi \preceq \Psi$, e se as duas condições são verdadeiras, ambos têm o mesmo espectro de Schmidt e portanto podem ser levados um ao outro por operações locais (unitárias, nesse caso).

Desde os primeiros tempos da teoria quântica, vários físicos importantes (Einstein, Schrödinger e de Broglie, para citar poucos) acreditavam que o caráter probabilístico intrínseco da teoria deveria apenas refletir a nossa falta de conhecimento sobre a *real* situação. Deveria haver outra descrição mais profunda da situação física, e esta deveria ser determinística, como a relação entre a mecânica

clássica, determinística, e a mecânica estatística, naturalmente probabilística, mas onde as probabilidades surgem como efeito da impossibilidade (prática e mesmo teórica, mesmo não havendo nada como relações de incerteza) de se descrever com precisão arbitrária todos os graus de liberdade de um sistema macroscópico.

Logo nos primeiros tempos, von Neumann apresentou uma demonstração da impossibilidade de se complementar a descrição de um estado quântico com as chamadas *variáveis escondidas* (em inglês, *hidden variables*)[10]. Mas em 1952, Bohm apresentou uma maneira bastante natural de incluir variáveis escondidas[11] na descrição de sistemas quânticos que possuem análogo clássico[11]. Mais uma década se passou até Bell apontar uma hipótese tácita da demonstração de von Neumann, que invalida sua conclusão[12].

O mesmo John Bell inaugurou outro caminho[13]. Ao invés de procurar contradições com outros aspectos teóricos, Bell buscou estabelecer condições que deveriam ser satisfeitas pela estatística de resultados, para que estes pudessem ser explicados por uma teoria de variáveis "escondidas" que obedecessem condições que ficaram conhecidas como *realismo local*. Surgem então as desigualdades de Bell, que ao longo dos anos ganharam várias versões (*e.g.*: ref. [14]). Há toda uma linha de pesquisa relacionada a definir quais tipos de teorias de variáveis escondidas são excluídas por cada tipo de resultado experimental, mas não pretendemos prosseguir por esse tema.

Dois Qubits: um pouco de geometria

Vamos adotar um ponto de vista um pouco mais geométrico neste trecho, mas vamos evitar o jargão técnico, em benefício do leitor. A referência básica é o artigo de Brody e Hughstone[15], que faz um apanhado da chamada *Mecânica Quântica Geométrica*[12].

Conforme discutido em 1.1.2, devemos trabalhar na projetivização do espaço de estados, visto que só consideramos estados normalizados e fases globais são irrelevantes. Para um qubit devemos trabalhar na projetivização de $\mathbb{C}^2$, usualmente denotado $\mathbb{P}^1$. Esta variedade tem dimensão complexa 1 e é homeomomorfa à superfície esférica de dimensão real 2, S^2. É fácil enxergar isto se usamos a seguinte parametrização para os estados puros de um qubit

$$|\psi(\theta,\phi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\mathrm{sen}\frac{\theta}{2}|1\rangle\,, \tag{1.4}$$

e em mecânica quântica é comum chamar esta esfera de estados puros de *esfera de Bloch*. Já para o espaço de dois qubits, temos o vetorial $\mathbb{C}^4$, com projetivo $\mathbb{P}^3$, uma variedade de dimensão complexa 3, que corresponde a dimensão real 6. Os estados fatoráveis de dois qubits estão em correspondência biunívoca com pares de estados de um qubit, portanto a variedade de estados fatoráveis corresponde a um produto cartesiano $\mathbb{P}^1 \times \mathbb{P}^1 \subset \mathbb{P}^3$. De fato, a construção de produtos cartesianos de projetivos e a sua imersão em projetivos de dimensão maior é um

[11] John Bell, um admirador do trabalho de David Bohm, sempre se opôs à denominação variáveis *escondidas*, pois são justamente elas que se manifestam experimentalmente a cada teste (segundo esta interpretação não-canônica da mecânica quântica).

[12] Não se deve confundir *Mecânica Quântica Geométrica* (*Geometric Quantum Mechanics*) com *Quantização Geométrica* (*Geometric Quantization*). Enquanto a primeira parte do espaço de estados usual da mecânica quântica, a segunda inicia pelo espaço de fase da mecânica clássica, com sua estrutura simplética.

resultado clássico da geometria algébrica, conhecido como *Produto de Serre*[16, 17]. Os estados fatoráveis constituem uma subvariedade de dimensão complexa 2, e portanto co-dimensão 1, no conjunto de todos os estados puros. Uma conseqüência disso é que, com respeito a qualquer medida regular, o conjunto de estados fatoráveis tem medida nula e fatorabilidade é uma propriedade rara em estados puros de sistemas bipartites. Dito de outra forma, se escolhermos ao acaso um estado puro de dois qubits, este estado será emaranhado com probabilidade[13] 1! É hora então de tentarmos quantificar o emaranhamento de sistemas bipartites, em especial de dois qubits.

Medidas entrópicas de emaranhamento

Desde o século XIX é comum buscar-se *entropias* para quantificar a desordem de um sistema. Como será discutido mais adiante, uma das maneiras do emaranhamento se manifestar é em termos da desordem das partes. No contexto de estados puros, vamos apenas definir uma medida (no sentido de quantificação) entrópica de emaranhamento a partir do espectro de Schmidt $\{\lambda_i\}$ do estado $|\Psi\rangle$. Como já vimos na definição do ordenamento (1.2), são os quadrados desses coeficientes que são considerados. De fato, como são números positivos e de soma 1, podemos dar uma interpretação probabilística a estes números. Vamos usar então como medida entrópica

$$E(\Psi) = -\sum_i \lambda_i^2 \log_2 \lambda_i^2. \tag{1.5}$$

Essa expressão é essencialmente a entropia de Boltzmann para a distribuição de probabilidades $\left\{\lambda_i^2\right\}$, com a única diferença do logaritmo ser calculado na base 2. Essa escolha pode ser vista de duas formas[14]: ou como influência da teoria da informação, onde todos os logaritmos são calculados nesta base; ou por efeito de normalização, visto que o estado $|EPRB\rangle$ tem $E(EPRB) = 1$. De fato, a definição termodinâmica de entropia dá a esta a dimensão de energia. Boltzmann, em sua derivação estatística, usou a constante que hoje tem seu nome para fazer a ligação entre os dois conceitos. Nas teorias de informação e de probabilidades, porém, é mais natural considerar entropias como grandezas adimensionais. A definição aqui dá ao estado de Einstein-Podolsky-Rosen-Bohm uma unidade de emaranhamento, e muitas vezes esta unidade é definida como um *ebit*, do inglês *entanglement bit*.

Quantificações de emaranhamento são desejadas por dois principais motivos: primeiro para responder à questão se um estado tem mais emaranhamento que outro; segundo porque as aplicações práticas do emaranhamento vêem essa grandeza como um *recurso* (do inglês, *resource*) a ser utilizado, onde cada aplicação precisaria de uma determinada *quantidade* deste recurso[15]. Para essa segunda motivação, pode ser mais interessante definir outras maneiras de quantificar, mais diretamente ligadas à aplicação que se queira dar ao emaranhamento. Já

[13] O leitor deve lembrar que probabilidade zero não significa que um evento seja impossível. Um exemplo é a probabilidade de obter um dado número real em um sorteio honesto no intervalo $[0, 1]$.

[14] Com essa escolha, e a interpretação da teoria da informação, esta é a chamada *entropia de Shannon*. Para uma excelente introdução a este aspecto da entropia, veja ref. [5, cap. 11].

[15] Vale pensar na analogia com o combustível de um automóvel, onde para cada viagem precisa-se de uma quantidade definida de combustível.

para a questão do ordenamento, temos uma situação delicada. Como vimos, o conceito mais natural de ordem, que leva em conta todo o espectro de Schmidt, leva a um ordenamento parcial, com estados que não podem ser comparados. Essa medida entrópica vai associar a cada estado um número, implicando assim um ordenamento total. De certa forma, tornamos comparável o que era originalmente incomparável, o que traz sempre riscos. Voltaremos ao tema de medidas entrópicas quando discutirmos os chamados estados mistos.

Sistemas com mais Dimensões

Enquanto trabalhamos com estados puros de sistemas bipartites, a decomposição de Schmidt nos diz que, efetivamente, só precisamos considerar dois espaços de mesma dimensão. Em termos geométricos, temos novamente um produto de Serre. Se cada parte for um espaço vetorial de dimensão $m+1$, os estados fatoráveis corresponderão a $\mathbb{P}^m \times \mathbb{P}^m \subset \mathbb{P}^{m^2+2m}$, que mostra que a co-dimensão da variedade dos estados fatoráveis cresce como m^2; ou seja, para dimensões maiores, fatorabilidade (de estados puros) é ainda mais rara que para dois qubits.

Para $m \geq 2$, a ordem apresentada na expressão (1.2) é parcial. Porém, sempre que tivermos dimensão finita, existe o conceito de "(a classe de equivalência do) estado mais emaranhado" para aquele espaço. Este é dado por

$$|\Psi\rangle = \frac{1}{\sqrt{m+1}} \sum_{i=0}^{m} |i\rangle_A \otimes |i\rangle_B \,, \tag{1.6}$$

já escrito em sua decomposição de Schmidt, que apresenta o maior número possível de termos, e todos com o mesmo coeficente[16].

Um caso particular interessante é para $m = 3$, caso em que podemos considerar que Ana e Bernardo compartilham dois pares de qubits[17]. O estado com máximo de emaranhamento é

$$|\Psi\rangle = \frac{1}{2} \left\{ |0_A 0_B\rangle + |1_A 1_B\rangle + |2_A 2_B\rangle + |3_A 3_B\rangle \right\}, \tag{1.7}$$

e pela quantificação (1.5) possui 2 *ebits* de emaranhamento. De fato, o estado (1.7) corresponde a considerar cada um dos dois pares maximamente emaranhado, portanto dois pares, cada qual com 1 *ebit*. Mais explicitamente:

$$|\Psi\rangle \equiv \left\{ \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle + |1_A 1_B\rangle \right) \right\} \otimes \left\{ \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle + |1_A 1_B\rangle \right) \right\}, \tag{1.8}$$

onde o produto tensorial explicitado é feito em cada parte. Este resultado tem generalização imediata para os casos onde os espaços de estados de Ana e Bernardo possuem dimensão 2^n, e seu estado maximamente emaranhado possui n *ebits* de emaranhamento.

[16] Vale comparar com probabilidades: para um espaço amostral finito, a distribuição de probabilidade que contém menos *informação* é aquela que dá probabilidades iguais a todos os possíveis eventos.

[17] A noção de compartilhar pares de qubits sempre significa que cada parte possui um membro de cada par.

1.2.2 Sistemas Multipartites

Para sistemas com mais que duas partes, o problema torna-se ainda mais delicado. Uma primeira questão é que pode haver emaranhamento entre algumas partes, deixando outras de lado. Por exemplo, para três qubits, podemos ter um par EPRB entre os dois primeiros, fatorado do terceiro. É claro que há emaranhamento em um tal estado, mas este não é considerado um emaranhamento *genuíno* de três partes, visto que uma delas está fatorada. Portanto, uma primeira questão para um sistema de n partes é definir quando um estado tem emaranhamento entre todas as partes. A outra, mais difícil, é caracterizar este emaranhamento.

Nesta secção vamos dar especial atenção ao caso de três qubits, pois ele representa um bom modelo de como a complexidade do problema cresce, e de como a quantificação se torna delicada. Ao final da secção comentaremos alguns resultados conhecidos para mais que três qubits, bem como para sistemas de dimensão maior.

Três Qubits: Abordagem Geométrica

Para três qubits, o espaço de estados é isomorfo a $\mathbb{C}^8$, com projetivo $\mathbb{P}^7$. Uma subvariedade importante é a dos estados completamente fatorados, dada por um produto de Serre de três fatores: $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \subset \mathbb{P}^7$, que é uma subvariedade de dimensão complexa 3, e codimensão 4. Temos ainda três subvariedades (mutuamente) homeomorfas que representam estados com uma parte fatorada do outro par. Geometricamente elas são descritas por $\mathbb{P}^3 \times \mathbb{P}^1 \subset \mathbb{P}^7$, variedades de dimensão complexa 4 e codimensão 3. Um interessante resultado é que a intersecção de quaisquer duas dessas é a variedade dos estados completamente fatorados. Por fim, qualquer estado que não faz parte de nenhuma das subvariedades já descritas apresenta emaranhamento genuíno entre as três partes. Novamente, o conjunto dos estados emaranhandos é um aberto denso do conjunto de todos os estados puros, mostrando que o emaranhamento genuíno é uma propriedade genérica dos estados puros de três qubits. Esse resultado se generaliza para sistemas multipartite quaisquer.

Um resultado recente e interessante[18] é que, para três qubits em um estado puro genérico, basta conhecer os resultados de testes envolvendo pares de qubits para conhecer unicamente o estado do sistema. Na secção 1.3 poderemos discutir este resultado com mais detalhes, usando o conceito de estado misto e na 1.4 apresentar uma "receita" prática para realizar esta tarefa.

Três Qubits: Estados W e GHZ

Um resultado importante, talvez não-intuitivo, e que mostra a riqueza e complexidade do conceito de emaranhamento multipartite foi apresentado por Dür, Vidal e Cirac[19]. Neste trabalho, os autores mostram que, para três qubits, existem dois estados puros totalmente distintos, no sentido que nenhum deles pode ser levado ao outro por LOCC. De fato, ambos são maximamente emaranhados, no sentido de emaranhamento genuíno de três partes, mas com aspectos

muito diferentes de emaranhamento. Exemplos destes estados são dados por

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\{|000\rangle + |111\rangle\}, \tag{1.9}$$

$$|W\rangle = \frac{1}{\sqrt{3}}\{|001\rangle + |010\rangle + |100\rangle\}, \tag{1.10}$$

onde o primeiro (1.9) é uma generalização do estado $|EPRB\rangle$ para três partículas, e já era utilizado nas discussões entre realismo local e mecânica quântica[20]. Uma característica importante do estado $|GHZ\rangle$ é que se um dos qubits for medido, os outros dois têm seus estados determinados. Por outro lado, se um qubit for perdido, o estado do par restante não apresenta emaranhamento. Já o estado $|W\rangle$ é um caso particular de um exemplo, apresentado na ref. [21]. Uma característica importante desse estado é ele "maximizar o emaranhamento de pares", em um sentido que ainda será feito preciso em 1.3.5.

Uma conseqüência imediata desse resultado é que não se deve buscar uma maneira única de quantificar o emaranhamento genuíno tripartite. *Há mais de uma forma de emaranhamento genuíno tripartite!* Há alguma discussão sobre a existência de hierarquia entre os dois tipos de emaranhamento[33], mas não abordaremos este tópico.

Voltando à descrição geométrica, as operações unitárias locais fazem com que os estados $|GHZ\rangle$ e $|W\rangle$ sejam representantes de subvariedades de dimensão complexa 3, com intersecção vazia entre elas.

Mais Qubits

Do ponto de vista geométrico, quanto mais partes forem incluídas, mais raro será um estado puro totalmente fatorado, e maior será a rede de possibilidades de emaranhamentos de algumas partes. Para quatro qubits, por exemplo, além de fatoração total e de emaranhamento genuíno, podemos ter um trio emaranhado e fatorado do qubit restante, bem como um ou dois pares emaranhados, mas fatorados do restante. Não vamos escrever tudo isso como produtos de Serre, mas isso poderia ser feito sem dificuldade.

Um recente resultado[22] mostra que, quando se tratam de quatro qubits, são possíveis nove famílias distintas de "emaranhamento" para estados puros. As aspas se devem ao fato que as classes construídas por esses autores incluem casos de emaranhamento não-genuíno.

Sistemas com mais Dimensões

Os diversos aspectos discutidos para mais qubits também se generalizam para sistemas de mais dimensões. Não vamos dar muita atenção a estes sistemas aqui. Novamente, quanto mais dimensões, mais "espaço" está disponível para o emaranhamento. Apenas como um exemplo, para três *qutrits* (sistemas com espaços de estado de dimensão complexa 3), teremos um espaço de estados de dimensão $3^3 = 27$, com projetivo $\mathbb{P}^{26}$. Os estados completamente fatorados formam uma subvariedade homeomorfa a $\mathbb{P}^2 \times \mathbb{P}^2 \times \mathbb{P}^2$, de dimensão complexa 6, enquanto estados com emaranhamento bipartite, fatorados da outra parte, formam subvariedades homeomorfas a $\mathbb{P}^8 \times \mathbb{P}^2$, de dimensão complexa 10, e portanto codimensão 16. Todos os demais estados apresentam (alguma forma de)

emaranhamento genuíno. Não há, para conhecimento deste autor, uma classificação dos diferentes emaranhamentos genuínos para este ou outros sistemas mais "complicados".

1.3 Emaranhamento de Estados Mistos

Como dito anteriormente, o problema do emaranhamento se torna ainda mais rico para estados mistos. Uma nova definição de emaranhamento se faz necessária, visto que correlações implicam não-fatorabilidade, mas correlações são parte essencial também da física clássica. O emaranhamento é então definido como uma correlação não-clássica, ou, em certo sentido, uma correlação "mais forte" que a clássica. Para prosseguir nesta discussão será necessário definir os *estados mistos*, ou *misturas estatísticas*. É o que fazemos na subsecção 1.3.1. Em seguida, na subsecção 1.3.2, poderemos definir estados *separáveis* (estados quânticos cujas correlações podem ser descritas classicamente) , e em oposição a estes, os estados *emaranhados*, retomando o problema da quantificação do emaranhamento, mas agora no contexto mais geral de estados mistos. Exemplos importantes de quantificações são apresentados na 1.3.3. Naturalmente é no caso mais simples de sistemas bipartites que mais resultados são conhecidos. Vamos discutir alguns deles na subsecção 1.3.4. A secção se encerra com mais alguns resultados sobre sistemas multipartites.

1.3.1 Estados Mistos

Estados Mistos via Projetores

Estados puros descrevem o melhor conhecimento que se pode ter de um sistema quântico. Na secção 1.1, estados puros foram tratados como vetores do espaço de estados, onde a multiplicação por um escalar não-nulo não apresentava qualquer efeito sensível pelos testes. Essa foi a justificativa para passarmos ao projetivo $\mathbb{P}^{n-1}$ em vez de permanecermos no vetorial $\mathbb{C}^n$. A mesma justificativa pode ser usada para dizermos que o que caracteriza o estado puro não é o vetor $|\psi\rangle$, e sim o subespaço vetorial que ele gera. Assim, ao invés do vetor $|\psi\rangle$, podemos usar o projetor $|\psi\rangle\langle\psi|$ para descrever um estado puro. Uma grande vantagem é que o tratamento por projetores nos permite tratar também dos estados não-puros, ou seja, estados sobre os quais não possuímos o conhecimento mais completo possível.

Uma maneira de descrever *estados mistos* é simplesmente considerar uma mistura estatística de estados puros. Ou seja, o sistema quântico que se quer descrever pode ser representado por algum estado puro $|\psi_i\rangle\langle\psi_i|$, com respectivas probabilidades[18] p_i. Neste caso, o estado do sistema deve ser considerado como a *combinação convexa* dos operadores $|\psi_i\rangle\langle\psi_i|$, dada pelas probabilidades p_i:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| . \tag{1.11}$$

O operador ρ é chamado *operador estatístico*, ou *operador densidade*. A estatística dos resultados de qualquer teste quântico realizado está descrita pelo

[18] Ou seja, os números p_i são não negativos e $\sum p_i = 1$.

operador ρ. Por exemplo, o valor esperado de um teste descrito pelo operador $\mathbf{A}$ será dado por

$$\langle A \rangle = \mathrm{Tr}\rho\mathbf{A}. \tag{1.12}$$

Como os testes são nossa fonte única de informação sobre o estado de um sistema, o operador estatístico representa a descrição mais completa que se pode dar para um estado. Isso inclui, como caso particular, os estados puros, caracterizados por ter $p_1 = 1$, caso único em que ρ é um projetor.

Um fato importante é que, se o estado do sistema não for puro, a decomposição apresentada no lado direito da equação (1.11) não é única. Ou seja, um mesmo operador estatístico pode ser descrito de diversas formas como um *ensemble* de estados puros. A menos que tenhamos alguma informação adicional sobre a preparação do estado, não há maneira física de discriminar entre essas possibilidades. Segredos podem ser escondidos em diversas formas de preparação que levem a um mesmo estado. Os primeiros protocolos de *criptografia quântica* se utilizam disso[23].

Como os operadores estatísticos foram definidos aqui como combinações convexas de projetores, segue imediatamente que tais operadores são hermitianos, positivos semi-definidos (no sentido que $\langle\psi|\,\rho\,|\psi\rangle \geq 0$ para todo $|\psi\rangle$) e de traço 1. Estes são os objetos que queremos estudar agora.

Estados como Funcionais Lineares

Um outro referencial teórico pode ser adotado para descrever os estados da mecânica quântica. Faremos aqui uma apresentação superficial por se tratar de uma maneira complementar de pensar os estados. Para mais detalhes, o leitor pode consultar a ref. [24].

Neste contexto, os primeiros objetos a serem definidos são os *observáveis*. Tais objetos formam uma *álgebra*, no sentido matemático da palavra, *i.e.*: um espaço vetorial dotado de uma estrutura adicional de uma *multiplicação* bilinear, associativa e com unidade. Denotaremos esta álgebra por $\mathcal{A}$. O corpo sobre o qual se trabalha em mecânica quântica é o corpo complexo, $\mathbb{C}$, e vamos definir uma *conjugação* em $\mathcal{A}$. A conjugação é um mapa $* : \mathcal{A} \to \mathcal{A}$ tal que:

1. $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$,
2. $(\mathbf{a}+\mathbf{b})^* = \mathbf{a}^* + \mathbf{b}^*$,
3. $(\alpha\mathbf{a})^* = \alpha^*\mathbf{a}^*$, e
4. $\mathbf{a}^{**} = \mathbf{a}$,

para todo $\mathbf{a}, \mathbf{b} \in \mathcal{A}$ e $\alpha \in \mathbb{C}$, e α^* denota o complexo conjugado (usual) de α. Uma álgebra dotada de uma conjugação é chamada uma *álgebra* $*$.

A estrutura de espaço vetorial, por si só, não permite que conceitos topológicos como continuidade e convergência sejam adotados. Para isso é preciso ter estruturas adicionais, como, por exemplo, uma *norma*. Com a norma vem o conceito de distância, e podemos adotar a *topologia métrica*. Um espaço vetorial com norma, com a propriedade que toda seqüência de Cauchy é convergente[19], é chamado um *espaço de Banach*. De uma maneira relaxada, podemos dizer

[19] Espaços topológicos tais que toda seqüência de Cauchy é convergente são chamados *completos*.

que espaços de Banach são os espaços vetoriais onde faz sentido o conceito de *vizinhança*, e ainda, onde se tomamos elementos que se tornam arbitrariamente próximos, temos uma seqüência convergente (para um elemento do espaço).

Uma *álgebra C∗* é ao mesmo tempo uma álgebra $*$ e um espaço de Banach, com as seguintes relações de compatibilidade entre a parte algébrica e a parte topológica:

1. $\|\mathbf{ab}\| \leq \|\mathbf{a}\| \, \|\mathbf{b}\|$,
2. $\|\mathbf{a}^*\| = \|\mathbf{a}\|$,
3. $\|\mathbf{aa}^*\| = \|\mathbf{a}\| \, \|\mathbf{a}^*\|$,
4. $\|\mathbf{1}\| = 1$,

onde $\mathbf{1}$ é a unidade de $\mathcal{A}$ e $\|\cdot\|$ é a notação usual para norma. Estas propriedades são importantes para garantir que a multiplicação e a conjugação sejam contínuas.

Como a álgebra C∗ dos observáveis é naturalmente um espaço vetorial, podemos definir *funcionais lineares* $\mathcal{A} \to \mathbb{C}$. Um funcional f é dito *positivo* se, e somente se, $f(\mathbf{aa}^*) \geq 0$ para todo $\mathbf{a} \in \mathcal{A}$. Um *estado* é definido como um funcional positivo sobre a álgebra dos observáveis tal que $f(\mathbf{1}) = 1$. Com essa definição, $f(\mathbf{a})$ é dito o *valor esperado* do observável $\mathbf{a}$ no estado f.

Embora reconhecidamente mais abstrata que a definição de estados trabalhada anteriormente, esta agora apresentada tem o mérito de apresentar os conceitos em uma ordem bastante peculiar e natural: primeiro vêm os observáveis, e estados são maneiras de relacionar os observáveis com os valores esperados quando medições são realizadas. Deve-se notar que é também assim que se trabalha, de maneira mais rigorosa, em *mecânica estatística*: os observáveis são funções sobre o *espaço de fase*, e os estados são funcionais sobre os observáveis, que podem ser relacionados a medidas de probabilidade sobre o espaço de fase. Neste sentido, a "única" diferença entre mecânica estatística e mecânica quântica está em suas álgebras de observáveis: enquanto na primeira tem-se uma álgebra comutativa sobre os reais, na segunda temos uma álgebra C∗ não-comutativa sobre os complexos.

A ligação entre as duas definições apresentadas segue da constatação que, se os observáveis forem dados por matrizes $n \times n$, então cada matriz $n \times n$, ρ, positiva (semi-definida), define um estado dado por $\mathbf{a} \mapsto \mathrm{Tr}(\rho\mathbf{a})$, que deve ser comparada à eq. (1.12).

Com essa nova definição, segue que combinações convexas de estados também são estados, e portanto o conjunto dos estados é um conjunto convexo. Os pontos *extremais* deste conjunto, aqueles que não podem ser escritos como combinação convexa de outros elementos, são os *estados puros*, e esta caracterização coincide com a noção anteriormente apresentada de estados puros.

Emaranhamento e Estados Reduzidos

Uma questão natural para um sistema de muitas partes é definir o estado de uma parte. Ou seja, descrever o resultado de todos os possíveis testes locais realizados sobre uma das partes. Vamos tratar desta questão usando sistemas bipartites, mas neste caso sem perder generalidade, pois sempre podemos considerar a parte que nos interessa como *uma* parte e todas as demais como *a outra*. Neste

contexto, denotaremos a parte de nosso interesse por S (de *sistema*) e a outra parte por E (de *entorno*[20]).

Supondo que o sistema global seja descrito por um estado puro, a decomposição de Schmidt pode ser adotada para escrevermos

$$|\Psi\rangle = \sum_i \lambda_i \, |\psi_i\rangle_S \otimes |\epsilon_i\rangle_E \, . \tag{1.13}$$

O projetor $|\Psi\rangle\langle\Psi|$ pode também ser usado para descrever este estado. Testes locais serão dados por operadores da forma $\mathbf{A} = \mathbf{A}_S \otimes \mathbf{1}_E$. O valor esperado destes testes será dado por

$$\begin{aligned} \langle A \rangle &= \mathrm{Tr}|\Psi\rangle\langle\Psi| \, \mathbf{A} = \langle\Psi| \, \mathbf{A} \, |\Psi\rangle = \sum_i \lambda_i^2 \, \langle\psi_i| \, \mathbf{A}_S \, |\psi_i\rangle \\ &= \mathrm{Tr}\left\{ \left(\sum_i |\psi_i\rangle \, \lambda_i^2 \, \langle\psi_i| \right) \mathbf{A}_S \right\}, \end{aligned} \tag{1.14}$$

assim, o *estado reduzido* será descrito pelo operador

$$\rho_S = \sum_i |\psi_i\rangle \, \lambda_i^2 \, \langle\psi_i| \, , \tag{1.15}$$

que está relacionado com $\rho = |\Psi\rangle\langle\Psi|$ pela operação chamada *traço parcial* (no subsistema E), que leva operadores sobre $\mathsf{E}_S \otimes \mathsf{E}_E$ em operadores sobre E_S. O operador ρ_S contém toda a informação local do sistema S, e nenhuma informação sobre suas correlações com as demais partes do sistema composto.

É importante notar a importância do espectro de Schmidt na eq. (1.15). O espectro do operador ρ_S é $\left\{\lambda_i^2\right\}$. Deve-se notar então que, para um sistema bipartite com estado global puro[21], os dois estados locais possuem espectros idênticos, e esses espectros refletem diretamente o emaranhamento entre as partes. Portanto, se temos um estado global puro, a informação sobre o emaranhamento está disponível nas partes, e quanto mais emaranhados estiverem os subsistemas, mais misturados serão seus estados reduzidos, num sentido que será feito preciso mais adiante.

Como a operação do traço parcial é linear, o argumento acima, que empregou a decomposição de Schmidt, pode imediatamente ser generalizado para estados mistos, com o traço parcial sendo o caminho para passar do estado do sistema global para o estado (parcial) de cada subsistema. É importante notar que, para estados mistos, o conhecimento dos estados parciais não determina o estado global. Agora podemos tornar um pouco mais preciso o interessante resultado de Linden, Popescu e Wootters[18], já apresentado na 1.2.2: para três qubits em estado puro $|\Psi\rangle$, a menos de um conjunto de medida nula, o conhecimento dos operadores reduzidos ρ_{AB}, ρ_{AC} e ρ_{BC} é suficiente para determinar $|\Psi\rangle$. É claro que este resultado depende da hipótese de estado global puro. Também é importante enfatizar que não seria suficiente, por exemplo, conhecer apenas os estados individuais ρ_A, ρ_B e ρ_C; ou seja, é necessário também ter informação sobre as correlações, e para este caso, as correlações de pares são suficientes.

[20] Do inglês, *environment*.

[21] É fundamental a hipótese de *estado global puro*, e essa hipótese não pode ser testada localmente.

Diósi mostra[25] ainda que, genericamente, dois pares são suficientes neste problema. Linden e Wootters discutem no caso mais geral, quanta informação sobre a partes é suficiente para determinar um estado global (puro)[26]. Voltaremos a esse tema mais adiante.

Ordenamento de Estados Mistos e Medidas Entrópicas

Uma vez que o conceito geral de estado traz consigo a idéia de *mistura estatística* de estados puros, torna-se natural querer comparar dois estados: qual é "mais misturado"? Um fato que dificulta responder esta questão é que para qualquer estado não-extremal (*i.e.*: estado não-puro) existem infinitas maneiras equivalentes de escrevê-lo como combinação convexa de extremais[22].

O conceito mais natural de ordenamento de estados (ver ref. [27]) deve, ao lado da discussão anterior sobre estados reduzidos e decomposição de Schmidt, esclarecer a relação de ordem apresentada em (1.2). Para introduzir este conceito, primeiramente notamos que, se há uma transformação unitária $\mathbf{U}$ tal que $\rho' = \mathbf{U}\rho\mathbf{U}^\dagger$, então ρ e ρ' são "igualmente misturados". Ou seja, mudam quais os estados puros que são utilizados para descrever um ou outro estado, mas a forma como eles são misturados é idêntica. Temos portanto uma relação de equivalência e agora queremos definir uma relação de ordem entre as classes de equivalência (*i.e.*: no *quociente*).

Vamos definir a relação de ordem da seguinte maneira: ρ' será *mais misturado* que ρ se existirem operadores unitários $\mathbf{U}_k$, e coeficientes $\mu_k \geq 0$, com $\sum_k \mu_k = 1$, tais que se possa escrever

$$\rho' = \sum_k \mu_k \mathbf{U}_k \rho \mathbf{U}_k^\dagger. \tag{1.16}$$

Para interpretar esta definição vamos primeiro notar que, por construção , todos os estados são mais misturados que estados puros. Portanto, a definição (1.16) diz que, dado um estado definido por seu operador densidade ρ, primeiro devemos obter todos os estados equivalentes a ρ. Serão mais misturados que ρ todos aqueles que podem ser obtidos como combinação convexa dos diversos $\mathbf{U}\rho\mathbf{U}^\dagger$, ou seja, todos os estados que podem ser descritos como misturas de estados tão misturados quanto ρ.

Pela definição (1.16), a relação de ordem dos estados depende somente do espectro de seu operador densidade (computadas as multiplicidades). Dois operadores com mesmo espectro são igualmente misturados, e uma vez colocados em ordem decrescente os autovalores r_i de ρ e r'_j de ρ', a relação de ordem (1.16) também se escreve como ρ' é mais misturado que ρ se, e somente se,

$$\sum_{i=0}^{k} r'_i \leq \sum_{i=0}^{k} r_i, \forall k, \tag{1.17}$$

que deve ser comparada com a relação (1.2), tendo em mente a ligação entre o estado parcial e a decomposição de Schmidt de um estado global (bipartite) puro.

[22] Geometricamente podemos entender este resultado como *por cada ponto interior de um disco passam infinitas cordas.*

Há um resultado muito interessante que relaciona este ordenamento a *funções convexas*[23]. Se uma função é definida usando séries de potências, ela pode ser estendida a operadores. Para o caso de operadores diagonalizáveis, o operador $f(\mathbf{A})$ tem os mesmos autovetores que $\mathbf{A}$, e os autovalores são $f(a_i)$, com a_i os autovalores de $\mathbf{A}$. Temos então o seguinte

Teorema 1 *O estado ρ' é mais misturado que ρ se, e somente se, para toda função convexa k,* $\mathrm{Tr}\{k(\rho')\} \leq \mathrm{Tr}\{k(\rho)\}$.

Uma demonstração para esse resultado é dada em [27, 2.1.15].

Uma maneira natural de buscar *quantificar desordem* é o uso de entropias. Uma das exigências naturais que são feitas sobre entropias é a convexidade[24]. O teorema aqui citado diz que um estado ρ' é mais misturado que ρ se todas as (boas) entropias que se possam utilizar concordem em dizer isto. Novamente, o cerne da questão é o fato que o ordenamento aqui proposto não é total. Existem estados para os quais não se pode dizer que um seja mais misturado que outros. Novamente, um bom exemplo são os estados dados por

$$\begin{pmatrix} \frac{1}{2} & & \\ & \frac{1}{2} & \\ & & 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} \frac{3}{4} & & \\ & \frac{1}{8} & \\ & & \frac{1}{8} \end{pmatrix}. \tag{1.18}$$

Por sua vez, como uma entropia de um estado é um número real, está-se impondo um ordenamento ao escolher uma entropia. A analogia mais natural é com projeções: ao escolher uma entropia estamos projetando um conjunto multidimensional sobre uma reta, e com isso perdemos vários de seus detalhes. O teorema (na sua parte *somente se*) diz que, no que concerne o ordenamento, se conhecermos todas as possíveis projeções, não perdemos nenhum "detalhe", ou seja, conseguimos um espécie de reconstrução tomográfica do conjunto multidimensional.

1.3.2 Sistemas Bipartites

Estados Separáveis

Já descrevemos como estados mistos podem ser obtidos como misturas estatísticas de estados puros, e como estados puros podem ser obtidos a partir de testes quânticos. Vamos agora voltar a contexto de sistemas bipartites (Ana e Bernardo) e nos perguntar: quais estados Ana e Bernardo podem preparar usando testes locais e misturas estatísticas.

Se Ana e Bernardo procedem testes locais, um estado puro fatorado $|\alpha, \beta\rangle$ é preparado. Por operações unitárias locais, qualquer estado puro fatorado pode ser preparado a partir destes, ou seja, existem procedimentos específicos que podem ser usados para que Ana e Bernardo obtenham qualquer estado puro fatorado. Se dispusermos de algum sistema honesto de sorteios, podemos criar

[23] Uma função $f : D \to \mathbb{R}$ é dita convexa se seu domínio D for um conjunto convexo e, para $x, y \in D$ e $\lambda \in [0,1]$, valer $f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda) f(y)$. Para o caso de funções diferenciáveis, isso coincide com a segunda derivada ser não-negativa em todo D. Autores diferentes usam sinais diferentes na definição de função convexa. Estamos adotando a mesma definição da ref. [27].

[24] Novamente, cuidado deve ser tomado com a questão do sinal na definição de funções convexas.

um protocolo onde os estados $|\alpha_i, \beta_i\rangle$ sejam preparados com probabilidades p_i, ou seja, qualquer estado que pode ser escrito na forma

$$\rho_{AB} = \sum_i p_i \left|\alpha_i, \beta_i\right\rangle \left\langle\alpha_i, \beta_i\right|, \tag{1.19}$$

com $p_i \geq 0$ e $\sum_i p_i = 1$, pode ser criado por Ana e Bernardo apenas com operações locais e comunicação clássica[25]. Os estados assim preparados, em geral, exibem *correlações*, ou seja, os resultados de testes locais realizados por Ana estarão correlacionados a resultados de testes locais realizados por Bernado. Mas essa correlação é clássica. Por isso, Werner classificou estes estados como *classicamente correlacionados*[28], mais uma vez no contexto de discutir quando resultados podem ser descritos por teorias de variáveis escondidas locais. Com o tempo, o adjetivo que se tornou mais usual para estes estados é *separável*, no sentido que podem ser obtidos agindo separadamente nas partes.

A pergunta natural então é: existem estados que não possam ser preparados desta forma por Ana e Bernardo? Ou seja, existem estados que não podem ser escritos na forma (1.19)? A resposta, naturalmente, é sim. Como já vimos, estados puros não podem ser obtidos como combinação convexa de outros estados puros (ou seja, eles são pontos extremais do conjunto de estados), e, como sabemos que existem estados puros não-fatoráveis, estes são exemplos de estados *não-separáveis*. O outro nome natural para estados não-separáveis é *estados emaranhados*. Dessa forma definimos emaranhamento para estados mistos.

Critérios para Separabilidade

Agora que já sabemos o que significa um estado misto ser emaranhado, a pergunta seguinte é como saber se um estado é separável ou emaranhado? A definição dada pela fórmula (1.19) pode ser comparada à definição "por épsilons e deltas" para convergência de séries. É uma definição precisa, útil em várias demonstrações, mas muito pouco prática para ser aplicada em exemplos. É o que se costumou chamar de um critério *não-operacional*. Queremos então critérios *operacionais* de separabilidade, ou seja, uma receita tal que, dado um estado ρ, a aplicação de alguns procedimentos permita uma resposta: *separável*, ou *emaranhado*, ou ainda, o que acontece para vários critérios: *não decidido*. Novamente, a comparação natural é com ferramentas como o *teste da razão* ou o *teste da raiz* para seqüências numéricas.

Uma estratégia bastante comum para obter tais critérios é demonstrar que, se ρ é separável, então possui uma certa propriedade. Assim, estados que violem esta propriedade serão emaranhados. Demonstrações assim levam a teste inconclusivos, no sentido que, se a dita propriedade for verificada, não sabemos (em geral) se o estado é ou não separável. Vamos apresentar dois interessantes exemplos de testes como esses: um que usa a chamada *transposição parcial* e outro que usa o conceito de *majoração*, comparando se os estados locais são mais ou menos misturados que o estado global.

Critério de Peres Vamos apresentar um importante critério, criado por Asher Peres[29]. Este é um *critério operacional* que testa uma propriedade

[25] A comunicação clássica é necessária pois tanto Ana quanto Bernardo precisam ser comunicados sobre o resultado do sorteio.

necessária para um estado ser separável. No trabalho original, Peres conjectura a suficiência desta condição, mas M., P. e R. Horodecki[30] demonstram que somente em dimensões muito baixas este critério é suficiente.

Tal critério parte da seguinte observação: se ρ representa um estado físico, então sua complexa conjugada[26], ρ^*, também representa um estado físico[27]. Em particular, como todo operador densidade é positivo (semi-definido), também a transposta de um operador densidade será um operador positivo.

Peres usa então a operação chamada *transposição parcial*: se

$$\rho = \sum_{m,n,\mu,\nu} \rho_{m\mu,n\nu} \left|m,\mu\right\rangle \left\langle n,\nu\right|, \tag{1.20}$$

sua *transposta parcial* (com relação ao segundo fator) é, por definição,

$$\rho^{t_2} = \sum_{m,n,\mu,\nu} \rho_{m\mu,n\nu} \left|m,\nu\right\rangle \left\langle n,\mu\right|, \tag{1.21}$$

ou seja, faz-se a transposição apenas do segundo fator do produto tensorial (os índices gregos). A transposição parcial é uma operação linear no espaço (real) dos operadores hermitianos. Considere agora um estado separável para um sistema bipartite. Então esse estado pode ser escrito como

$$\rho_{AB} = \sum_i p_i \rho_{Ai} \otimes \rho_{Bi}, \tag{1.22}$$

e sua transposta parcial será dada por

$$\rho_{AB}^{t_2} = \sum_i p_i \rho_{Ai} \otimes \rho_{Bi}^*. \tag{1.23}$$

Como ρ_{Bi}^* são operadores que também podem representar estados, a expressão de $\rho_{AB}^{t_2}$ é a de um operador positivo. Ou seja, Peres demonstrou que, se um operador densidade é separável, então sua transposta parcial[28] é positiva. Segue então o

Critério 1 (Peres) *Se a transposta parcial de ρ não for positiva, ρ é não-separável.*

Na ref. [30], os autores mostram que a propriedade essencial de que Peres se utilizou é que a transposição é um *mapa positivo que não é completamente positivo*. Nesse contexto, a palavra *mapa* é utilizada para designar um operador que age no espaço dos operadores. Ou seja, se $\mathbf{A} : \mathbb{C}^n \to \mathbb{C}^n$, então $\mathcal{M}\mathbf{A}$ também é um operador. Um mapa $\mathcal{M}$ é dito positivo quando leva operadores positivos em operadores positivos. A primeira parte do argumento que leva ao critério de Peres é para mostrar que a transposição $\mathcal{T}$ é um mapa positivo.

[26] Aqui está se fazendo apenas a conjugação complexa, e não a conjugação hermitiana. Como ρ é uma matriz hermitiana, $\rho^* = \rho^t$.

[27] É importante notar que a transposição é uma operação que depende da escolha de base que se faz. Depende, principalmente, das fases que são escolhidas para os vetores da base, assim, o mais adequado seria dizer *conjugação com respeito à base...*, mas isso ficará sempre subentendido.

[28] Com respeito ao segundo fator, mas o resultado é análogo para transposição no primeiro fator.

A definição de *mapa completamente positivo* (CP) é mais sutil. Todo operador $\mathbf{A}$ sobre V pode ser estendido ao produto tensorial $\mathsf{V} \otimes \mathsf{W}$, fazendo $\mathbf{A} \otimes \mathbf{1}$. Da mesma forma para mapas, onde o mapa 1 tem a interpretação usual da identidade. Um mapa é dito *completamente positivo* quando é positivo e sua extensão a qualquer produto tensorial é também positiva. A transposição parcial é a extensão da transposição, e a utilidade do critério de Peres vem do fato de a transposição não ser CP.

O mesmo argumento que mostra que a transposição parcial de um estado separável é um operador positivo mostra que todo mapa positivo, quando aplicado a estados separáveis, resulta em operadores positivos. Com argumentos de análise funcional, os autores demonstram que, se ρ não é separável, então existe um mapa positivo $\mathcal{M}$ tal que $\mathcal{M}\rho$ não é positivo. Com isso, obtêm o

Critério 2 (Horodecki) *Um estado ρ é separável se, e somente se, para qualquer mapa positivo $\mathcal{M}$, $\mathcal{M}\rho$ é positivo.*

Com este critério, os Horodecki mostraram que o problema de classificar mapas positivos que não são completamente positivos é muito importante para a física e para a teoria de informação quântica. Tal classificação é conhecida[30] apenas para mapas sobre operadores de $\mathbb{C}^2 \otimes \mathbb{C}^2$ e de $\mathbb{C}^3 \otimes \mathbb{C}^2$ e diz que todos os mapas positivos podem ser obtidos por mapas CP e a transposição parcial $\mathcal{T}_2 = 1 \otimes \mathcal{T}$. Com isso, o critério de Peres se mostra suficiente para esses casos. Para dimensões maiores são conhecidos exemplos de estados não-separáveis com transposta parcial positiva. Diz-se que estes estados possuem *emaranhamento preso* (do inglês *bound entanglement*), um conceito ao qual voltaremos mais adiante (1.3.3).

Critério de Nielsen e Kempe Uma abordagem bastante diferente foi dada por Nielsen e Kempe[31]. A motivação começa pela observação que, classicamente, se um sistema tem duas partes, a *desordem* do sistema global é maior que a desordem de cada parte. Uma das formas usuais de quantificar a desordem de um sistema é utilizando uma *entropia*, e a maneira quantitativa de expressar a observação anterior é que a entropia do sistema global não pode ser menor que a entropia de cada subsistema. Assim, escolhida uma entropia $S(\rho)$, define-se a *entropia condicional* por

$$S(A \mid B) = S(A, B) - S(A), \tag{1.24}$$

onde $S(A, B)$ denota a entropia conjunta, ou seja, a entropia do sistema global. A interpretação de $S(A \mid B)$ é da entropia de A, uma vez que conhecemos B[29]. Quando se trabalha com probabilidades clássicas, $S(A \mid B)$ é sempre positiva. Para estados fatoráveis, se uma entropia *extensiva* for usada, $S(A \mid B) = S(B)$, e portanto não-negativa; pela convexidade de S, para um estado separável $S(A \mid B)$ será não-negativa. Com isso, temos mais um critério para separabilidade:

Critério 3 (entrópico) *Se $S(A \mid B) < 0$, então ρ_{AB} é não-separável.*

A importância de não se escolher previamente uma entropia é que cada entropia escolhida dará resultados diferentes pelo critério entrópico. Este fato deve ser

[29] É claro que $S(B \mid A)$ pode ser definida e interpretada de maneira análoga.

comparado ao teorema 1, o que deve tornar mais natural o critério de Nielsen e Kempe que apresentamos a seguir.

O critério apresentado por Nielsen e Kempe faz uso da relação de ordem da eq. (1.16), e da observação que, para estados separáveis, o estado global ρ_{AB} é necessariamente mais misturado que os estados locais ρ_A e ρ_B. Pode então ser escrito como

Critério 4 (Nielsen e Kempe) *Se ρ_A (ou ρ_B) for mais misturado que ρ_{AB}, então ρ_{AB} é um estado não-separável.*

Vale citar que Nielsen e Kempe chamam[30] a relação de *ser mais misturado que* de *majorar*. Por este motivo, este critério é muitas vezes chamado de *critério de majoração*.

Existem vários outros critérios de separabilidade, mas que não serão abordados aqui.

Outro tópico interessante que não será abordado aqui são as diversas entropias que podem ser utilizadas. Para uma excelente introdução aos aspectos de teoria de informação relacionados à entropia de Shannon, ver ref. [5, cap. 11]. Para uma introdução ao assunto, ver ref. [32].

1.3.3 Quantificação do Emaranhamento

Uma vez que o emaranhamento pode ser visto como um recurso a ser utilizado para manipular ou transmitir informação (apresentando alguma vantagem sobre os meios "clássicos"), torna-se natural querer quantificar este recurso, ou seja, dizer quanto desse recurso está presente em um sistema físico, ou ainda quanto desse recurso está disponível para ser utilizado.

Embora esse desejo seja natural, e para várias tarefas existam quantificadores deste recurso, o próprio fato destes quantificadores serem distintos mostra que ainda não se adquiriu o conhecimento suficiente para descrever o emaranhamento em tantos detalhes. O ponto de vista aqui apresentado é que a pergunta a ser feita não é "quanto de emaranhamento existe num dado estado?", pois esta pergunta traz tacitamente consigo a idéia de ordenamento total. Como vimos, estados mistos não são completamente ordenados (sec. 1.3.1) e no tocante a emaranhamento, nem mesmo estados puros, em casos mais gerais[31], podem ser completamente ordenados segundo seu emaranhamento (sec. 1.2.1).

Ainda assim, vários resultados parciais interessantes foram obtidos, e vários quantificadores com interpretações distintas foram apresentados. Vamos descrever alguns destes. Nossa abordagem, nesta parte, estará próxima do artigo de revisão de Bruß[33]. Começamos discutindo algumas características gerais desejáveis a quantificadores de emaranhamento (bipartite), para depois apresentar alguns quantificadores conhecidos, mesmo quando não obedecem a todas essas condições.

Condições Gerais para Quantificadores

Vamos listar agora sete condições que são desejáveis para uma quantificação de emaranhamento, E. Note que, na verdade, as condições aqui feitas consideram

[30] Seguindo a tradição de alguns autores preocupados com o problema de ordenamento para probabilidades. Ver referências em [31].

[31] Excluindo o caso de dois qubits.

uma família de quantificadores $E(\mathsf{V} \otimes \mathsf{W})$, mas vamos omitir este detalhe. Em seguida discutimos o significado de cada uma delas.

1. Se ρ é separável, então $E(\rho) = 0$.

2. *Normalização*: O estado puro $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j,j\rangle$ possui emaranhamento
$$E(|\Psi\rangle\langle\Psi|) = \log d. \tag{1.25}$$

3. *Não-crescente por LOCC*: Se $\mathcal{M}$ representa um mapa que pode ser implementado por operações locais e comunicação clássica, então
$$E(\mathcal{M}\rho) \leq E(\rho). \tag{1.26}$$

4. *Continuidade*: E deve ser uma função contínua de ρ.

5. *Aditividade*: Denotamos por $\rho^{\otimes n}$ o estado de n cópias idênticas de um estado ρ (*i.e.*: o produto tensorial de n cópias de ρ). Os quantificadores E devem obedecer:
$$E\left(\rho^{\otimes n}\right) = nE(\rho). \tag{1.27}$$

6. *Subaditividade*: Se Ana e Bernardo compartilham estados ρ e σ sobre sistemas independentes, podemos dizer que eles compartilham $\rho \otimes \sigma$ e os quantificadores E devem obeder:
$$E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma). \tag{1.28}$$

7. *Convexidade*: E deve ser uma função convexa[32] no espaço dos operadores, *i.e.*:
$$E(\lambda\rho + (1-\lambda)\sigma) \leq \lambda E(\rho) + (1-\lambda) E(\sigma). \tag{1.29}$$

A condição 1 é a exigência natural que apenas estados não-separáveis possuam alguma quantidade de emaranhamento. A condição 2 é uma normalização conveniente, que escolhe como "unidade de emaranhamento" o *ebit*, e define este como a quantidade de emaranhamento presente em um par EPRB (ver subsec. 1.2.1).A condição 3 é fundamental por tudo aquilo que discutimos sobre LOCC na secção 1.2.1. A condição 4 é desejável, pois como usualmente acontece em física, as grandezas não podem ser conhecidas com precisão arbitrária. Visto de outra forma, quer-se que operações infinitesimais gerem, ou destruam, quantidade infinitesimais de emaranhamento. A condição 5 pede apenas que n cópias independentes de um estado ρ tenham n vezes a quantidade de emaranhamento de cada cópia. A condição seguinte, 6, diz que, para estados diferentes, ρ e σ, a aditividade pode ser relaxada, podendo haver menos emaranhamento em ter os dois estados do que em cada um deles, separadamente. A útima condição, 7, é compatível com a noção que combinações convexas são *mais misturadas*, e portanto menos emaranhadas, que seus estados extremais.

[32] Ver nota 23.

Emaranhamento de Formação

O *emaranhamento de formação* faz uso de dois conceitos essenciais em sua definição: (i) todo estado pode ser escrito como combinação convexa de estados puros (eq. (1.11)); (ii) uma boa quantificação de emaranhamento para estados puros (bipartites) é a *entropia de von Neumann*[33] para os estados reduzidos, dada pela expressão (1.5). O conceito (i) é um fato, já o conceito (ii) é uma escolha, que tem suas limitações, como já foi discutido.

Dado um estado ρ_{AB}, podemos decompô-lo como combinação convexa de estados puros:

$$\rho_{AB} = \sum_i \mu_i \left|\Psi_i\right\rangle \left\langle\Psi_i\right|, \tag{1.30}$$

em seguida calcular, usando a quantificação para estados puros escolhida, o emaranhamento de cada estado puro, $S\left(\Psi_i\right)$, e tomar a combinação convexa (dada pelos μ_i) destes resultados como a quantidade de emaranhamento para a decomposição (1.30):

$$\tilde{E}\left(\{\mu_i, \Psi_i\}\right) = \sum_i \mu_i S\left(\Psi_i\right). \tag{1.31}$$

O ponto importante, e aqui enfatizado até na notação, é que, se ρ_{AB} representa um estado de mistura, a decomposição (1.30) não é única. A bem da verdade, existe uma infinidade delas. Assim, se não temos qualquer informação adicional sobre o processo de preparação do estado ρ_{AB}, devemos considerar todas as possíveis decomposições[34]. O *emaranhamento de formação* é definido então como o ínfimo[35] sobre todas essas possíveis decomposições:

$$E_f\left(\rho_{AB}\right) = \inf_{\text{Decomposições}} \tilde{E}\left(\{\mu_i, \Psi_i\}\right). \tag{1.32}$$

O emaranhamento de formação é um quantificador bastante razoável para o emaranhamento. Não é sabido ainda se ele obedece às condições 5 e 6, enquanto todas as demais são satisfeitas. Porém, por envolver um processo de extremização sobre todas as possíveis decomposições de um estado (como combinação convexa de estados puros), torna-se um quantificador "não-operacional", *i.e.*: de difícil aplicação. Uma interessante exceção é o caso de dois qubits, onde existe um procedimento algorítmico para calcular o emaranhamento de formação, como será discutido na subsecção 1.3.4.

Custo de Emaranhamento

"*... fundamental measures of information arise as the answers to fundamental questions about the physical resources required to solve some information processing problem.*" M.A. Nielsen e I.L. Chuang

[33] A definição geral da entropia de von Neumann é $S\left(\rho\right) = \mathrm{Tr}\left\{\rho \log \rho\right\}$. No contexto de teoria da informação o logaritmo é calculado na base 2. Para estados reduzidos a partir de um estado puro bipartite vale a fórmula (1.5). Mais detalhes na ref. [5, cap. 11].

[34] Cada decomposição pode ser vista como um esquema de preparação para o estado ρ_{AB}, onde devemos ter estratégias para preparar os estados puros $\left|\Psi_i\right\rangle$ e fazer sorteios com probabilidades μ_i para cada resposta.

[35] Se o espaço de estados em que trabalhamos tiver dimensão finita, como usualmente é o caso em informação quântica, este ínfimo será um mínimo, e essas palavras podem ser trocadas na definição.

Passamos agora a maneiras de quantificar o emaranhamento mais próximas da teoria da informação. O primeiro exemplo que vamos tratar é o *custo de emaranhamento*, que pode ser resumido como *quantos pares EPRB Ana e Bernardo devem compartilhar para, através de LOCC, produzirem o estado* ρ_{AB}*?* Vamos agora ser mais cuidadosos e traduzir esta questão para o significado preciso do *custo de emaranhamento*, E_c.

Um ponto importante, e que não apareceu na frase resumida acima, é que trabalhamos aqui com o conceito *assintótico*. Ou seja, não queremos saber quantos pares EPRB serão necessários para produzir uma cópia do estado ρ_{AB}, mas sim a razão entre o número de pares EPRB e o número de cópias do estado ρ_{AB}, quando estes números se tornam arbitrariamente grandes. Assim, a idéia é tomar uma grande quantidade, m, de pares EPRB, e obter uma grande quantidade, n, de cópias de ρ_{AB}. Se for possível, usando LOCC, passar de $\rho_{AB}^{\otimes n}$ a $\rho_{EPRB}^{\otimes m}$ e vice-versa, teremos que estes estados têm a mesma "quantidade de emaranhamento", e usando a aditividade, concluímos que $E(\rho_{AB}) = \frac{m}{n} ebits$.

Um inconveniente da discussão anterior é que precisaríamos obter dois protocolos de LOCC, um que leva m pares EPRB em n cópias de ρ_{AB}, e outro que leva n cópias de ρ_{AB} em m pares EPRB. A definição do *custo de emaranhamento* só se preocupa com a primeira destas tarefas. Se encontramos um procedimento capaz de levar, por LOCC, $\tilde{m}$ pares EPRB em $\tilde{n}$ cópias de ρ_{AB}, saberemos que $E_c(\rho_{AB}) \leq \frac{\tilde{m}}{\tilde{n}}$. O custo de emaranhamento é então definido como o ínfimo sobre todas os possíveis protocolos de LOCC da razão $\frac{\tilde{m}}{\tilde{n}}$.

Novamente, como grande inconveniente, temos um processo de extremização em um domínio não muito simples. Neste caso, dos protocolos LOCC. Assim, o custo de emaranhamento é mais um quantificador não-operacional. Não se sabe se este quantificador é contínuo. Existe uma interessante conjectura que emaranhamento de formação e custo de emaranhamento são idênticos. Deve-se notar que, se tal conjectura for demonstrada, teremos um quantificador de emaranhamento obedecendo às sete condições desejadas, e com duas interpretações distintas e interessantes.

Destilação de Emaranhamento

Enquanto o *custo de emaranhamento* se preocupa em preparar um estado, o conceito de *destilação de emaranhamento* considerará a situação oposta: suponha uma fonte que gere o estado ρ, o que podemos fazer com este estado? Ou ainda, quantas cópias deste estado serão necessárias para realizar uma dada tarefa?

Novamente, como unidade básica de emaranhamento (bipartite) podemos considerar o *ebit* (*i.e.*: a quantidade de emaranhamento de um par EPRB). Assim, no processo de *Destilação de Emaranhamento*, que dá origem ao quantificador *emaranhamento destilável*, queremos fazer o processo assintótico de passar de $\tilde{m}$ cópias do estado ρ_{AB} para $\tilde{n}$ pares EPRB, usando protocolos de LOCC. Se existe um protocolo assim, o emaranhamento destilável, E_d, obedece $E_d \geq \frac{\tilde{n}}{\tilde{m}}$. Formalmente, definimos o *emaranhamento destilável* como o supremo sobre todos os protocolos de LOCC da razão $\frac{\tilde{n}}{\tilde{m}}$.

Como LOCC não podem aumentar o emaranhamento, compondo protocolos

$$\rho_{EPRB}^{\otimes n} \overset{custo}{\longmapsto} \rho_{AB}^{\otimes m} \text{ e } \rho_{AB}^{\otimes m} \overset{dist}{\longmapsto} \rho_{EPRB}^{\otimes n'}, \tag{1.33}$$

segue da exigência $n' \leq n$ a desigualdade $E_d \leq E_c$ para todo estado ρ_{AB}.

Já é sabido que esta desigualdade pode se tornar uma igualdade em alguns casos, como para estados puros[34] e para estados mistos de dois qubits[35]. Mas também se sabe que há casos em que a desigualdade é estrita, caso em que se diz haver *emaranhamento preso* (do inglês, *bound entanglement*[36]), ou seja, um emaranhamento que não pode ser destilado[36].

Partindo da conjectura que *custo de emaranhamento* e *emaranhamento de formação* são iguais, há uma interessante argumentação que busca explicar a existência de *emaranhamento preso*: em um processo de formação do estado ρ_{AB} devemos ser capazes de misturar os estados $|\Psi_i\rangle$ nas proporções dadas pelos μ_i, conforme a eq. (1.30); uma vez que os estados $|\Psi_i\rangle$ sejam distingüíveis, pode-se transmitir informação desde o formador do estado ρ_{AB} até o seu receptor, desde que o receptor tivesse conhecimento *a priori* dos estados $|\Psi_i\rangle$ utilizados. Essa informação não está disponível quando apenas se caracteriza o estado ρ_{AB}! Assim, usa-se mais informação na preparação de um estado não-separável do que é possível obter deste. Esse *excesso de informação* deve estar ligado ao conceito de *emaranhamento preso*.

Assim como para o custo de emaranhamento, por estar definido em termos de extremizações sobre possíveis protocolos de LOCC, não se sabe se o emaranhamento destilável depende continuamente de ρ. Há ainda uma crítica interessante de Nielsen[37] sobre estes dois quantificadores, relacionados à escolha dos estados $EPRB$ como "unidade de emaranhamento". Nielsen define o σ-custo de emaranhamento e o emaranhamento σ-destilável, e mostra que a razão entre as quantificações usuais e estes "novos padrões" não é constante, como é usual em mudanças de unidades (*e.g.*: centímetros para polegadas). O próprio Nielsen argumenta que esta crítica não é motivo para se descartar tais quantificadores, mas que esta dependência do "padrão" é mais uma propriedade que deve ser levada em conta quando buscamos compreender o emaranhamento e suas quantificações.

1.3.4 Dois Qubits

Na secção 1.2.1 discutimos com detalhes os estados puros de um sistema de dois qubits. Agora queremos tratar o problema mais geral de seus estados mistos. Lembramos (sec. 1.3.2) que para dois qubits o critério de Peres é decisivo, *i.e.*: um operador densidade ρ representa um estado separável de dois qubits se, e somente se, sua transposição parcial gera um operador positivo.

Tomografia de Spin

Durante várias décadas houve algum desconforto com a noçao de estado quântico. A crítica mais natural era que a teoria quântica usava-se do conceito de estado "apenas" como uma ferramenta intermediária, pois o que realmente era acessível, do ponto de vista experimental, eram os *testes*, que poderiam ser usados para preparar estados puros, como discutimos na 1.1.1, e os *valores esperados de observáveis*, ou seja, médias sobre muitas realizações de um mesmo experimento. Sob esse ponto de vista, o *estado quântico* não poderia ser deter-

[36] Esse nome é dado[35] com inspiração na analogia termodinâmica com o conceito de energia, onde a energia *livre* é aquela que pode ser transformada em trabalho. O emaranhamento livre seria aquele que pode ser destilado para utilização nas aplicações.

minado experimentalmente, e talvez não devesse assumir o status de elemento essencial da teoria.

Para esclarecer esta questão, primeiro devemos concordar que não se deve buscar determinar o estado de uma única realização de um sistema físico. É claro que, para obtermos informação sobre um sistema teremos que interagir com ele, e, dessa forma, após a interação, ele já não mais estará no estado que eventualmente teríamos determinado. O que é natural é caracterizar o estado que uma certa "fonte" gera, *i.e.*: em que estado átomos saem de um certo forno, em que estado fótons são emitidos em um determinado processo, ou qual o estado de um modo de campo em uma cavidade sujeita a determinados processos.

A pergunta que surge é: dada uma certa fonte de sistemas quânticos igualmente preparados, podemos obter informação suficiente sobre o estado destes sistemas de modo a preparar um estado idêntico[37] a este por um outro procedimento? Por esse motivo, esse problema ficou conhecido como *reconstrução de estados quânticos*. Do ponto de vista estritamente teórico, a pergunta é: podemos determinar todos os elementos da matriz do operador densidade com respeito a alguma base?

Neste instante vamos manter esta discussão no âmbito de espaços de estados de dimensão finita. Como o protótipo de um sistema quântico com espaço de estados de dimensão finita são *spins*, queremos tratar o problema de *reconstrução de estados quânticos de spin*. Como mostraremos, esse problema é resolvido pela técnica chamada *tomografia de spin*. Maiores detalhes podem ser encontrados na ref. [38].

Em essência, consideramos que é possível determinar, com precisão arbitrária, o valor esperado de qualquer observável do sistema. E que este valor esperado é dado por

$$\langle \mathbf{A} \rangle = \mathrm{Tr}\rho\mathbf{A}, \tag{1.34}$$

ou seja, o valor esperado de qualquer operador é uma função linear dos elementos de matriz de ρ. Tudo que se precisa, então, é escolher uma quantidade suficiente de observáveis $\mathbf{A}_i$ (usualmente chamada um *quorum*), de modo a resolvermos o sistema

$$\mathrm{Tr}\rho\mathbf{A}_i = \langle \mathbf{A}_i \rangle \tag{1.35}$$

com relação à "incógnita" ρ. Do ponto de vista de obter o mínimo de observáveis a serem medidos, para um espaço de estados de dimensão n, o operador densidade ρ é determinado por $n^2 - 1$ números reais, e portanto basta escolher $n^2 - 1$ operadores de modo que as equações (1.35) sejam linearmente independentes[38].

Antes de apresentarmos exemplos de como obter tomograficamente um estado quântico, faremos uma pequena digressão.

Digressão

Dois comentários são oportunos neste momento (mas também podem ser ignorados sem perda de continuidade). Um é sobre a noção de estado, e o outro sobre a sua determinação.

[37] Idêntico no sentido que os mesmos resultados poderão ser obtidos em medições, com as mesmas probabilidades, qualquer que seja a medição que se escolha fazer.

[38] Se lembrarmos que as medições podem ser vistas como *testes*, no sentido de Peres[1], e que podemos experimentalmente determinar as probabilidades de cada resultado de um teste, é possível reconstruir estados com um número menor de realizações experimentais do que as aqui discutidas.

Estados Quânticos De uma forma operacional, conhecer o estado quântico de um sistema é saber determinar, para qualquer observável do sistema, as probabilidades de todos os possíveis resultados de sua medição. A técnica de tomografia permite fazer o caminho contrário, e descrever completamente o estado quântico a partir das informações sobre uma certa quantidade de observáveis. Assim, podemos considerar estas informações como o estado quântico propriamente dito, ou ao menos como uma representação deste. Este ponto de vista foi adotado na década de 1990 por V. Man'ko e colaboradores[39], e permite evitar discussões como a "redução do pacote de onda" e outras questões correlatas em fundamentos de mecânica quântica.

Função de Wigner e sua Medição Para o caso do oscilador harmônico, o operador densidade é um operador sobre um espaço vetorial de dimensão infinita. Em 1932, Wigner[40] utilizou-se de uma representação para o estado como uma distribuição sobre o "espaço de fase", com variáveis p e q semelhantes às variáveis clássicas. Enquanto na descrição clássica, um estado pode ser caracterizado por uma distribuição de probabilidades, a *função de Wigner* pode, por exemplo, assumir valores negativos em alguns pontos. Apesar disso, ela retém uma grande quantidade de propriedades das distribuições clássicas de probabilidades, sendo por isso chamada uma *distribuição de quasi-probabilidade*, usualmente denotada W. Para mais detalhes, ver ref. [41].

No espírito daquelas discussões sobre a (im)possibilidade de determinação do estado quântico, encontramos no excelente livro de Mandel e Wolf[42, p. 542] a afirmação

> *"Of course, $W(q,p)$ does not correspond to any directly measurable quantity, because the joint probability of a pair of canonically conjugate variables cannot be measured, and indeed has no meaning in quantum mechanics."*

Esta afirmação está errada! Vögel e Rinsken[43] mostraram como é possível, a partir de distribuições de probabilidade $P_\theta(q_\theta)$ para as chamadas *quadraturas*, obter $W(q,p)$, pelo processo da *transformada de Radon inversa*. Esse é precisamente o processo utilizado para se fazer *tomografia*. Por isso este processo ficou conhecido como *tomografia de estado quântico*. Assim, a função de Wigner pode ser medida, mesmo sem se fazer medições incompatíveis sobre um mesmo sistema.

Uma crítica possível a este procedimento é que não se tem acesso direto à função de Wigner de um ponto (q,p), mas apenas por um procedimento que involve uma transformada integral. Para evitar esta crítica, Lutterbach e Davidovich[44] fizeram uma proposta para medição direta de pontos da função de Wigner de um modo de campo eletromagnético em uma cavidade (formalmente idêntico a um oscilador harmônico). Esta técnica já foi utilizada[45], e hoje em dia já se tem algumas funções de Wigner medidas, quer seja por tomografia, quer seja por "medição direta" (mais detalhes na ref. [41]).

Parametrização por Coeficientes Tomográficos

O primeiro exemplo, simples, importante e bastante conhecido, de descrição tomográfica de um estado quântico é o caso de um qubit. Para isso, usamos as

matrizes de Pauli

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.36}$$

que juntamente com a identidade, que denotaremos σ_0, formam uma base para o espaço vetorial real dos operadores auto-adjuntos sobre $\mathbb{C}^2$. Portanto, qualquer operador densidade ρ para o estado de um qubit pode ser escrito como combinação linear real de[39] σ_μ. Como $\mathrm{Tr}\sigma_i = 0$, a condição $\mathrm{Tr}\rho = 1$ implica que o coeficiente de σ_0 é $\frac{1}{2}$. Podemos então escrever

$$\rho = \frac{1}{2}\left\{\sigma_0 + \sum_i s_i \sigma_i\right\}. \tag{1.37}$$

É imediato calcular o determinante

$$\det \rho = \frac{1}{4}\left(1 - \|\vec{s}\|^2\right), \tag{1.38}$$

com o que conclui-se que, para ter ρ positivo, $\|\vec{s}\| \leq 1$, e para que ρ represente um estado puro, deve-se ter $\|\vec{s}\| = 1$. O vetor $\vec{s}$ é usualmente referido como *vetor de Bloch*; os estados puros constituem a chamada *esfera de Bloch* e a forma da eq. (1.37) é invariante por combinações convexas, assim os estados de mistura estão no interior da chamada *bola de Bloch*[40].

Se considerarmos o produto escalar $\langle \mathbf{A}, \mathbf{B}\rangle = \mathrm{Tr}\{\mathbf{A}^\dagger \mathbf{B}\}$, a base $\{\sigma_\mu\}$ é ortogonal, e todos os vetores têm norma $\sqrt{2}$. É imediato obter da eq. (1.37) que

$$s_i = \langle \sigma_i \rangle = \mathrm{Tr}\{\rho\sigma_i\}, \tag{1.39}$$

o que justifica chamarmos as componentes do vetor de Bloch de *coeficientes tomográficos*: elas podem ser diretamente obtidas por um processo de tomografia de spin!

Vale notar que a direção do vetor de Bloch depende da escolha de eixos x, y e z. Uma transformação ortogonal $\mathbf{O}$ em $\mathbb{R}^3$ pode levar o vetor de Bloch para a direção z. Assim, a bola de Bloch pode ser "descascada como uma cebola", com vetores de mesma norma sendo unitariamente equivalentes, *i.e.*: existe uma transformação unitária $\mathbf{U}$, associada a $\mathbf{O}$, que leva um estado ao outro por conjugação[41]:

$$\rho \mapsto \mathbf{U}\rho\mathbf{U}^\dagger. \tag{1.40}$$

Esse exemplo é simples demais, mas já ilustra várias facetas do problema. Agora vamos repetir esse procedimento para um par de qubits, onde já poderemos discutir as manifestações do emaranhamento. Vamos definir

$$\mathbf{S}_{\mu\nu} = \sigma_\mu \otimes \sigma_\nu, \tag{1.41}$$

[39] Vamos adotar a convenção que índices gregos valem 0, 1, 2 ou 3, enquanto índices latinos 1, 2 ou 3.

[40] A nomenclatura adotada aqui é a mais adequada do ponto de vista geométrico, mas cabe destacar que muitos textos de física irão se referir também aos estados mistos como constituintes da "esfera" de Bloch.

[41] O fato matemático por trás desta afirmação é que o grupo $SU(2)$ das transformações unitárias, com determinante 1, em $\mathbb{C}^2$ é o *duplo recobrimento* do grupo $SO(3)$ das transformações ortogonais de $\mathbb{R}^3$ que preservam orientação. Usando a conjugação (1.40) na representação de Bloch (1.37), obtemos outro operador densidade que pode ser representado pelo novo vetor de Bloch $\vec{s}'$. Como a conjugção é linear sobre ρ, $\vec{s}' = \mathbf{R}(\mathbf{U})\,\vec{s}$. Explicitar $\mathbf{R}(\mathbf{U})$ é um exercício de álgebra linear[46].

que formam uma base ortogonal para o espaço vetorial real (com dimensão 16) de operadores auto-adjuntos sobre $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$. Novamente é simples obter $\mathrm{Tr}S_{\mu\nu} = 4\delta_{\mu 0}\delta_{\nu 0}$, e podemos escrever

$$\rho = \frac{1}{4}\sum_{\mu\nu} a_{\mu\nu}\mathbf{S}_{\mu\nu}, \tag{1.42}$$

com $a_{00} = 1$. Novamente os coeficientes $a_{\mu\nu}$ podem ser obtidos tomograficamente usando

$$a_{\mu\nu} = \mathrm{Tr}\{\rho\mathbf{S}_{\mu\nu}\}. \tag{1.43}$$

Queremos agora interpretar geometricamente estes coeficientes, bem como buscar informações sobre o emaranhamento neles. Para isso, porém, é melhor reesecrever a eq. (1.42) na forma

$$\rho = \frac{1}{4}\left\{\mathbf{S}_{00} + \sum_i r_i\mathbf{S}_{i0} + \sum_j s_j\mathbf{S}_{0j} + \sum_{i,j} t_{ij}\mathbf{S}_{ij}\right\}, \tag{1.44}$$

onde se reconhecem dois vetores, $\vec{r}$ e $\vec{s}$ e um tensor de segunda ordem $\mathbf{t}$. A importância desses parâmetros pode ser reconhecida tanto na equação (1.43), quanto na sua ligação com os operadores densidade reduzida e as correlações. Para isso, deve-se notar que segue da eq. (1.44):

$$\rho_A = \frac{1}{2}\left\{\sigma_0 + \sum_i r_i\sigma_i\right\}, \tag{1.45}$$

$$\rho_B = \frac{1}{2}\left\{\sigma_0 + \sum_j s_j\sigma_j\right\}, \tag{1.46}$$

onde se reconhece que $\vec{r}$ e $\vec{s}$ determinam os *estados locais*, *i.e.*: aqueles acessíveis por medições apenas de Ana ou apenas de Bernardo. Deve-se notar que a maneira de obter tais coeficientes tomograficamente envolve sempre um operador σ_i em uma das partes e a identidade na outra, o que caracteriza uma medição local. É claro, então, que toda a informação sobre correlações em geral, e emaranhamento em particular, está no tensor $\mathbf{t}$.

Deve-se notar que operações unitárias em um dos qubits correspondem a transformações ortogonais do vetor de Bloch correspondente, no espírito da nota 41. Temos então liberdade para utilizar este tipo de transformação em cada parte do sistema (ou seja, agir com $\mathbf{U}_A \otimes \mathbf{U}_B$) sem alterar propriedades do estado (estas transformações podem ser interpretadas como escolhas independentes dos eixos de referência por Ana e Bernardo). Aravind se utilizou desta liberdade para alinhar $\vec{r}$ e $\vec{s}$ com seus eixos z, e a liberdade adicional de rotacionar em torno destes novos eixos z para simplificar o tensor $\mathbf{t}$ e interpretar geometricamente a decomposição de Schmidt[47] (claro, usando a condição adicional de o estado ser puro). Englert e Metwally, por outro lado, preferiram usar esta liberdade para diagonalizar $\mathbf{t}$, e proceder uma classificação dos estados de acordo com o posto e a degenerescência dessa matriz[48].

Também utilizando-se das transformações unitárias locais para diagonalizar $\mathbf{t}$, os Horodecki mostraram uma série de resultados bastante interessantes, tanto com respeito à geometria do conjunto de estados separáveis e não-separáveis[49],

quanto puderam demonstrar que, para um par de qubits, qualquer estado não-separável permite a destilação de pares EPRB[35]. Vale notar que, com o tensor **t** diagonalizado, suas três componentes diagonais podem ser consideradas como um vetor, e assim $\left(\vec{r},\vec{s},\vec{t}\right)$ descrevem, a menos de transformações unitárias locais, os estados de dois qubits. Uma rápida contagem de parâmetros reforça esta conclusão: o conjunto dos estados mistos de dois qubits tem dimensão 15, como estabelece a eq. (1.42). O grupo de Lie $SU\left(2\right)$ (assim como $SO\left(3\right)$) tem dimensão real 3, e portanto o grupo das transformações unitárias locais, $SU\left(2\right)\times SU\left(2\right)$ tem dimensão 6. Restam 9 parâmetros, que podem ser usados para descrever os vetores $\vec{r}$, $\vec{s}$ e $\vec{t}$.

Em particular, vale notar o efeito da transposição parcial nos coeficientes tomográficos. Como $\mathbf{1}$, σ_1 e σ_3 são invariantes pela transposição, enquanto $\sigma_2^t=-\sigma_2$, segue que o vetor de Bloch de ρ^t é a imagem do vetor de Bloch de ρ pela reflexão no plano xz. Da mesma forma, quando fazemos a transposição parcial no segundo fator, os coeficientes $\mathbf{S}_{\mu 2}$ (e apenas eles) mudarão de sinal.

Na secção 1.4.1 vamos descrever um método tomográfico de caracterização de estados puros de três qubits, no espírito do resultado de Linden, Popescu e Wootters[18].

Fórmula de Wootters

Este último resultado que queremos comentar sobre dois qubits diz respeito ao emaranhamento de formação. Conforme apresentado na sec. 1.3.3, a definição do emaranhamento de formação envolve uma minimização sobre todas as possíveis preparações do estado ρ, o que o torna não-operacional. Hill e Wootters mostraram[50] um procedimento algorítmico para calcular o emaranhamento de formação para estados de dois qubits com posto 2. Mais tarde, Wootters demonstrou que tal procedimento é geral, e que portanto há uma fórmula para se calcular o emaranhamento de formação para qualquer estado de dois qubits[51].

O primeiro passo para a fórmula de Wootters é a definição da *concorrência*[42] (do inglês, *concurrence*), que por si só pode ser considerada um quantificador de emaranhamento. A concorrência está diretamente ligada à semelhança entre um estado e seu *"spin flip"*. Formalmente, se ρ descreve um estado quântico, o seu "spin flip" é definido por

$$\tilde{\rho}=\sigma_2\otimes\sigma_2\rho^*\sigma_2\otimes\sigma_2. \tag{1.47}$$

É interessante usar a representação tomográfica para entender tal operação:

$$\tilde{\rho}=\sum_{\mu\nu}\left(-1\right)^{\mu+\nu}a_{\mu\nu}\mathbf{S}_{\nu\mu}. \tag{1.48}$$

Em particular, o estado de cada parte tem seus vetores de Bloch girados de 180^o em relação ao eixo y, o que justifica o nome da operação.

Para estados puros, $|\Psi\rangle$, a *concorrência* tem uma definição simples:

$$C\left(\Psi\right)=\left|\left\langle\Psi\mid\tilde{\Psi}\right\rangle\right|, \tag{1.49}$$

[42] Concorrência no sentido de cooperação, acordo, e não de competição.

onde $\left|\tilde{\Psi}\right\rangle$ denota o *spin flip* do estado $|\Psi\rangle$. Para estados mistos, a definição é um pouco menos direta, envolvendo os autovalores da matriz $R = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$. De uma maneira mais operacional, cada um desses autovalores é a raiz quadrada de um autovalor da matriz não-hermitiana $\rho\tilde{\rho}$, que são todos não-negativos. Esses autovalores de R são organizados em ordem decrescente, denotados λ_i, e a concorrência de ρ é dada por

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}. \tag{1.50}$$

Com qualquer das duas definições, a concorrência varia de 0, para estados separáveis, a 1, para estados maximamente emaranhados. Conhecida a concorrência, o emaranhamento de formação pode ser diretamente obtido, primeiro por uma mudança de escala, e depois pela passagem a uma forma entrópica, como na definição do emaranhamento de formação:

$$\mathcal{E}(C) = h\left(\frac{1+\sqrt{1-C^2}}{2}\right), \tag{1.51}$$

$$h(x) = -x\log x - (1-x)\log(1-x). \tag{1.52}$$

Além da aplicação óbvia de permitir calcular diretamente o emaranhamento de formação para um sistema de dois qubits, sem a necessidade de processos de extremização, esta fórmula também permitiu avanços na área de emaranhamento multipartite, como será discutido brevemente na secção 1.3.5.

1.3.5 Sistemas Multipartites

Chegamos agora ao caso mais geral, e naturalmente de mais difícil compreensão, de emaranhamento: estados mistos de sistemas multipartites. Não temos a ambição de ser completos nesta secção, mas apenas de listar alguns resultados interessantes conhecidos, bem como apontar algumas das questões em aberto. Em vários pontos algumas especulações serão feitas, que podem ser interpretadas como conjecturas que bem exibem o quanto incompleto ainda é nosso conhecimento nesse tema. Tal incompletude deve ser vista como um convite à pesquisa.

Três Qubits: Emaranhamento Distribuído

Um primeiro resultado interessante é apresentado em [21], onde generaliza-se para estados parcialmente emaranhados o interessante fato por vezes chamado *monogamia do emaranhamento*: se um par de qubits encontra-se maximamente emaranhado, nenhum de seus constituintes pode ter emaranhamento com qualquer outro sistema. Vamos começar demonstrando e comentando tal afirmação, para depois apresentar a generalização de Coffman, Kundu e Wootters.

A primeira parte é simples: se A e B estão em um estado puro, não guardam correlação com qualquer outro sistema, visto que o traço parcial neste outro sistema resulta no estado puro ρ_{AB}. Como os estados maximamente emaranhados de qubits são puros, segue a afirmação da monogamia. Vale notar que a única exigência neste argumento é a pureza do subsistema. Um resultado preliminar obtido com Daniel Cavalcanti e Fernando Brandão[52] permite falar em *poligamia de emaranhamento*: se n sistemas quânticos encontram-se maximamente

emaranhados, seus constituintes não podem guardar correlação com qualquer outro sistema. O passo essencial é garantir que um estado maximamente emaranhado é puro. A dificuldade maior reside na ausência de uma definição única de quantidade de emaranhamento, que permitisse definir *maximamente emaranhado*. No trabalho em questão utilizamos como quantificador o *emaranhamento testemunhado*, criado por Fernando Brandão e Reinaldo Vianna[53].

Restritos ao problema de três qubits, Coffman, Kundu e Wootters mostraram uma interessante relação: primeiramente para estados puros de três qubits vale:

$$C^2_{AB} + C^2_{AC} \leq C^2_{A(BC)}, \tag{1.53}$$

onde C_{XY} denota a concorrência dos qubits X e Y e o termos $C_{A(BC)}$ se justifica devido à pureza do trio: a decomposição de Schmidt diz que apenas um subespaço bidimensional dos dois últimos qubits realmente importa, assim temos efetivamente dois qubits e a concorrência pode ser calculada. A partir desta, os autores definem a mínima concorrência quadrática entre A e BC, $\left(C^2\right)^{\min}_{A(BC)}$ a partir das concorrências quadráticas médias de todas as possíveis decomposições do estado em ensembles de estados puros, e obtêm

$$C^2_{AB} + C^2_{AC} \leq \left(C^2\right)^{\min}_{A(BC)}, \tag{1.54}$$

que pode ser assim interpretada: o emaranhamento (medido aqui pela concorrência quadrática) de um qubit (A) com um par de qubits (BC) dá um máximo à soma dos emaranhamentos AB e AC. É importante notar que não há qualquer restrição deste tipo para correlações clássicas. Por exemplo, a temperatura de várias cidades próximas podem estar perfeitamente correlacionadas, independente do número de cidades consideradas. No mesmo trabalho os autores mostram ainda que esta desigualdade é ótima no sentido que pode ser saturada (é aí que os autores usam do estado hoje conhecido como $|W\rangle$) e definem um "emaranhamento residual" a partir da diferença dos dois membros, que é máxima para estados como $|GHZ\rangle$.

Mais Qubits

A concorrência foi utilizada ainda em outros problemas interessantes. Um que abordaremos agora é o emaranhamento entre qubits vizinhos em uma cadeia. O'Connor e Wootters propõem o problema de obter o estado que maximiza o mínimo do emaranhamento entre vizinhos para um anel (cadeia fechada) de N qubits e dão uma solução parcial a este[54]. Trabalhando em uma classe restrita de estados estes autores calculam a concorrência entre vizinhos para $N \leq 10$, depois exibem uma fórmula assintótica e calculam o limite $N \to \infty$. Interessantemente este limite é um número finito, aproximado por $C_{\max} = 0,434$. O próprio Wootters[55] já havia obtido este mesmo valor considerando cadeias abertas, o que é bastante razoável quando $N \to \infty$. Mas vale notar que no problema correlato, mas diferente, de considerar o emaranhamento entre quaisquer pares para estados simétricos (por troca de qubits) de N qubits[56], a concorrência de qualquer par é $\frac{2}{N}$, que se torna evanescente no limite $N \to \infty$.

Estes resultados nos permitem especular um pouco: mesmo não havendo garantia que estes máximos sejam de fato os máximos globais, eles parecem indicar que o total de emaranhamento de pares cresce linearmente com N (assintoticamente). Assim, se o importante é maximizar o emaranhamento entre

os vizinhos, como a quantidade destes também cresce como N, é possível ter uma razão assintótica entre 0 e 1. Já no caso de emaranhamento entre qualquer par, a quantidade de pares cresce como N^2 e portanto a razão vai a zero. Cabe ressaltar que há outros tipos de emaranhamentos a serem considerados. Também é um problema natural procurar o mínimo de emaranhamento entre trios vizinhos, bem como entre trios em geral, uma vez escolhido um quantificador para o emaranhamento de trios. Novamente os trios vizinhos crescem como N em uma cadeia de qubits, enquanto os trios em geral como N^3. Será que no primeiro caso novamente teremos um limite assintótico bem definido, enquanto o emaranhamento de trios em geral vai a zero? Mais ainda, o que estes resultados nos permitem pensar sobre sistemas macroscópicos? É bem verdade que normalmente estes não são consituídos por qubits, e devemos postergar tal questão.

Sistemas com mais Dimensões

Classicamente, a informação pode ser traduzida em bits. Será que quanticamente esta afirmação também é válida? Será que há alguma diferença em sistemas de dimensão d, ou, pelo menos no limite de um grande número de cópias, podemos sempre pensar em termos de coleções de qubits? Uma parte da resposta a essa pergunta está em estudar sistemas de dimensão d em busca de suas características. Um trabalho importante nesta questão é de Dennison e Wootters[57], que aborda o caso de d sistemas de dimensão d (*qudits*) e 3 sistemas de dimensão d, em particular no caso $d = 7$.

Novamente a pergunta é sobre o máximo do mínimo emaranhamento de pares, e a estratégia é trabalhar com estados simétricos, onde basta buscar o máximo emaranhamento para um par específico, pois todos os outros são iguais. Neste trabalho os autores utilizam-se do emaranhamento de formação e exibem explicitamente um exemplo de estado de d qudits que possui exatamente 1 ebit para cada par. Deve-se notar que dois qudits podem compartilhar até $\log d$ ebits, portanto a razão entre o emaranhamento presente e esta "*capacidade de emaranhamento*" cai quando d aumenta.

O outro caso tratado busca responder a pergunta: para um número N fixo de subsistemas de dimensão d, como se comporta esta função com respeito a d? Como o caso de 3 qutrits já é conhecido pelo caso anterior, o exemplo seguinte trata de 3 sistemas com dimensão 7. Uma engenhosa construção de estado e cálculo do emaranhamento de formação permite aos autores concluir que neste exemplo tem-se mais de $1,99$ ebits por par, o que dá uma fração $0,71$ da capacidade de emaranhamento para este exemplo. Isso os permite especular que deve haver limite para esta razão quando $d \to \infty$, podendo valer um de dois casos: ou este limite é 1 e é possível emaranhar maximamente pares de sistemas de alta dimensão sem restrições, desde que a dimensão seja suficientemente grande, ou tal limite é estritamente menor que 1, exibindo uma característica curiosa e impondo uma cota a ser entendida para o emaranhamento de formação de pares, quando um trio é considerado.

Assim, a função $E_{\max}(N, d)$ é conhecida para alguns poucos casos, e tem cotas inferiores para vários outros. Sabe-se

1. $E_{\max}(2, d) = \log d$;
2. $E_{\max}(3, 2) = \mathcal{E}(2/3) = 0,550$, valor assumido pelo estado $|W\rangle$;

3. $E_{\max}(N,2) \geq \mathcal{E}(2/N)$;
4. $E_{\max}(d,d) \geq 1$;
5. $E_{\max}(3,7) \geq 1,99$.

Notamos, aparentemente, uma competição entre N e d: enquanto maiores valores de N, para d fixo, parecem diminuir $E_{\max}(N,d)$ (mais partículas disputando uma mesma "capacidade de emaranhamento"), maiores valores de d, para N fixo, parecem permitir que $E_{\max}(N,d)$ aumente (a "mais espaço" para as partículas se emaranharem). E nesse caso, $d = N$ parece ser um "divisor de águas".

Diferentes Emaranhamentos, Diferentes Quantificadores

Como já vimos, para mais que dois subsistemas existem diferentes tipos de emaranhamento. Existem alguns quantificadores que podem ser capazes de fazer esta separação. Vamos discuti-los superficialmente aqui.

Um primeiro é a *entropia relativa de emaranhamento* (em inglês, *relative entropy of entanglement*), proposta por vários pesquisadores, entre eles Vedral e Plenio[58, 59]. A motivação original é que o emaranhamento de um estado seja dado por alguma noção de "distância" deste estado ao conjunto dos estados sem emaranhamento[43]. Para a entropia relativa de emaranhamento, a noção de "distância" utilizada é a *entropia relativa quântica*[44],

$$S(\sigma\|\rho) = \mathrm{Tr}(\sigma\log\sigma) - \mathrm{Tr}(\sigma\log\rho), \tag{1.55}$$

que não é uma distância no sentido próprio da palavra, mas tem uma interpretação em teoria da informação no sentido de medir quão improvável é "confundir" um estado com o outro. Assim, a melhor interpretação da entropia relativa de emaranhamento é "quão longe o estado σ está de ser confundido com um estado ρ sem emaranhamento?"

Outra proposta interessante é a chamada *robustez* (*robustness*), proposta por Vidal e Tarrach[60]. Para isso eles primeiro definem a *robustez de um estado ρ relativa a um estado separável ρ_s*, denotada $R(\rho\|\rho_s)$, como o menor valor de s tal que

$$\rho(s) = \frac{1}{1+s}(\rho + s\rho_s) \tag{1.56}$$

é separável. Se ρ é separável, $R(\rho\|\rho_s)$ é nula, qualquer que seja ρ_s, mas para escolhas especiais de ρ e ρ_s podemos ter robustez relativa infinita. Isso não irá atrapalhar os passos seguintes, porém. Com a robustez relativa os autores definem dois quantificadores de emaranhamento: a *robustez aleatória* (*random robustness*) e a *robustez absoluta* (*absolute robstness*), ou simplesmente *robustez*. A primeira á a robustez relativa ao estado maximamente misturado, $\frac{1}{d}\mathbf{1}$, enquanto a segunda é o mínimo da robustez relativa quando fazemos ρ_s variar em todo o conjunto dos operadores densidade não-emaranhados.

As duas propostas são interessantes, e mesmo as extremizações que envolvem podem ser contornadas com alguns resultados de análise convexa. Mas a

[43] No caso bipartite, o conjunto dos separáveis. Em caso multipartite, é preciso definir o tipo de emaranhamento que deve estar ausente neste conjunto.

[44] A base do logaritmo costuma ser 2, mas os autores preferiram usar base e.

robustez padece da falta de um critério geral de separabilidade. Atualmente ela só é prática para os dois casos em que o Critério de Peres-Horodecki é decisivo: dois qubits e um qubit e um qutrit.

O terceiro exemplo que queremos discutir nos é bem próximo, proposto por Fernando Brandão e Reinaldo Vianna[53]. Como o conjunto dos estados sem um certo tipo de emaranhamento é sempre convexo e fechado, qualquer ponto fora deste conjunto pode ser *separado* deste por um hiperplano. A esta construção corresponde um funcional linear que assume valor negativo no ponto desejado e é positivo em todos os estados não-emaranhados. Este funcional é chamado uma *testemunha de emaranhamento*. Os autores desenvolvem um quantificador a partir de uma busca, computacionalmente eficiente, de uma *testemunha ótima*, e de uma função simples calculada sobre o valor deste funcional ótimo no estado de interesse. Os primeiros exemplos não triviais de aplicação deste quantificador ainda estão sendo produzidos, mas até o momento ele se mostra como a única alternativa realmente operacional (no sentido de ser calculada em exemplos práticos) de quantificador para os diferentes emaranhamentos multipartite.

1.4 Contribuições

1.4.1 As partes determinam o todo?

Já comentamos o interessante trabalho de Linden, Popescu e Wootters[18] que mostra que estados puros genéricos de três qubits podem ser completamente caracterizados pelo conhecimento de seus estados reduzidos de pares. Em colaboração com Daniel Cavalcanti e Leandro Martins Cioletti, apresentamos um protocolo tomográfico para realizar esta tarefa[61].

Antes de passar ao protocolo vale discutir que o resultado não é imediato: por exemplo, não vale o seu análogo para dois qubits: um estado puro genérico de dois qubits pode ser escrito como

$$|\Psi(\theta)\rangle = \cos\theta\,|u_1\rangle \otimes |v_1\rangle + \mathrm{sen}\theta\,|u_2\rangle \otimes |v_2\rangle\,, \tag{1.57}$$

com[45] $\theta \in \left(0, \frac{\pi}{4}\right)$. Mas fixadas estas bases, todos os demais estados

$$|\Psi(\theta,\phi)\rangle = \cos\theta\,|u_1\rangle \otimes |v_1\rangle + e^{i\phi}\mathrm{sen}\theta\,|u_2\rangle \otimes |v_2\rangle\,, \tag{1.58}$$

dão origem aos mesmos estados reduzidos. Em outras palavras, a fase ϕ é *localmente inacessível*.

Nosso trabalho parte da generalização para três qubits da descrição por coeficientes tomográficos que foi aqui apresentada na 1.3.4. Em lugar da eq. (1.42), teremos

$$\rho = \frac{1}{8}\sum_{\gamma\mu\nu} a_{\gamma\mu\nu}\mathbf{S}_{\gamma\mu\nu}, \tag{1.59}$$

onde

$$\mathbf{S}_{\gamma\mu\nu} = \sigma_\gamma \otimes \sigma_\mu \otimes \sigma_\nu, \tag{1.60}$$

[45] Os casos não genéricos correspondem a $\theta = 0$, quando o estado é fatorado e localmente determinável, e a $\theta = \frac{\pi}{4}$, que corresponde a estados maximamente emaranhados, e também maximamente indeterminados, pois nesse caso os estados locais são o de máxima mistura, e a degenerescência deste permite a livre escolha de $|u_1\rangle$ e $|v_1\rangle$, além da fase ϕ.

e os coeficientes tomográficos $a_{\gamma\mu\nu}$ podem ser diretamente obtidos por

$$a_{\gamma\mu\nu} = \mathrm{Tr}\rho\mathbf{S}_{\gamma\mu\nu}. \tag{1.61}$$

Assim, os coeficientes a_{i00}, a_{0j0} e a_{00k} são diretamente obtidos com detecções em apenas uma parte, a_{ij0}, a_{i0k} e a_{0jk} com detecções em coincidência de duas partes, enquanto os a_{ijk} dependem de detecções nas três partes. O problema que se põe é: podemos descrever o estado do sistema sem precisar das detecções nos trios? A resposta é: genericamente sim. Como? Veremos a seguir. Uma analogia geométrica pode ser interessante. Considere um disco como um exemplo de conjunto convexo. Para descrever um ponto no disco precisaremos de duas coordenadas (*e.g.*: x e y cartesianos, ou r e θ polares). Mas se tivermos a informação adicional que temos um ponto extremal do disco (voltando à mecânica quântica, um estado puro), basta dar um ângulo para determinar o ponto. Assim, é natural que, para o caso de um estado puro, sejam suficientes menos informações do que aquelas que seriam necessárias para decrever um operador densidade arbitrário.

Nosso ponto de partida foi usar a idempotência que caracteriza estados puros

$$\rho^2 = \rho, \tag{1.62}$$

para obter as correlações de maior ordem em termos das de menor. Neste caso, as de terceira ordem em termos das de primeira e segunda ordem. O conjunto de sessenta e quatro equações pode ser assim agrupado:

$$\sum_{ijk}(a_{i00}^2 + a_{0j0}^2 + a_{00k}^2 + a_{ij0}^2 + a_{i0k}^2 + a_{0jk}^2 + a_{ijk}^2) = 7, \tag{1.63a}$$

$$3a_{i00} = a_{ij0}a_{0j0} + a_{i0k}a_{00k} + \sum_{jk} a_{ijk}a_{0jk}, \tag{1.63b}$$

com equações similares por trocas de índices,

$$\begin{aligned} 3a_{ij0} &= a_{i00}a_{0j0} + \sum_k a_{00k}a_{ijk} + \sum_k a_{0jk}a_{i0k} \\ &\quad -\frac{1}{2}\sum_{ltmu} \epsilon_{ilt}\epsilon_{jmu}a_{lm0}a_{tu0} - \frac{1}{2}\sum_{ltmu} \epsilon_{ilt}\epsilon_{jmu}a_{tuk}a_{lmk}, \end{aligned} \tag{1.63c}$$

também com equações similares obtidas pelas permutações cíclicas dos índices, e com o símbolo se Levi-Civitta ϵ_{ijk} para o tensor totalmente anti-simétrico, com $\epsilon_{123} = 1$. Por fim, o quarto grupo

$$\begin{aligned} 3a_{ijk} &= a_{i00}a_{0jk} + a_{0j0}a_{i0k} + a_{00k}a_{ij0} - \sum_{ltmu} \epsilon_{ilt}\epsilon_{jmu}a_{tu0}a_{lmk} \\ &\quad -\sum_{ltnv} \epsilon_{ilt}\epsilon_{knv}a_{t0v}a_{ljn} - \sum_{munv} \epsilon_{jmu}\epsilon_{knv}a_{0uv}a_{imn}. \end{aligned} \tag{1.63d}$$

O protocolo é então dado pela determinação direta dos coeficientes a_{i00}, a_{0j0} e a_{00k} com medições individuais, bem como a_{ij0}, a_{i0k} e a_{0jk} pelas detecções de pares. O sistema de 64 equações (1.63) pode ser visto como um sistema de equações a serem obedecidas pelas 27 "incógnitas" a_{ijk} sempre que o estado global for puro. O argumento de Linden, Popescu e Wootters[18] garante que

genericamente este sistema tem solução. Nossa conjectura é que sempre que o sistema (1.63) possui solução única, o subsistema linear (1.63d) é suficiente para determinar esta solução. Testamos isso numericamente: sorteando de forma aleatória estados puros de três qubits, construímos a matriz do sistema (1.63d) e calculamos seu determinante: para mais de uma centena de realizações este foi sempre diferente de zero.

Existem exceções, porém. Para estados como

$$|GHZ(\theta,\phi)\rangle = \cos\theta\,|000\rangle + e^{i\phi}\mathrm{sen}\theta\,|111\rangle\,, \tag{1.64}$$

a fase ϕ não pode ser determinada por medições restritas a pares, por ser uma fase relativa entre vetores triortogonais e por isso não aparecer nos estados reduzidos. Esta classe de exemplos generaliza perfeitamente o caso de dois qubits, eq. (1.58). Dessa maneira podemos entender todas as exceções: são os vetores obtidos de (1.64) por transformações unitárias locais, visto que para qualquer outro caso, as fases relativas[46] poderão todas ser obtidas nas densidades reduzidas. Acreditamos que um estudo mais geométrico do sistema (1.63d) seja também capaz de levar a estas mesmas conclusões.

Já sabemos que as exceções formam um conjunto de medida nula (por isso numericamente 100% dos casos foram favoráveis), mas uma contagem de parâmetros mostra mais: elas formam uma subvariedade de dimensão[47] 1 enquanto as classes de estados formam uma variedade de dimensão 5. Para esta conclusão usamos o fato bem conhecido que o grupo de Lie $SU(2)$ possui dimensão 3. Um vetor de $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ é dado por 8 números complexos, portanto 16 números reais. Normalização e fase global eliminam dois destes. As transformações unitárias locais serão dadas por três cópias de $SU(2)$, portanto dimensão 9. Assim, os estados de três qubits não-localmente equivalentes formam uma variedade de dimensão 5 (*i.e.*: $14-3\times3$). Já a família GHZ, quando considerada a menos de tranformações unitárias locais, será descrita apenas pelo parâmetro θ, já que a fase ϕ pode ser obtida usando a transformação $|0\rangle\mapsto e^{-i\frac{\phi}{2}}|0\rangle$ e $|1\rangle\mapsto e^{i\frac{\phi}{2}}|1\rangle$ em qualquer dos três qubits. Assim, as exceções formam uma curva em uma variedade de dimensão 5.

Embora o protocolo seja pensado inicialmente para estados puros, ele possui um mérito a mais: para estados não-puros, a eq. (1.62) é falsa, o que implica que o sistema (1.63) terá equações incompatíveis. O protocolo torna-se mais confiável então se após medir os valores esperados individuais e de pares, e resolver o sistema (1.63d), o experimentador usar as demais trinta e sete equações (1.63a, 1.63b, 1.63c) como testes (dentro de sua precisão) da pureza do estado.

[46] Os módulos são sempre acessíveis.

[47] Neste parágrafo, as dimensões são sempre sobre os reais.

Bibliografia

[1] A. Peres, *Quantum Theory: Concepts and Methods*, (Kluwer Academic Publishers, Dordrecht, 1995).

[2] R.P. Feynman, R.B. Leighton e M. Sands, *The Feynman Lectures on Physics*, vol. 3, (Addison-Wesley publishing company, Reading, 1965).

[3] J.S. Bell, *Speakable and unspeakable in quantum mechanics*, (Cambridge University Press, Cambridge, 1987).

[4] A.I. Kostrikin e Yu.I. Manin, *Linear Algebra and Geometry*(Gordon and Breach Science Publishers, Amsterdam, 1989).

[5] M.A. Nielsen e I.L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).

[6] A. Ekert e P.L. Knight, "Entangled quantum systems and the Schmidt decomposition," *Am. J. Phys.* **63**, 415 (1995).

[7] H.-K. Lo e S. Popescu, "Concentrating entanglement with local actions - beyond mean values," quant-ph/9707038.

[8] A. Einstein, Podolsky e N. Rosen, "Can quantum mechanics be considered a complete theory?," *Phys. Rev.* **47**, 777 (1935).

[9] D. Bohm, *Quantum Theory*, (Prentice-Hall, New Jersey, 1951).

[10] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*, (Sringer-Verlag, Berlin, 1932); tradução para o inglês: *Mathematical Foundations of Quantum Mechanics*, (Princeton Unversity Press, Princeton, 1955).

[11] D. Bohm, "A suggested interpretation of quantum theory in terms of "hidden" variables. I," *Phys. Rev.* **85**, 166 (1952); "A suggested interpretation of quantum theory in terms of "hidden" variables. II," *Phys. Rev.* **85**, 180 (1952).

[12] J.S. Bell, "On the problem of hidden variables in quantum theory," *Rev. Mod. Phys.* **38**, 447 (1966). Reimpresso na ref. [3].

[13] J.S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics* **1**, 195 (1965). Reimpresso na ref. [3].

[14] J.F. Clauser, M.A. Horne, A. Shimony e R.A. Holt, "Proposed experiment to test local hiden-variable theories," *Phys. Rev. Lett.* **23**, 880 (1969).

[15] D.C. Brody e L.P. Hughstone, "Geometric quantum mechanics," *J. Geom. Phys.* **38**, 19 (2001).

[16] J. Harris, *Algebraic Geometry - A First Course*, (Springer-Verlag, New York, 1992).

[17] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, (Springer-Verlag, New York, 1977).

[18] N. Linden, S. Popescu e W.K. Wootters, "Almost every pure state of three qubits is completely determined by its two-particle reduced density matrices," *Phys. Rev. Lett.* **89**, 207901 (2002).

[19] W. Dür, G. Vidal e J.I. Cirac, "Three qubits can be entangled in two inequivalet ways," *Phys. Rev. A* **62**, 062314 (2000).

[20] D.M. Greenberger, M.A. Horne, A. Shimony e A. Zeilinger, "Bell's theorem witout inequalities," *Am. J. Phys.* **58**, 1131 (1990); D.M. Greenberger, M.A. Horne e A. Zeilinger, Multiparticle interferometry and the superposition principle," *Phys. Today*, 22 (August, 1993); N.D. Mermin, "What's wrong with these elements of reality?," *Phys. Today*, 9 (June, 1990); "Quantum mysteries revisited," *Am. J. Phys.* **58**, 731 (1990).

[21] V. Coffman, J. Kundu e W.K. Wootters, "Distributed entanglement," *Phys. Rev. A* **61**, 052306 (2000).

[22] F. Verstraete, J. Dehaene, B. De Moor e H. Verschelde, "Four qubits can be entangled in nine different ways," *Phys. Rev. A* **65**, 052112 (2002).

[23] C. Bennett e G. Brassard "Quantum cryptography: public key distribution and coin tossing," *Proceedings of IEEE Conference on Computers, Systems, and Signal Processing, Bangalore, Índia* p. 175 (IEEE, New York, 1984). Disponível em www.research.ibm.com/people/b/bennetc

[24] W. Thirring, *A Course in Mathematical Physics 3: Quantum Mechanics of Atoms and Molecules*, (Springer-Verlag, New York, 1981).

[25] L. Diósi, "Three-party pure quantum states are determined by two-party reduced states," *Phys. Rev. A* **70**, 010302(R) (2004).

[26] N. Linden e W.K. Wootters, "The parts determine the whole in a generic pure quantum state," *Phys. Rev. Lett.* **89**, 277906 (2002).

[27] W. Thirring, *A Course in Mathematical Physics 4: Quantum Mechanics of Large Systems*, (Springer-Verlag, New York, 1983).

[28] R. Werner, "Quantum states with Einstein-Podolski-Rosen correlations admitting a hidden-variable model," *Phys. Rev. A* **40**, 4277 (1989).

[29] A. Peres, "Separability criterion for density matrices," *Phys. Rev. Lett.* **76**, 1413 (1996).

[30] M. Horodecki, P. Horodecki e R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," *Phys. Lett. A* **223**, 1 (1996).

[31] M.A. Nielsen e J. Kempe, "Separable states are more disordered globally than locally," *Phys. Rev. Lett.* **86**, 5184 (2001).

[32] B.N.B. Lima, L.M. Cioletti, M.O. Terra Cunha e G.A. Braga, *"Entropia: introdução à teoria matemática da (des)informação"*, II Bienal da SBM (SBM, Salvador, 2004).

[33] D. Bruß, "Characterizing entanglement," *J. Math. Phys.* **43**, 4237 (2002).

[34] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin e W.K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A* **54**, 3824 (1996).

[35] M. Horodecki, P. Horodecki e R. Horodecki, "Inseparable two spin-$\frac{1}{2}$ density matrices can be distilled to a singlet form," *Phys. Rev. Lett.* **78**, 574 (1997).

[36] M. Horodecki, P. Horodecki e R. Horodecki, "Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?" *Phys. Rev. Lett.* **80**, 5239 (1998).

[37] M.A. Nielsen, "On the units of bipartite entanglement: Is sixteen ounces of entanglement always equal to one pound?" quant-ph/0011063.

[38] S. Weigert, "Pauli problem for a spin of arbitrary length: A simple method to determine its wave function," *Phys. Rev. A* **45**, 7688 (1992).

[39] V.I. Man'ko, "Classical formulation of quantum mechanics," *J. Russ. Laser Res.* **17**, 579 (1996). V.V. Dodonov e V.I. Man'ko, "Positive distribution description for spin states," *Phys. Lett. A* **229**, 335 (1997).

[40] E.P. Wigner, "On the quantum correction for thermodynamical equilibrium," *Phys. Rev.* **40**, 749 (1932).

[41] L. Davidovich, "Decoherence and quantum-state measurement in quantum optics" quant-ph/0301129.

[42] L. Mandel e E. Wolf, *Optical Coherence and Quantum Optics*, (Cambridge University Press, Cambridge, 1995).

[43] K. Vögel e H. Rinsken, "Determination of quasiprobability distribution in terms of probability distributions for the rotated quadrature phase," *Phys. Rev. A* **40**, 2847(R) (1989).

[44] L.G. Lutterbach e L. Davidovich, "Method for direct measurement of the Wigner function in cavity QED and ion traps," *Phys. Rev. Lett.* **78**, 2547 (1997).

[45] P. Bertet *et al.*, , Direct measurement of the Wigner function of a one-photon Fock state in a cavity," *Phys. Rev. Lett.* **89**, 200402 (2002).

[46] J.J. Sakurai, *Modern Quantum Mechanics* (Addison Wesley, Reading, 1994).

[47] P.K. Aravind, "Geometry of the Schmidt decomposition and Hardy's theorem," *Am. J. Phys.* **64**, 1143 (1996).

[48] B.-G. Englert e N. Metwally, "Remarks on 2−q-bit states," *App. Phys. B* **72**, 35 (2001); Também disponível em quant-ph/0007053.

[49] R. Horodecki e M. Horodecki, "Information-theoretic aspects of inseparability of mixed states," *Phys. Rev. A* **54**, 1838 (1996). R. Horodecki, M. Horodecki e P. Horodecki, "Teleportation, Bell's inequalities and inseparability," *Phys. Lett. A* **222**, 21 (1996).

[50] S. Hill e W.K. Wootters, "Entanglement of a pair of quantum bits," *Phys. Rev. Lett.* **78**, 5022 (1997).

[51] W.K. Wootters, "Entanglement of formation of an arbitrary state of two qubits," *Phys. Rev. Lett.* **80**, 2245 (1998).

[52] D. Cavalcanti, F.G.S.L. Brandão e M.O. Terra Cunha, em preparação.

[53] F.G.S.L. Brandão e R.O. Vianna, "Witnessed entanglement," quant-ph/0405096.

[54] K.M. O'Connor e W.K. Wootters, "Entangled rings," *Phys. Rev. A* **63**, 052302 (2001).

[55] W.K. Wootters, "Entangled chains," quant-ph/0001114.

[56] M. Koashi, V. Bužek e N. Imoto, "Entangled webs: Tight bound for symmetric sharing of entanglement," *Phys. Rev. A* **62**, 050302 (2000).

[57] K.A. Dennison e W.K. Wootters, "Entanglement sharing among quantum particles with more than two orthogonal states," *Phys. Rev. A* **65**, 010301(R) (2001).

[58] V. Vedral, M.B. Plenio, M.A. Rippin e P.L. Knight, "Quantifying entanglement," *Phys. Rev. Lett.* **78**, 2275 (1997).

[59] V. Vedral e M.B. Plenio, "Entanglement measures and purification procedures," *Phys. Rev. A* **57**, 1619 (1997).

[60] G. Vidal e R. Tarrach, "Robustness of entanglement," *Phys. Rev. A* **59**, 141 (1999).

[61] D. Cavalcanti, L.M. Cioletti e M.O. Terra Cunha, "Tomographic characterization of three-qubit pure states with only two-qubit detectors," quant-ph/0408022. Submetido à *Phys. Rev. A*.