Não-localidade quântica: matemática e fundamentos

Dissertação de mestrado

Candidato: Rafael Luiz da Silva Rabelo
Orientador: Prof. Marcelo de Oliveira Terra Cunha

Dissertação apresentada ao Programa de pós-graduação em Física da Universidade Federal de Minas Gerais como requisito parcial para a obtenção do título de Mestre em Física.

Abril de 2010

Aos meus pais. Ambos não sabem o quanto procuro me espelhar em seus exemplos.

Agradecimentos

Esta dissertação jamais teria sido escrita sem o apoio e o incentivo de várias pessoas. Agradeço sinceramente a todos aqueles que me ajudaram a chegar até aqui.

Primeiramente, agradeço ao Marcelo, excelente orientador e grande amigo. Sou profundamente grato por me apresentar à mecânica quântica, e, desde então, me guiar pelos caminhos da pesquisa com infinitas paciência e atenção, sempre deixando uma incômoda liberdade - essencial na formação de um pesquisador. Agradeço muito por todos os conselhos e broncas, e por tudo o que me ensinou - física, matemática, e todo o resto.

Aos meus pais, Vera e José Luiz, agradeço por tudo; pelos valores, pelos exemplos, pelos conselhos e pelo apoio incondicional. Ao Rodrigo, agradeço pela cumplicidade e amizade, e por me inspirar sempre a ser uma pessoa melhor.

Um agradecimento especial dedico à Camila, minha namorada. Sou imensamente grato pela dedicação, pelo companheirismo, pela paciência e por todos os ótimos momentos que passamos juntos. Sem você teria sido mais difícil.

À minha família, em especial, à minha avó Zely, e às tias Carmem, Lúcia e Lena, agradeço por todo o carinho.

Aos grandes amigos e bons companheiros Guto, Nando, Saulo e Lavínia, meus sinceros agradecimentos por todos os anos de convivência, sempre harmoniosa.

Aos amigos da física, em particular ao Diogão, ao Emilson, ao Samuel, ao Dudu, ao Marquinhos, ao Breno, ao Romero e ao Kaka, agradeço pelas discussões, pelas cervejas, pelo incentivo e pelo ótimo ambiente. Existe um pouco de cada um de vocês nesta dissertação.

Aos colegas do EnLight, agradeço por excelentes discussões. Em especial, agradeço ao Marcelo França, pela amizade e por todas as aulas informais, e ao Sebastião, por todas as aulas formais.

Ao Daniel, agradeço pela colaboração e por apontar importantes referências.

Aos amigos de São João: Gui, Toad, Jota, C. A., Carlos, João Paulo, Diogo, Marcelo, Gustavo, Marcus, Feijão, Sid, Bóia, Vinícius e Beleza, agradeço por memoráveis momentos. Ao Tinno, ao Totona, ao John e ao Matheus, agradeço pela amizade inabalável e pelo companheirismo. Ao Dani, agradeço por, inúmeras vezes, me mostrar que a vida não é tão complicada quanto parece. Sem todos vocês, a vida seria menos divertida.

Índice

Resumo

A mecânica quântica prevê a existência de fortes correlações entre sistemas espacialmente afastados que não podem ser explicadas por teorias realistas locais - teorias nas quais propriedades individuais são atribuídas a cada um dos sistemas. Nas últimas décadas, essa notável característica chamou a atenção devido a seu forte caráter contra-intuitivo, mas, com o desenvolvimento recente da teoria quântica da informação, correlações não-locais foram identificadas como importante recurso em protocolos de processamento de informação, garantindo, por exemplo, segurança incondicional em protocolos de distribuição de chaves criptográficas.

Nesta dissertação estudamos diferentes aspectos da não-localidade: seus fundamentos físicos e matemáticos e aplicações na teoria da informação, passando por uma análise detalhada dos conjuntos de correlações locais e não-locais, dando especial atenção às correlações quânticas e sua relação com o emaranhamento.

Abstract

Quantum mechanics predicts the existence of strong correlations between distant systems that cannot be explained by local realistic theories - theories in which individual properties are assigned to each one of the systems. On the last decades, this remarkable feature has called attention because of its strong counter-intuitive character, but, with the recent development of quantum information theory, nonlocal correlations have been noted to be an important resource in information processing protocols, responsible, for instance, for unconditional security in cryptographic key distribution protocols.

In this dissertation, we study different aspects of nonlocality, from its physical and mathematical foundations to applications in information theory, including a detailed analisys of the sets of local and nonlocal correlations, giving special attention to quantum correlations and entanglement.

Introdução

Cerca de 80 anos se passaram desde o surgimento da mecânica quântica, em meados de 1920. Ao longo desse período, a teoria quântica firmou-se como uma poderosa e bem sucedida teoria científica, capaz de tratar com precisão uma vasta gama de fenômenos naturais. Por outro lado, apesar de enormes desenvolvimentos teóricos e experimentais obtidos através da mecânica quântica ao longo do século XX, pouco ainda se sabe sobre seus fundamentos. Não há consenso sobre a interpretação de seu formalismo, e não se sabe quais são os princípios físicos fundamentais que regem os fenômenos quânticos.

Vários aspectos da teoria quântica sugerem que o mundo que ela descreve é bem diferente do mundo macroscópico. Um dos mais intrigantes é um conceito conhecido como não-localidade, que está relacionado a fortes correlações entre os resultados de medições realizadas em sistemas espacialmente afastados. Qualquer teoria em que o resultado de cada medição pode ser pré-determinado e depende somente de causas locais - eventos no cone de luz passado de cada sistema - é incapaz de reproduzir as correlações não-locais previstas pela mecânica quântica. Todas as teorias físicas pré-quânticas são locais, nesse sentido, e a ruptura entre elas e a teoria quântica gerou desconforto em parte da comunidade científica. Muitos não aceitavam, e não aceitam, que uma teoria com características não-locais seja uma descrição satisfatória da Natureza.

Resta saber, então, como a Natureza se comporta. Vários experimentos foram realizados, e os resultados obtidos em todos eles concordam com os previstos pela mecânica quântica. No entanto, em todos os experimentos há detalhes, ora tecnológicos, ora metodológicos, que permitem que possíveis teorias locais reproduzam os resultados observados. Permanece o desafio de se realizar um experimento conclusivo que comprove a existência das correlações não-locais previstas pela mecânica quântica.

Com o desenvolvimento recente da teoria quântica da informação, a não-localidade foi identificada como um importante recurso para a realização

de protocolos de processamento de informação. Essa teoria surgiu com a observação de que, se sistemas quânticos são usados para armazenamento e processamento de informação, então inúmeras novas possibilidades surgem. Tarefas que, acredita-se, são difíceis de se processar em computadores clássicos, como a fatoração de números, podem ser eficientemente executadas em computadores quânticos; criptografia, em particular distribuição de chaves criptográficas, pode ser realizada de forma absolutamente segura; informação pode ser teletransportada entre sistemas afastados. Esses são apenas alguns exemplos de uma lista que tem crescido com o desenvolvimento da teoria quântica da informação. Em muitas dessas tarefas, a não-localidade tem importante papel, mostrando que, além de sua óbvia importância para os fundamentos da teoria quântica, esse conceito tem também importância prática e operacional.

Nesta dissertação, procuramos reunir e apresentar de forma clara alguns dos mais importantes aspectos da não-localidade quântica, focando, principalmente, na bela matemática por trás desse conceito e em seus aspectos fundamentais. No capítulo 1, preliminar, introduzimos algumas noções da mecânica quântica importantes para o entendimento do restante do texto, como o conceito de emaranhamento e o formalismo de medições. No capítulo 2, apresentamos o paradoxo de EPR: um argumento introduzido por Einstein, Podolski e Rosen com o objetivo de provar que a mecânica quântica não é uma teoria completa, que, exatamente devido a noção rudimentar de não-localidade, não poderia ser uma descrição satisfatória da Natureza. No capítulo 3, estudamos as correlações locais e sua rica estrutura geométrica, da qual emergem naturalmente as desigualdades de Bell, objetos centrais na teoria de não-localidade. No capítulo 4, introduzimos as correlações quânticas e o teorema de Bell, que evidencia sua não-localidade; apresentamos o paradoxo de GHZ; detalhamos o conceito de emaranhamento; e, por fim, citamos alguns dos testes experimentais de não-localidade realizados. O derradeiro capítulo 5 tem um apelo 'informacional', e é onde abordamos correlações mais gerais e ainda mais fortes que as quânticas, e algumas de suas consequências na teoria da informação.

1

Mecânica quântica

Quantum mechanics: real black magic calculus.

- Albert Einstein.

Neste capítulo preliminar, apresentaremos noções de uma das mais poderosas e bem sucedidas teorias científicas já desenvolvidas: a mecânica quântica. Não temos a pretensão de sermos completos nesta introdução; nosso objetivo é apresentar, especialmente ao leitor não especializado, conceitos que serão importantes no decorrer desta dissertação. Àqueles interessados em se aprofundar nos fundamentos da mecânica quântica e na teoria quântica da informação, indicamos os livros de Peres [1], von Neumann [2], Feynman [3], Cohen-Tannoudji [4], Nielsen e Chuang [5] e Terra Cunha [6].

1.1 Sistemas e estados quânticos

A mecânica quântica aborda uma ampla variedade de fenômenos, da escala sub-atômica à macroscópica. Por um lado, esta gama enorme de aplicações reforça a crença de que seu formalismo é universal, capaz de descrever toda a natureza[1]. Por outro, torna muito difícil, senão impossível, destacar *a priori* para quais sistemas físicos uma abordagem quântica seria vantajosa, computável e precisa. Recorrendo ao pragmatismo, Asher Peres ([1], pg.24) responde a esta questão de uma maneira interessante, conscientemente tautológica, mas muito útil:

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

[1]Persiste determinada incompatibilidade entre o formalismo quântico e a teoria da relatividade geral que impede que se possa afirmar que a mecânica quântica é geral, neste sentido.

A matemática por trás da teoria quântica tem a regância da álgebra linear. A todo sistema quântico está associado um *espaço de Hilbert* complexo $\mathcal{H}$ - um caso especial de espaço vetorial complexo dotado de produto interno[2]. Nesta dissertação, somente serão abordados sistemas cujos espaços de Hilbert tenham dimensão finita; caso a dimensão d de $\mathcal{H}$ seja explicitamente importante em algum contexto, o espaço de Hilbert será denotado $\mathcal{H}^d$.

Um vetor arbitrário de $\mathcal{H}^d$ será escrito, utilizando-se a muito conveniente notação de Dirac, como $|\psi\rangle$ - lê-se *ket* psi. O produto interno entre dois vetores $|\psi\rangle$ e $|\chi\rangle$ será denotado $\langle\psi \mid \chi\rangle$. Através dele, para cada vetor $|\chi\rangle$ é definido um funcional linear $\langle\chi|$ - lê-se *bra* chi - ; o produto interno, assim, forma um *braket*[3]. A norma de um vetor é definida como $||\psi\rangle| \equiv \sqrt{\langle\psi \mid \psi\rangle}$.

É possível, com esta notação, definir um *produto externo*, $|\psi\rangle\langle\chi|$. Este, ao contrário do produto interno, representa um *operador linear*[4], e não um escalar. Um exemplo importante é o *operador identidade*, denotado $\mathbf{1}$ e definido pela equação $\mathbf{1}|\psi\rangle \equiv |\psi\rangle$, para todo $|\psi\rangle$. Outro operador que merece destaque é o *projetor*. Denotado, em geral, $\mathbf{\Pi}$, o projetor - como seu nome sugere - , projeta um vetor em um sub-espaço do espaço de Hilbert. *Projetores unidimensionais* são particularmente importantes; o projetor unidimensional no sub-espaço gerado por $|\psi\rangle$ é escrito como $\mathbf{\Pi} = |\psi\rangle\langle\psi|$.

O objeto matemático utilizado para a descrição de um sistema físico, em determinado instante de tempo, é chamado de *estado*. Na mecânica quântica, o estado é um operador ρ definido no espaço de Hilbert associado ao sistema que ele descreve. O *operador densidade* ρ, como é chamado, é definido segundo as condições:

1. *Hermiticidade*: ρ é *hermitiano*, $\rho = \rho^\dagger$, onde $\rho^\dagger$ é o operador *adjunto*[5] de ρ.

2. *Positividade*: ρ é *positivo semi-definido*, *i.e.*, $\langle\psi|\rho|\psi\rangle \geq 0$ para todo $|\psi\rangle \in \mathcal{H}$. Denota-se $\rho \geq 0$.

3. *Normalização*: $\mathrm{Tr}(\rho) = 1$, onde $\mathrm{Tr}(.)$ denota traço.

[2]Mais informações sobre espaços de Hilbert, em particular sobre sua associação com sistemas quânticos, podem ser encontrados no livro de von Neumann [2].

[3]O termo *bracket* significa parênteses, em inglês.

[4]Um operador linear entre espaços $\mathcal{H}^{d_1}$ e $\mathcal{H}^{d_2}$ é uma função $\mathbf{A} : \mathcal{H}^{d_1} \to \mathcal{H}^{d_2}$. Definidas bases destes espaços, um operador pode ser identificado como uma matriz $d_2 \times d_1$. Usualmente escreve-se $\mathbf{A}|\psi\rangle$ para se denotar $\mathbf{A}(|\psi\rangle)$, e diz-se que um operador $\mathbf{A}$ é definido no espaço $\mathcal{H}$ se $\mathbf{A} : \mathcal{H} \to \mathcal{H}$.

[5]Dada uma base $\{|\xi_i\rangle\}$ de $\mathcal{H}$, um operador linear $\mathbf{A}$ pode ser escrito como $\mathbf{A} = \sum_{i,j} A_{ij}|\xi_i\rangle\langle\xi_j|$. O operador $\mathbf{A}^\dagger$ é representado, nesta base, por $\mathbf{A}^\dagger = \sum_{i,j} A^*_{ij}|\xi_j\rangle\langle\xi_i|$.

Todo operador densidade pode ser escrito como *combinação convexa* de projetores unidimensionais,

$$\rho = \sum_i q_i \left|\psi_i\right\rangle \left\langle\psi_i\right|; \quad \sum_i q_i = 1, \quad q_i \geq 0; \tag{1.1}$$

desde que $||\psi_i\rangle| = 1$. Esta decomposição, em geral, não é única. Contra-exemplos são os estado dados por um único projetor unidimensional, $\rho = |\psi\rangle \langle\psi|$. Um estado com esta característica é dito *puro*, e, sem ambigüidade, será descrito pelo vetor normalizado $|\psi\rangle$ somente. Estados que não são puros são ditos *mistos*.

1.1.1 Qubits

O *bit* é o conceito básico da teoria clássica da informação e da computação. A computação quântica e a teoria quântica da computação são construídas sobre um conceito análogo, o *bit quântico*, ou *qubit*.

Qubits são abstrações matemáticas que remetem aos sistemas quânticos mais simples, não triviais. Seu espaço de Hilbert associado é $\mathcal{H}^2 = \mathbb{C}^2$. Partículas de spin-1/2 (elétrons, pósitrons, e todos os demais férmions fundamentais), átomos de dois níveis eletrônicos, SQUIDs[6], e polarização de fótons são exemplos comuns de sistemas físicos que implementam qubits.

Em $\mathcal{H}^2$, a base ortonormal canônica, comumente chamada na literatura de *base computacional*, é definida como

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.2}$$

Um estado puro geral pode ser convenientemente parametrizado através de dois ângulos:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\text{sen}\left(\frac{\theta}{2}\right)|1\rangle, \tag{1.3}$$

sendo que $\theta \in [0, \pi]$, e $\phi \in [0, 2\pi]$. É importante destacar que fases globais não têm efeitos observáveis; por isso, $|\psi\rangle$ e $e^{i\gamma}|\psi\rangle$ representam o mesmo estado quântico.

Assim como os estados puros, estados mistos admitem uma parametrização conveniente. Definidas a *matriz identidade* - representação matricial do operador de mesmo nome - ,

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{1.4}$$

[6]Sigla para *superconducting quantum interference devices*, dispositivos supercondutores de interferência quântica.

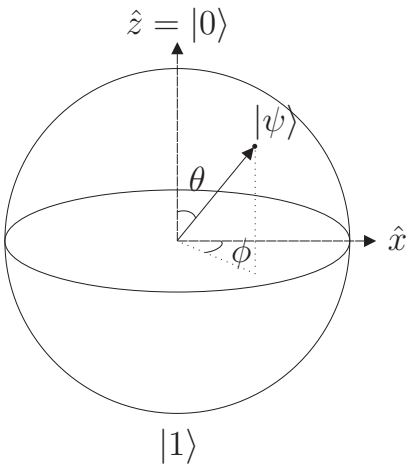

Figura 1.1: Esfera de Bloch. Representação geométrica do estado puro $|\psi\rangle$ de um qubit.

e as três *matrizes de Pauli*

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.5}$$

qualquer estado quântico de um qubit pode ser escrito como

$$\rho = \frac{\mathbf{1} + \vec{a}.\vec{\sigma}}{2}, \tag{1.6}$$

onde $\vec{a} \in \mathbb{R}^3$, $|\vec{a}| \leq 1$; $\vec{\sigma}$ é um vetor formado pelas matrizes de Pauli. Uma das grandes vantagens desta parametrização é a interpretação geométrica direta do espaço de estados de um qubit. A correspondência entre operadores densidade e vetores $\vec{a}$ é 1-para-1, e isso permite identificar o espaço de estados de $\mathcal{H}^2$ com a *bola* tridimensional de raio unitário, inserida em $\mathbb{R}^3$, formada pelos vetores reais $\vec{a}$ de norma menor ou igual a 1. Nesta correspondência, combinações convexas são preservadas, no sentido que, se ρ_1 é associado ao vetor $\vec{a}_1$ e ρ_2 associado a $\vec{a}_2$, então associado a $\vec{a}_3 \equiv q\,\vec{a}_1 + (1-q)\,\vec{a}_2$ está o operadors $\rho_3 = q\,\rho_1 + (1-q)\,\rho_2$, onde $q \in [0,1]$. Isso permite que os estados puros, que são *extremais* (não podem ser escritos como combinações convexas de outros estados), sejam identificados com os pontos na superfície desta bola, constituindo a chamada *esfera de Bloch* (*vide* [5], pg. 15, [6], pg. 10).

1.2 Sistemas compostos

O espaço de Hilbert associado a um sistema composto de duas ou mais partes é formado pelo *produto tensorial* dos espaços associados aos subsistemas. Um sistema bipartido, constituído de subsistemas cujos espaços de Hilbert são $\mathcal{H}_A$ e $\mathcal{H}_B$, tem associado a si o espaço $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. A extensão para sistemas de mais partes é trivial.

Sejam $\{|\xi_i\rangle\}$ e $\{|\varphi_j\rangle\}$ bases ortonormais de $\mathcal{H}_A$ e $\mathcal{H}_B$, respectivamente. Qualquer estado puro de $\mathcal{H}_{AB}$ pode ser escrito como

$$|\psi\rangle = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} c_{ij} \, |\xi_i\rangle \otimes |\varphi_j\rangle \,, \quad \sum_{ij} |c_{ij}|^2 = 1. \tag{1.7}$$

Um importante teorema, conhecido como *decomposição de Schmidt* (*vide* [5], pg. 109), tem o seguinte enunciado: para todo $|\psi\rangle \in \mathcal{H}_{AB}$, existem bases ortonormais $\{|\xi_i'\rangle\}$ de $\mathcal{H}_A$ e $\left\{\left|\varphi_j'\right\rangle\right\}$ de $\mathcal{H}_B$, e números reais não-negativos c_i tais que

$$|\psi\rangle = \sum_{i=1}^{d_A} c_i \, |\xi_i'\rangle \otimes |\varphi_i'\rangle \,, \quad \sum_{i} c_i^2 = 1. \tag{1.8}$$

A soma tem um só índice, e assumiu-se, sem perda de generalidade, que $d_A \leq d_B$. Existem infinitas bases ortonormais distintas nas quais um estado puro pode ser decomposto na forma (1.8); os coeficientes c_i, ao contrário, são únicos.

Um caso particular que mostra a força deste resultado é aquele em que $d_A = 2$. O estado puro de um sistema bipartido em que uma das partes é um qubit é, efetivamente, um estado puro de um sistema de dois qubits, qualquer que seja d_B.

1.2.1 Emaranhamento

Um dos mais intrigantes aspectos da mecânica quântica toma, neste ponto, sua forma. Suponha que um sistema bipartido se encontra no estado puro $|\psi\rangle$ tal que, em sua decomposição de Schmidt, dois ou mais *coeficientes de Schmidt* c_i sejam não-nulos. Então, é *impossível* escrever o estado $|\psi\rangle$ como produto tensorial de estados dos subsitemas, $|\psi\rangle \neq |\xi\rangle \otimes |\varphi\rangle$. Em outras palavras, não é possível identificar os estados individuais das partes do sistema, mesmo se sabendo o estado $|\psi\rangle$ do sistema composto. Estados com esta característica apresentam uma importante propriedade chamada *emaranhamento*.

O termo emaranhamento - *verschränkung*, em alemão - foi cunhado por Erwin Schrödinger em 1935 [7] para descrever estes estados fortemente

correlacionados. Uma definição formal de seu significado, porém, data de 1989 [8], por Reinhardt Werner.

Considere um sistema quântico bipartido, cujo espaço de Hilbert seja $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Um estado *produto* - ou *não-correlacionado* - deste sistema é um estado da forma $\rho^{AB} = \rho^A \otimes \rho^B$, onde ρ^A e ρ^B são os estados dos subsistemas A e B, respectivamente. Um estado produto pode ser facilmente preparado usando-se dois dispositivos preparadores, que funcionam independentemente e preparam os estados ρ^A e ρ^B, respectivamente. Agora, suponha que cada um dos dispositivos preparadores é capaz preparar n diferentes estados; escolhendo-se um número $r \in \{1, 2, ..., n\}$, os dispositivos preparam o subsistema A no estado ρ_r^A e o subsistema B no estado ρ_r^B. Se um gerador de números aleatórios, que produz os números $r \in \{1, 2, ..., n\}$ com probabilidade p_r, opera em conjunto com estes dispositivos, é possível correlacionar as preparações e obter estados da forma

$$\rho = \sum_{r=1}^{n} q_r \rho_r^A \otimes \rho_r^B, \quad q_r \geq 0, \quad \sum_{r=1}^{n} q_r = 1. \tag{1.9}$$

Estes estados são ditos *separáveis* ou *classicamente correlacionados*. Estados que não podem ser assim preparados, e são incompatíveis com a forma (1.9), são ditos *emaranhados*.

1.2.2 Traço parcial

O traço parcial é a operação que representa o descarte de partes do sistema. Ele esté relacionado a situações em que se tem interesse exclusivo em uma parte do sistema composto, e é utilizado na obtenção do *estado reduzido* desta parte.

Considere um sistema quântico bipartido no estado ρ, que, definidas bases $\{|\xi_i\rangle\}$ e $\{|\varphi_\mu\rangle\}$[7] de $\mathcal{H}_A$ e $\mathcal{H}_B$, respectivamente, pode ser escrito como

$$\rho = \sum_{i,\mu,j,\nu} \rho_{i\mu,j\nu} \left|\xi_i\, \varphi_\mu\right\rangle \left\langle \xi_j\, \varphi_\nu\right|. \tag{1.10}$$

onde $|\xi\, \varphi\rangle \equiv |\xi\rangle \otimes |\varphi\rangle$. O estado reduzido ρ_A do subsistema A, nesta base, pode ser representado por

$$\rho_A \equiv \mathrm{Tr}_B(\rho) = \sum_{i,j} \sum_{\mu} \rho_{i\mu,j\mu} \left|\xi_i\right\rangle \left\langle \xi_j\right|. \tag{1.11}$$

[7] índices latinos remetem ao subsistema A e, índices gregos, ao subsistema B.

De forma análoga, o estado reduzido ρ_B do subsistema B é

$$\rho_B \equiv \mathrm{Tr}_A(\rho) = \sum_{\mu,\nu} \sum_i \rho_{i\mu,i\nu} |\varphi_\mu\rangle \langle\varphi_\nu| . \tag{1.12}$$

É muito importante observar que o estado de um sistema composto não é, necessariamente, o produto tensorial dos estados reduzidos. Isso é verdade apenas para estados não-correlacionados, uma vez que, tomado o traço parcial, todas as correlações entre os subsistemas, sejam elas clássicas ou não, são ignoradas.

1.3 Medições

Que informação sobre o sistema um estado quântico traz consigo? A resposta desta questão envolve mais uma das interessantes e perturbadoras características da mecânica quântica: seu caráter probabilístico. Nas palavras de Asher Peres ([1], pg. 13):

> 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.

Não é possível, de acordo com o formalismo quântico, prever deterministicamente o resultado de todas as medições que podem ser realizadas em um sistema quântico, mesmo que se tenha o melhor conhecimento possível[8] acerca do sistema em questão.

Devido a este caráter probabilístico, as previsões da mecânica quântica só podem ser testadas se um grande número de cópias do sistema for identicamente preparado no mesmo estado, e medições forem realizadas igualmente em todas elas. Desta forma, as distribuições estatísticas dos resultados podem ser comparadas com as probabilidades previstas. Neste sentido, o estado pode ser entendido como a descrição de um *ensemble* de sistemas identicamente preparados, do qual o sistema em questão é um elemento aleatoriamente escolhido.

Uma medição quântica é descrita por um conjunto de *operadores de medição*, definidos no espaço de Hilbert do sistema. Cada operador é associado a um possível resultado da medição, e sua natureza matemática varia de acordo com a classe de medições considerada. Nesta seção, serão

[8] Segundo a mecânica quântica, a melhor descrição possível de um sistema é feita através de um estado puro. Isso porque, para estados puros, existe pelo menos uma medição completa para a qual o resultado pode ser deterministicamente previsto.

apresentadas duas importantes classes de medições quânticas: as *medições projetivas* (MPs) e as *medições por operadores positivos* (POVMs)[9].

1.3.1 Medições projetivas

Em uma medição projetiva (MP) x, realizada em um sistema quântico cujo espaço de Hilbert é $\mathcal{H}^d$, cada resultado a é associado a um projetor $\mathbf{\Pi}_{a|x}$, de forma que projetores associados a resultados diferentes correspondam a subespaços ortogonais, *i.e.*, $\mathrm{Tr}\left(\mathbf{\Pi}_{a|x}\mathbf{\Pi}_{a'|x}\right) = \delta_{a,a'}$, e $\sum_{a=0}^{d'} \mathbf{\Pi}_{a|x} = \mathbf{1}$. Sem perda de generalidade, os resultados serão rotulados $a \in \{0, ..., d'-1\}$, onde $d' \leq d$ é o número de possíveis resultados da medição. A MP é dita *completa* se $d' = d$; neste caso, todos projetores correspondem a subespaços unidimensionais de $\mathcal{H}^d$.

Realizada uma medição x em um sistema quântico cujo estado é ρ, a probabilidade do resultado a ser obtido é dada por

$$p_{a|x} = \mathrm{Tr}\left(\rho\, \mathbf{\Pi}_{a|x}\right). \tag{1.13}$$

Uma propriedade importante que destaca a classe de medições projetivas é a *reprodutibilidade*: caso a mesma MP seja realizada mais de uma vez, de forma consecutiva, o resultado obtido na primeira realização é reobtido nas demais com probabilidade 1, qualquer que seja ele. Esta propriedade se reflete no formalismo através do estado do sistema após a medição. Supondo que, realizada a MP x, o resultado a foi obtido, o sistema quântico é, então, descrito pelo estado

$$\rho' = \frac{\mathbf{\Pi}_{a|x}\, \rho\, \mathbf{\Pi}_{a|x}}{\mathrm{Tr}\left(\rho\, \mathbf{\Pi}_{a|x}\right)}. \tag{1.14}$$

Outro importante conceito ligado a esta classe de medições é o de *observável*. Um observável é um operador hermitiano definido no espaço de Hilbert do sistema, associado a uma medição projetiva. Entende-se que, quando uma medição é experimentalmente realizada, o que se observa são números reais o_a; os rótulos a indexam os possíveis resultados. Um observável $\mathbf{O}$ associado à medição x tem a decomposição espectral:

$$\mathbf{O}_x \equiv \sum_{a=0}^{d'} o_a \mathbf{\Pi}_{a|x}. \tag{1.15}$$

O valor esperado de um observável é dado pela média dos resultados o_a, pesados pela probabilidade do valor a ser obtido na medição projetiva as-

[9] O acrônimo POVM remete a *positive operator-value measure*.

sociada. Assim,

$$\langle \mathbf{O}_x \rangle_\rho = \sum_{a=0}^{d'} o_a \, p_{a|x} = \mathrm{Tr}\left(\rho \, \mathbf{O}\right). \tag{1.16}$$

Segue de sua definição que a medição de um observável é reprodutível.

Suponha que, em um sistema quântico, é realizada a medição do observável $\mathbf{O}_1$, seguida da medição do oberservável $\mathbf{O}_2$. Se após a medição de $\mathbf{O}_2$ é realizada uma segunda medição de $\mathbf{O}_1$, e esta reproduz o resultado obtido na primeira, $\mathbf{O}_1$ e $\mathbf{O}_2$ são ditos *compatíveis*[10]. A compatibilidade entre dois observáveis permite que os resultados das medições de ambos sejam simultaneamente conhecidos, pois são independentes da ordem em que estas medições são realizadas. Dois observáveis são compatíveis se, e somente se, eles *comutam*, *i.e.*, $[\mathbf{O}_1, \mathbf{O}_2] \equiv \mathbf{O}_1\mathbf{O}_2 - \mathbf{O}_2\mathbf{O}_1 = 0$.

1.3.2 POVMs

O formalismo de MPs apresentado envolve dois principais elementos, as regras que permitem calcular as probabilidades dos possíveis resultados e, realizada a medição, a descrição o estado posterior do sistema. Contudo, em algumas aplicações o estado do sistema após a medição é de pouco interesse, ou mesmo não tem sentido físico - medições realizadas através da detecção de fótons, por exemplo. Para estes casos, em que o foco é voltado para as probabilidades de se obter os resultados, o formalismo de POVMs é especialmente eficaz.

Em um *POVM* x, realizado em um sistema cujo espaço de Hilbert é $\mathcal{H}^d$, aos possíveis resultados a são associados operadores $\mathbf{E}_{a|x}$ chamados *efeitos*. Eles devem satisfazer:

- $\mathbf{E}_{a|x} \geq 0$;
- $\sum_{a=0} \mathbf{E}_{a|x} = \mathbf{1}$.

A probabilidade do resultado a ser obtido se o estado do sistema é ρ é dada por

$$p_{a|x} = \mathrm{Tr}\left(\rho \mathbf{E}_{a|x}\right). \tag{1.17}$$

Ao contrário do que acontece nas MPs, o número de efeitos - conseqüentemente, o número de possíveis resultados da medição - não é limitado pela dimensão do espaço de Hilbert associado ao sistema. Em geral, POVMs

[10] Compatibilidade de observáveis é um conceito quântico, relacionado às *relações de incerteza* de Heisenberg (*vide* [5], pg. 89). Na mecânica clássica, todas os observáveis são compatíveis.

não são reprodutíveis, e não é possível determinar o estado do sistema após a medição. Um caso especial é aquele em que todos os efeitos são da forma $\mathbf{E}_{a|x} = \mathbf{M}_{a|x}^{\dagger}\mathbf{M}_{a|x}$, para algum conjunto de operadores $\left\{\mathbf{M}_{a|x}\right\}$. O estado posterior à medição pode ser escrito como

$$\rho' = \frac{\mathbf{M}_{a|x}\,\rho\,\mathbf{M}_{a|x}^{\dagger}}{\mathrm{Tr}\left(\rho\,\mathbf{E}_{a|x}\right)}. \tag{1.18}$$

Em particular, os operadores $\mathbf{M}_{a|x}$ podem ser projetores, caso em que POVMs se resumem a MPs. Neste sentido, a classe de medições por operadores positivos é mais geral que a classe de medições projetivas. Por outro lado, todas as probabilidades obtidas através de um POVM realizado em um sistema quântico de espaço de Hilbert $\mathcal{H}^d$ podem ser reproduzidas em uma MP realizada em um sistema de espaço $\mathcal{H}^{d'}$, onde $d' \geq d$. Este resultado segue do *teorema de Neumark* (*vide* [1], pg. 285).

2

O paradoxo de EPR

> Very simple was my explanation, and plausible enough - as most wrong theories are!
>
> - *The Time Machine*, de H.G. Wells.

Em 1935, Albert Einstein, Boris Podolski e Nathan Rosen - EPR - publicaram, na *Physical Review*, um artigo intitulado *"Can quantum-mechanical description of physical reality be considered complete?"* [9]. Nele, propuseram um experimento de pensamento[1] que, segundo os autores, demonstrava que a mecânica quântica não era uma teoria completa, uma descrição satisfatória da natureza.

Neste capítulo apresentamos o chamado *paradoxo de EPR* como uma introdução histórica e conceitual aos capítulos seguintes. Introduzimos os principais conceitos, e, seguindo a formulação de David Bohm ([10], pg. 611), apresentamos os argumentos que levaram EPR a questionar a completude da teoria quântica.

2.1 Realidade

Segundo EPR, duas questões são primordiais para se determinar o sucesso de uma teoria física:

1. A teoria é correta?
2. A descrição dada pela teoria é completa?

Para eles, uma teoria satisfatória deve responder positivamente a ambas.

A primeira questão é respondida comparando-se as previsões da teoria com observações experimentais; o grau de concordância entre estes dois

[1] Do alemão *gedankenexperiment*.

fatores determina quão correta é a teoria. A resposta à segunda questão, no entanto, não é tão direta, e envolve, primeiramente, que se faça uma definição precisa do termo *completa*. Segundo EPR, para que uma teoria seja completa, é necessário que todo *elemento da realidade* seja representado por um elemento correspondente na teoria. Para que uma grandeza física seja um elemento da realidade, por sua vez, é suficiente que satisfaça o seguinte critério, como originalmente enunciado em [9]:

> If, without in any way disturbing a system, we can predict with certainty (*i.e.*, with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.

Neste critério é possível observar uma hipótese forte que reflete o posicionamento dos autores - e também de uma ampla corrente de cientistas e filósofos - frente ao que se entende por realidade, hoje conhecida como *realismo local*. Pressupor *realismo* é assumir que as propriedades físicas de uma partícula ou corpo, *e.g.*, sua posição e momento, têm existência intrínsica, independente da observação. Realizadas medições nestas partículas, seus resultados meramente revelariam tais propriedades pré-existentes. Realismo local, por sua vez, é a premissa de que estas propriedades físicas estão localmente atribuídas à partícula, e a única forma de modificá-las é intervir diretamente no sistema físico em questão.

2.2 O experimento de EPR-Bohm

Considere um sistema quântico de 2 qubits preparado no estado puro

$$\left|\psi^{-}\right\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.1}$$

Suponha que em uma das partículas, A, é realizada a medição de um observável arbitrário $\mathbf{V}$, e, em seguida, é realizada a medição do mesmo observável na partícula B. Seja

$$\mathbf{V} \equiv v_0\mathbf{\Pi}_0 + v_1\mathbf{\Pi}_1 = v_0\left|\xi_0\right\rangle\left\langle\xi_0\right| + v_1\left|\xi_1\right\rangle\left\langle\xi_1\right|, \tag{2.2}$$

onde $v_0, v_1 \in \mathbb{R}$, e $\langle \xi_i \mid \xi_j \rangle = \delta_{i,j}$. Este operador induz observáveis

$$\mathbf{V}^A = \mathbf{V} \otimes \mathbf{1}, \tag{2.3}$$

$$\mathbf{V}^B = \mathbf{1} \otimes \mathbf{V}; \tag{2.4}$$

definidos no espaço de Hilbert do sistema composto. A medição de $\mathbf{V}$ no subsistema A é dada pela medição de $\mathbf{V}^A$ no sistema bipartido.

Para avaliar as probabilidades dos resultados v_0 e v_1 serem obtidos em cada uma das medições, é conveniente representar o estado (2.1) na base de $\mathcal{H}^2$ formada pelos autovetores de $\mathbf{V}$. Os elementos da base computacional podem ser escritos, de forma geral, em uma base arbitrária ortogonal $\{|\xi_0\rangle, |\xi_1\rangle\}$ como

$$|0\rangle = \cos\left(\frac{\theta}{2}\right)|\xi_0\rangle + e^{i\phi}\text{sen}\left(\frac{\theta}{2}\right)|\xi_1\rangle, \tag{2.5a}$$

$$|1\rangle = \text{sen}\left(\frac{\theta}{2}\right)|\xi_0\rangle - e^{i\phi}\cos\left(\frac{\theta}{2}\right)|\xi_1\rangle, \tag{2.5b}$$

Substituindo no estado (2.1), tem-se, a menos de uma fase global,

$$\left|\psi^-\right\rangle = \frac{|\xi_0\,\xi_1\rangle - |\xi_1\,\xi_0\rangle}{\sqrt{2}}. \tag{2.6}$$

Assim, na medição de $\mathbf{V}^A$, a probabilidade de se obter o resultado v_0 é

$$p_0 = \text{Tr}\left(\left|\psi^-\right\rangle\left\langle\psi^-\right|\left(|\xi_0\rangle\langle\xi_0|\otimes\mathbf{1}\right)\right) = \frac{1}{2}. \tag{2.7}$$

Uma vez obtido este resultado, o estado pós-medição do sistema é

$$|\psi\rangle' = |\xi_0\rangle|\xi_1\rangle. \tag{2.8}$$

Realizada, pois, a medição de $\mathbf{V}^B$ neste novo estado do sistema, o resultado v_1 é obtido com probabilidade 1. Voltando à medição de $\mathbf{V}^A$, no estado (2.1), a probabilidade de se obter v_1 é, também, $p_1 = 1/2$. Obtendo-se este resultado, o sistema passa a ser descrito pelo estado

$$|\psi\rangle' = |\xi_1\rangle|\xi_0\rangle. \tag{2.9}$$

Da medição de $\mathbf{V}^B$ neste estado, obtém-se, com probabilidade 1, o resultado v_1. É uma importante propriedade do estado (2.1) - conhecido como *estado singleto de spin*, por razões históricas - que, realizadas medições de um mesmo observável nas duas partes do sistema, os resultados obtidos serão diferentes, e isto com probabilidade 1, qualquer que seja o observável medido.

Suponha que duas partes remotamente afastadas compartilham sistemas quânticos no estado (2.1). Por hipótese, as partículas não mais interagem, devido à distância que as separa, e, por isso, uma medição no subsistema

A não pode ter influência alguma, instantaneamente, no subsistema B. Sabendo-se que o sistema se encontra no estado singleto (2.1), é possível, a partir da medição do observável $\mathbf{V}^A$, determinar com probabilidade 1 o resultado da medição de $\mathbf{V}^B$, sem que qualquer intervenção seja realizada no subsistema B. Da mesma forma, a partir da medição de um observável $\mathbf{W}^B$, é possível determinar o resultado da medição de $\mathbf{W}^A$. Segundo o critério de EPR, portanto, $\mathbf{V}^B$ e $\mathbf{W}^A$ são elementos da realidade, localmente definidos como propriedades intrínsicas às partículas B e A, respectivamente, que têm existência independente e prévia às medições realizadas nas partículas A e B.

Na mecânica quântica, se duas grandezas físicas são descritas por observáveis $\mathbf{V}$ e $\mathbf{W}$ que não comutam, $[\mathbf{V}, \mathbf{W}] \neq 0$, não existe estado quântico, puro ou misto, para o qual os resultados das medições de ambos os observáveis possam ser determinados simultaneamente. Segundo as definições de EPR, desta impossibilidade segue que, ou (1) a descrição quântica da natureza não é completa, ou (2) ambas as quantidades não podem ter realidade simultânea, ou seja, não correspondem, simultaneamente, a elementos da realidade.

Pressuponha que a premissa (1) é falsa; a melhor descrição possível do sistema é dada pelo estado singleto. A única possibilidade restante é que seja verdadeira a premissa (2). No entanto, observe que, mesmo que $[\mathbf{V}, \mathbf{W}] \neq 0$, é sempre verdade que $\left[\mathbf{V}^A, \mathbf{W}^B\right] = 0$, ou seja, os resultados das medições de $\mathbf{V}^A$ e $\mathbf{W}^B$ podem ser determinados simultaneamente. Determinados, pois, estes resultados, somados à conclusão prévia de que $\mathbf{V}^B$ e $\mathbf{W}^A$ são elementos da realidade, o que se tem é que são elementos da realidade, simultaneamente, os resultados de $\mathbf{V}^A$ e $\mathbf{W}^A$, e $\mathbf{V}^B$ e $\mathbf{W}^B$, mesmo que $\left[\mathbf{V}^A, \mathbf{W}^A\right] = \left[\mathbf{V}^B, \mathbf{W}^B\right] \neq 0$. Esta conclusão implica que a premissa (2) é falsa. Deste aparente paradoxo, EPR concluem que a premissa (1) é verdadeira, *i.e.*, a mecânica quântica não é uma teoria completa.

3

Correlações locais

...correlations cry out for explanation.

- John Bell.

Em 1964, John Bell lançou nova luz à questão colocada por Einstein, Podolski e Rosen em [9]. No artigo "*On the EPR paradox*" [11], Bell interpretou de forma brilhante a hipótese de realismo local, implícita nos elementos de realidade de EPR, e a incorporou em um novo formalismo matemático, destacando as principais características de qualquer teoria em que esta hipótese é assumida.

Neste capítulo[1], apresentamos o formalismo de correlações e os cenários de Bell, a importante hipótese de causalidade local e as conseqüências de sua pressuposição. A estrutura das correlações locais é estudada em detalhes, evidenciando a rica matemática por trás das conhecidas desigualdades de Bell.

3.1 Probabilidades conjuntas e marginais

Suponha o seguinte cenário. Duas partículas, A e B, são criadas em uma fonte F, e enviadas a laboratórios L_A e L_B, respectivamente. É muito comum em textos de teoria quântica da informação associar observadores fictícios aos laboratórios. Como na maioria deles, nesta dissertação Alice comandará os procedimentos no laboratório L_A, e Bob será o chefe do laboratório L_B. Assim que as partículas chegam aos respectivos laboratórios, Alice e Bob devem realizar medições. De um conjunto Q_A das possíveis medições que pode realizar, Alice opta pela medição x; da mesma forma, de um conjunto Q_B, Bob decide pela medição y. As medições escolhidas

[1]Este capítulo foi inspirado na referência [12].

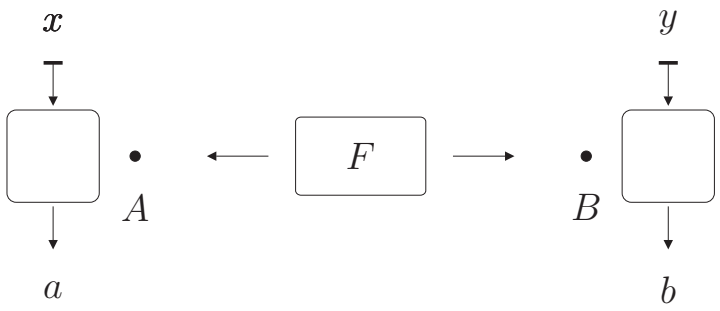

Figura 3.1: A fonte F produz pares de partículas A e B, que são submetidas às medições x e y, respectivamente. Os resultados obtidos são a e b.

têm, cada uma, um conjunto de possíveis resultados: R_x, para cada medição x, e R_y, para cada medição y. Elementos destes conjuntos, os resultados obtidos por Alice e Bob são, respectivamente, a e b.

De forma geral, a melhor descrição deste experimento é feita através das probabilidades conjuntas de se obter cada par de possíveis resultados a e b quando são realizadas as medições x e y. Esta probabilidade será denotada $p_{a,b|x,y}$.

Cada uma das partes pode descrever seu experimento individual através de *probabilidades marginais*:

$$p_{a|x,y} \equiv \sum_b p_{a,b|x,y}; \tag{3.1a}$$

$$p_{b|x,y} \equiv \sum_a p_{a,b|x,y}. \tag{3.1b}$$

A primeira, (3.1a), representa a probabilidade de Alice observar o resultado a quando realiza o experimento x e Bob realiza o experimento y. Esta dependência na medição y pode ser justificada se, por exemplo, o aparato experimental de Bob conter um transmissor que se comunica com um receptor no aparato de Alice. O mesmo vale para a probabilidade marginal de Bob, (3.1b).

3.2 Não-sinalização

Suponha, agora, que os laboratórios estão *remotamente afastados*, sendo d a distância que os separa. Ainda, suponha que as medições em L_A e L_B sejam *sincronizadas*. Estas condições são introduzidas com o objetivo de prevenir que informações sejam transmitidas de um laboratório a outro enquanto

as medições são realizadas. No pior dos casos, o objetivo é evitar que um sinal luminoso emitido em L_A no instante em que Alice opta pela medição x percorra a distância d até L_B antes que o resultado b seja obtido. O mesmo deve ser verdade para qualquer sinal equivalente emitido em L_B. Desta forma, não é necessário que as medições ocorram de maneira estritamente simultânea; é suficiente que cada uma delas tenha fim em um tempo $t < d/c$ após o início da outra, onde c é a velocidade da luz no meio por onde é transmitido o sinal.

Tais condições podem ser melhor formuladas em uma linguagem própria da teoria da relatividade especial. Um *evento* é definido como um *ponto* no espaço-tempo, um conceito geral utilizado como referência a algo que ocorre em um ponto no espaço em um instante de tempo. O termo *evento de medição* será utilizado com um significado um pouco mais amplo, como referência às *regiões* do espaço-tempo nas quais ocorrem os processos de medição de Alice e Bob[2]. Seja $\mathcal{M}_A$ um evento de medição que ocorre em L_A, que tem início na *escolha* da medição x e término na obtenção do resultado a. Da mesma forma, $\mathcal{M}_B$ é definido como um evento de medição que ocorre em L_B, que tem início na escolha da medição y e término na obtenção do resultado b. Diz-se que $\mathcal{M}_A$ e $\mathcal{M}_B$ têm uma *separação tipo espaço* caso nenhum sinal possa ser enviado entre eles em velocidade não superior à da luz, em qualquer referencial inercial. Para que esta condição seja verdadeira, é necessário e suficiente que $\mathcal{M}_A$ não intersecte o cone de luz de $\mathcal{M}_B$, e nem $\mathcal{M}_B$ o cone de luz de $\mathcal{A}$, em qualquer referencial inercial.

Esta restrição tem reflexos nas probabilidades $p_{a,b|x,y}$ que descrevem o experimento. Considere o seguinte contexto, onde esta afirmação fica evidente. Tome dois eventos de medição $\mathcal{M}_A$ e $\mathcal{M}_B$, espacialmente separados, em que A e B são *ensembles* de partículas idênticas, cujos representantes são criados aos pares na fonte F; cada par criado é constituído de um representante de A e um representante de B. As medições x e y são realizadas individualmente e simultaneamente em todos os representantes do *ensemble* correspondente, e, dos resultados obtidos, pode-se inferir sua distribuição estatística. No limite em que os *ensembles* têm um grande número de partículas, as distribuições estatísticas obtidas tendem para as distribuições de probabilidades que descrevem o experimento. Alice e Bob podem, localmente, inferir as distribuições marginais de seus resultados. Se a distribuição marginal observada por Alice, por exemplo, pudesse depender da medição escolhida por Bob, Alice poderia, através de seus resul-

[2]No contexto considerado, pode-se, sem prejuízo algum para o formalismo, definir que as medições são instantâneas e ocorrem em um único ponto no espaço, constituindo, portanto, eventos, no sentido estrito do termo.

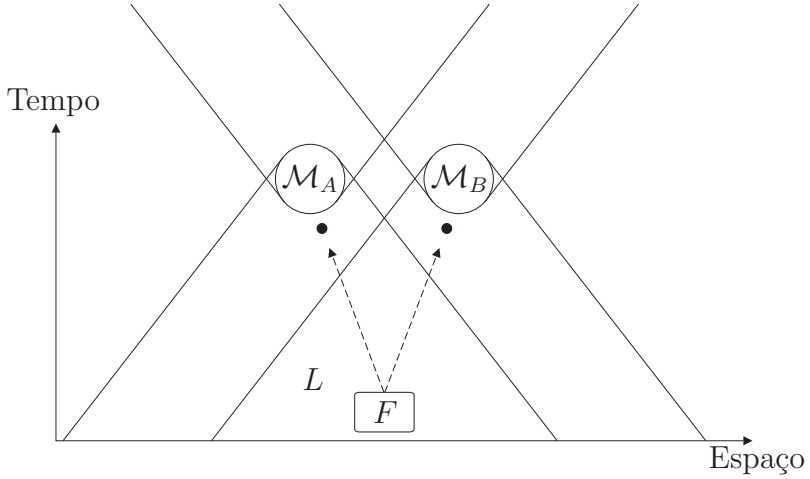

Figura 3.2: Eventos de medição $\mathcal{M}_A$ e $\mathcal{M}_B$ espacialmente separados.

tados somente, obter informações sobre y. Escolhendo sua medição, Bob poderia enviar uma mensagem a Alice. Como os eventos de medição são espacialmente separados, esta informação necessariamente teria percorrido a distância d que separa os laboratórios em velocidade superluminal. Para que isto seja evitado, deve valer a seguinte *condição de não-sinalização*,

$$\sum_{b\in R_y} p_{a,b|x,y} = \sum_{b\in R_{y'}} p_{a,b|x,y'} = p_{a|x}, \quad \forall\ a,x,y,y'; \tag{3.2a}$$

$$\sum_{a\in R_x} p_{a,b|x,y} = \sum_{a\in R_{x'}} p_{a,b|x',y} = p_{b|y}, \quad \forall\ b,x,x',y. \tag{3.2b}$$

3.3 Causalidade local

A condição de não-sinalização não é suficiente para garantir que dois eventos de medição, $\mathcal{M}_A$ e $\mathcal{M}_B$, sejam *independentes*, mesmo que espacialmente separados. Neste contexto, apesar de prevenir que mensagens sejam transmitidas a velocidades arbitrárias, esta condição nada diz a respeito de possíveis *correlações* existentes entre os sistemas, não sendo detectadas nas probabilidades marginais. Os eventos são correlacionados caso as probabilidades conjuntas que descrevem o experimento não sejam iguais ao produto de suas probabilidades marginais, *i.e.*,

$$p_{a,b|x,y} \neq p_{a|x}\, p_{b|y}. \tag{3.3}$$

Classicamente, correlações são fruto de *relações causais* - ou seja, da existência de *causas* e *efeitos* associados - entre eventos, sejam elas diretas

ou indiretas. Relações causais diretas seriam aquelas em que uma causa associada ao evento $\mathcal{A}$, diga-se, implicaria um efeito associado ao evento $\mathcal{B}$. Relações causais indiretas seriam aquelas estabelecidas por uma causa comum que implicaria efeitos associados a ambos os eventos $\mathcal{A}e\mathcal{B}$. Neste contexto surge a hipótese de *causalidade local*, que diz que, para que qualquer relação causal seja estabelecida entre dois eventos, é necessário que informação seja transmitida entre eles a velocidade igual à da luz ou inferior. Assumindo-se que os eventos de medição são espacialmente separados, relações causais diretas são automaticamente excluídas como possível explicação de quaisquer correlações. Restam, portanto, as relações causais indiretas, que, ligadas à hipótese de causalidade local, implicam que todas as correlações existentes entre $\mathcal{M}_A$ e $\mathcal{M}_B$ têm origem no passado comum dos eventos - a região L na figura 3.2.

Para formalizar esta idéia, suponha uma teoria em que, dada uma coleção de variáveis λ, seja possível calcular a probabilidade $p_{a,b|x,y,\lambda}$ de se obter os resultados a e b nas medições x e y. Suponha ainda que a coleção λ seja *completa*, e represente *todas* as variáveis que poderiam ser causas locais de ambos os eventos de medição. Nenhuma hipótese será assumida quanto à natureza destas variáveis: se são reais ou complexas, contínuas ou discretas. Suponha também que esta teoria assume a hipótese de causalidade local - teorias que assumem esta hipótese serão ditas *locais*. Assim, fixadas λ, nenhum outro fator seria capaz de correlacionar os eventos $\mathcal{M}_A$ e $\mathcal{M}_B$, que, assim, tornar-se-iam independentes, *i.e.*,

$$p_{a,b|x,y,\lambda} = p_{a|x,\lambda}\, p_{b|y,\lambda}. \tag{3.4}$$

Dadas as probabilidades $p_{a,b|x,y}$, para se saber se as correlações por elas descritas admitem uma *interpretação local* é necessário que nenhuma teoria seja descartada *a priori*. Devem ser consideradas, inclusive, todas aquelas em que λ representa variáveis não consideradas em nenhuma teoria atual, possivelmente porque são grandezas ligadas a um grau de refinamento experimental ainda não alcançado, ou a teorias mais gerais, ainda não descobertas. Em outras palavras, λ pode representar "variáveis ocultas". Sem que haja perda de generalidade, assumir-se-á que λ é uma única variável contínua, representando esta coleção de variáveis. Na falta de conhecimento completo a respeito desta variável - conhecimento este que é virtualmente inacessível mesmo em teorias locais nas quais esta variável representa grandezas, diga-se, mais "ortodoxas" que "ocultas" - , a melhor forma de descrever o experimento é através da média sobre seus valores,

$$p_{a,b|x,y} = \int_\Lambda q_\lambda\, p_{a|x,\lambda}\, p_{b|y,\lambda}\, d\lambda, \tag{3.5}$$

onde q_λ é uma distribuição da variável λ em um conjunto Λ. Assim, segundo teorias locais, as correlações observadas são fruto da ignorância a respeito da variável λ, e serão ditas *correlações locais* todas as probabilidades $p_{a,b|x,y}$ que podem ser escritas na forma (3.5).

3.4 Cenários de Bell

Um *cenário de Bell* é um experimento de pensamento em que duas ou mais partes recebem partículas preparadas na mesma fonte, e, cada uma delas, de um conjunto pré-estabelecido de medições, deve escolher aquela que irá realizar, respeitando a condição de que todos os eventos de medição tenham separação tipo espaço. Determinam um cenário de Bell os seguintes valores, que devem ser finitos:

- o número de partes;
- o número de possíveis medições de cada parte;
- o número de possíveis resultados de cada possível medição de cada parte.

Esta caracterização é feita através da notação

$$(v_{10}, \ldots, v_{1m_1-1}; v_{20}, \ldots, v_{2m_2-1}; \ldots; v_{n1}, \ldots, v_{nm_n-1}), \tag{3.6}$$

onde v_{ij} é o número de possíveis resultados da medição j da parte i. Por exemplo, $(3, 3; 2, 2, 4)$ denota um cenário de Bell de 2 partes, em que a primeira parte pode realizar 2 medições, cada uma com 3 possíveis resultados, e a segunda parte pode realizar 3 medições, duas das quais têm 2 possíveis resultados e a terceira 4 possíveis resultados. Está implícito que, em um cenário de n partes, elas serão indexadas por $i \in \{1, \ldots, n\}$, e as medições da parte i, indexadas por $j \in Q_i = \{0, \ldots, m_i - 1\}$. Caso necessário, os possíveis resultados da medição j, na parte i, serão indexados por $r \in R_{ij} = \{0, \ldots, v_{ij} - 1\}$. Cenários em que as n partes podem realizar o mesmo número m de medições, todas elas com v possíveis resultados, serão denotados por (n, m, v). Nos cenários de duas e três partes serão adotadas as seguintes notação e nomenclatura: as partes serão chamadas Alice, Bob e Charlie, ou A, B e C; os índices das respectivas medições serão x, y e z; os índices dos respectivos resultados serão a, b e c.

Definido um cenário de Bell, sua descrição é feita através das probabilidades conjuntas de ocorrência de todas as possíveis configurações de resultados e medições. Neste contexto geral, nenhuma hipótese, condição

ou teoria é assumida *a priori*, a não ser a condição de não-sinalização, que, por definição, deve ser satisfeita. No entanto, é interessante saber, dadas as correlações que descrevem o cenário, se admitem ou não interpretação local. As *desigualdades de Bell* são as mais importantes ferramentas que permitem discriminar correlações locais e correlações não-locais. Introduzidas por John Bell, em [11], essas desigualdades evidenciam vínculos não-triviais que, necessariamente, são satisfeitos por todas as correlações locais.

3.4.1 A desigualdade CHSH

Tome o cenário $(2, 2, 2)$, descrito por 16 probabilidades conjuntas,

$$p_{a,b|x,y} \quad \forall\ a, b, x, y \in \{0, 1\}\,. \tag{3.7}$$

Considere a seguinte expressão:

$$\begin{aligned}\beta_{CHSH} \equiv p_{a=b|0,0} - p_{a\neq b|0,0} + p_{a=b|0,1} - p_{a\neq b|0,1} + \\ + p_{a=b|1,0} - p_{a\neq b|1,0} - p_{a=b|1,1} + p_{a\neq b|1,1},\end{aligned} \tag{3.8}$$

onde $p_{a=b|x,y} = p_{0,0|x,y} + p_{1,1|x,y}$ e $p_{a\neq b|x,y} = p_{0,1|x,y} + p_{1,0|x,y}$. Suponha que as correlações que descrevem este cenário são locais, *i.e.*, existem q_λ, $p_{a|x,\lambda}$ e $p_{b|y,\lambda}$ tais que

$$p_{a=b|x,y} = \int_\Lambda q_\lambda \left[p_{0|x,\lambda}\, p_{0|y,\lambda} + p_{1|x,\lambda} p_{1|y,\lambda}\right] d\lambda, \tag{3.9a}$$

$$p_{a\neq b|x,y} = \int_\Lambda q_\lambda \left[p_{0|x,\lambda}\, p_{1|y,\lambda} + p_{1|x,\lambda} p_{0|y,\lambda}\right] d\lambda. \tag{3.9b}$$

Neste caso, a expressão (3.8) pode ser reescrita como

$$\begin{aligned}\beta_{CHSH} = 2 \int_\Lambda q_\lambda \left\{ \left[2p_{a=0|x=0,\lambda} - 1\right] \left[p_{b=0|y=0,\lambda} + p_{b=0|y=1,\lambda} - 1\right] + \right. \\ \left. + \left[2p_{a=0|x=1,\lambda} - 1\right] \left[p_{b=0|y=0,\lambda} - p_{b=0|y=1,\lambda}\right] \right\} d_\lambda,\end{aligned} \tag{3.10}$$

sendo que condições de normalização

$$\sum_{a\in R_x} \sum_{b\in R_y} p_{a,b|x,y} = 1 \tag{3.11}$$

foram utilizadas na simplificação do resultado. Para quaisquer probabilidades $p_{a=0|x=0,\lambda}$, $p_{a=0|x=1,\lambda}$, $p_{b=0|y=0,\lambda}$, $p_{b=0|y=1,\lambda}$, o termo entre chaves, na

expressão (3.10), pertence ao intervalo $[-1, 1]$. A média sobre estes valores necessariamente pertence ao mesmo intervalo. Assim,

$$|\beta_{CHSH}| \leq 2. \tag{3.12}$$

Devido a seus criadores John Clauser, Michael Horne, Abner Shimony e Richard Holt [13], esta importante desigualdade de Bell ficou conhecida como *desigualdade CHSH*.

3.5 O conjunto de correlações locais

As correlações $p_{a,b|x,y}$ que descrevem um cenário de Bell podem ser convenientemente representadas como componentes de um ponto $p \in \mathbb{R}^t$,

$$p = \begin{pmatrix} \vdots \\ p_{a,b|x,y} \\ \vdots \end{pmatrix}, \tag{3.13}$$

onde $t = \sum_{x=0}^{m_A-1} \sum_{y=0}^{m_B-1} v_x v_y$.

Não são todos os pontos de R^t que correspondem a correlações de um cenário de Bell. Como probabilidades, suas componentes devem satisfazer às condições de positividade,

$$p_{a,b|x,y} \geq 0, \quad \forall\ a, b, x, y; \tag{3.14}$$

e normalização,

$$\sum_{a=0}^{v_x-1} \sum_{b=0}^{v_y-1} p_{a,b|x,y} = 1, \quad \forall\ x, y. \tag{3.15}$$

Ainda, devem satisfazer à condição de não-sinalização,

$$\sum_{b=0}^{v_y-1} p_{a,b|x,y} = p_{a|x}, \quad \forall\ a, x, y; \tag{3.16a}$$

$$\sum_{a=0}^{v_x-1} p_{a,b|x,y} = p_{b|y}, \quad \forall\ b, x, y. \tag{3.16b}$$

O conjunto de todos os pontos $p \in \mathbb{R}^t$ que satisfazem às condições de positividade (3.14), normalização (3.15) e não-sinalização (3.16) será chamado *conjunto das correlações não-sinalizadoras* e denotado $\mathcal{P}$.

O *conjunto das correlações locais*, denotado $\mathcal{L}$, é o conjunto dos pontos $p \in \mathbb{R}^t$ que satisfazem às condições de positividade (3.14), normalização (3.15), e localidade, *i.e.*, existem q_λ, $p_{a|x,\lambda}$ e $p_{b|y,\lambda}$ tais que

$$p_{a,b|x,y} = \int_\Lambda q_\lambda \, p_{a|x,\lambda} \, p_{b|y,\lambda} \, d\lambda. \tag{3.17}$$

Seguem algumas propriedades de $\mathcal{L}$:

- Todas as correlações locais satisfazem à condição de não-sinalização,

$$\begin{aligned} \sum_{b=0}^{v_y-1} p_{a,b|x,y} &= \sum_{b=0}^{v_y-1} \int_\Lambda q_\lambda \, p_{a|x,\lambda} \, p_{b|y,\lambda} \, d\lambda \\ &= \int_\Lambda q_\lambda \, p_{a|x,\lambda} \left(\sum_{b=0}^{v_y-1} p_{b|y,\lambda} \right) d\lambda \\ &= p_{a|x}; \end{aligned} \tag{3.18a}$$

$$\begin{aligned} \sum_{a=0}^{v_x-1} p_{a,b|x,y} &= \sum_{a=0}^{v_x-1} \int_\Lambda q_\lambda \, p_{a|x,\lambda} \, p_{b|y,\lambda} \, d\lambda \\ &= \int_\Lambda q_\lambda \left(\sum_{a=0}^{v_x-1} p_{a|x,\lambda} \right) p_{b|y,\lambda} \, d\lambda \\ &= p_{b|y}. \end{aligned} \tag{3.18b}$$

  A recíproca, porém, não é verdadeira, pois existem pontos de $\mathcal{P}$ que não pertencem a $\mathcal{L}$. Assim, $\mathcal{L} \subset \mathcal{P}$.

- Por construção, o conjunto $\mathcal{L}$ é *convexo*[3]. Assim como todo conjunto convexo, $\mathcal{L}$ pode ser completamente caracterizado por sua fronteira.

- $\mathcal{L}$ tem um número finito de pontos extremais. Esta propriedade implica que o conjunto $\mathcal{L}$ é um *politopo convexo*[4], uma generalização dos polígonos e poliedros.

[3]Se $\mathcal{S}$ é um conjunto convexo, para todos $s_1, s_2, \ldots, s_r$ em $\mathcal{S}$ e números não negativos $q_1, q_2, \ldots, q_r$ tais que $\sum_k q_k = 1$, o vetor $\sum_k q_k s_k$ pertence a $\mathcal{S}$.

[4]Um politopo convexo pode ser definido como o *fecho convexo* de um número finito de pontos, ou seja, o menor conjunto convexo que contém os pontos em questão.

3.5.1 Correlações locais determinísticas

Sendo convexo o conjunto das correlações locais, existe um conjunto de pontos extremais $\mathcal{D}$ cujo fecho convexo é o conjunto $\mathcal{L}$, ou seja, $\mathcal{L}$ é o menor conjunto convexo que contém os pontos pertencentes a $\mathcal{D}$. Assim, qualquer correlação $p \in \mathcal{L}$ pode ser escrita como combinação convexa dos pontos de $\mathcal{D}$. O conjunto $\mathcal{D}$ é o conjunto de *pontos localmente determinísticos*, correlações locais cujas probabilidades marginais $p_{a|x,\lambda}$ e $p_{b|y,\lambda}$ são iguais a 0 ou 1, somente, para quaisquer medições e resultados. Os pontos do conjunto $\mathcal{D}$ representam as previsões de teorias realistas locais, em que todas as medições têm resultado localmente determinado.

Assim, vê-se que a hipótese de realismo local não é mais restritiva que a hipótese de causalidade local. Isso porque a aleatoriedade nas probabilidades marginais pode ser incorporada à aleatoriedade da variável λ. Considere, por exemplo, dois novos parâmetros $\mu_1, \mu_2 \in [0,1]$, e defina uma nova variável $\lambda' = \lambda'(\lambda, \mu_1, \mu_2)$. Novas probabilidades marginais de Alice e Bob podem ser definidas como

$$p'_{a|x,\lambda'} = \begin{cases} 1 & \text{se} \quad F_{a-1|x,\lambda} \leq \mu_1 < F_{a|x,\lambda} \\ 0 & \text{senão} \end{cases} \tag{3.19a}$$

$$p'_{b|y,\lambda'} = \begin{cases} 1 & \text{se} \quad F_{b-1|y,\lambda} \leq \mu_2 < F_{b|y,\lambda} \\ 0 & \text{senão} \end{cases} \tag{3.19b}$$

onde $F_{a|x,\lambda} = \sum_{a'<a} p_{a'|x,\lambda}$, $F_{b|y,\lambda} = \sum_{b'<b} p_{b'|y,\lambda}$, e $F_{-1|x,\lambda} = F_{-1|y,\lambda} \equiv 0$. Se $\tilde{q}$ é a distribuição uniforme no intervalo $[0,1]$, então

$$\begin{aligned} p_{a,b|x,y} &= \int_\Lambda q_\lambda \, p_{a|x,\lambda} \, p_{b|y,\lambda} \, d\lambda = \\ &= \int_\Lambda q_\lambda \left(\int \tilde{q} \, p'_{a|x,\lambda,\mu_1} d\mu_1 \right) \left(\int \tilde{q} \, p'_{b|y,\lambda,\mu_2} d\mu_2 \right) d\lambda = \\ &= \int q'_{\lambda'} \, p'_{a|x,\lambda'} \, p'_{b|y,\lambda'} \, d\lambda', \end{aligned} \tag{3.20}$$

onde $q'_{\lambda'}$ é a distribuição das novas variáveis λ'. Esta descoberta é devida a Arthur Fine [14]

Por definição, em um cenário de Bell são finitos os números de partes, medições por parte e possíveis resultados de cada medição. Então, também é finito o número de pontos locais determinísticos de um dado cenário. Cada um destes pontos á associado a um valor de λ, e, portanto, é suficiente que o conjunto Λ tenha um número finito de elementos. Como ilustração, defina $\chi \equiv (\chi_A; \chi_B) = (a_0, a_1, \ldots, a_{m_A-1}; b_0, b_1, \ldots, b_{m_B-1})$ como o conjunto dos resultados pré-determinados de cada uma das m_A possíveis medições de

Alice e m_B possíveis medições de Bob, e $\vec{d_\chi} \in \mathbb{R}^t$ o ponto local determinístico correspondente, cujas componentes são

$$d_{a,b|x,y,\chi} = \begin{cases} 1 & \text{se} \quad \chi_A(x) = a, \chi_B(y) = b, \\ 0 & \text{senão} \end{cases} \tag{3.21}$$

Repare que, neste caso, as variáveis λ podem ser definidas como os próprios conjuntos χ, $\lambda \equiv \chi$, caso em que as variáveis "ocultas" seriam os resultados das medições. O conjunto $\mathcal{D}$ pode ser definido como o conjunto de todos os pontos $d \in \mathcal{P}$ cujas componentes são da forma (3.21). Assim, um ponto $p \in \mathcal{P}$ pertence a $\mathcal{L}$ se, e somente se, existe uma distribuição de probabilidades q_λ tal que

$$p = \sum_\lambda q_\lambda d_\lambda. \tag{3.22}$$

3.5.2 Politopos convexos e desigualdades de Bell

Como observado, $\mathcal{L}$ é o fecho convexo de um número finito de pontos; $\mathcal{L}$ é, portanto, um politopo convexo. Existe um resultado básico em geometria convexa, conhecido como *teorema de Minkowski*, que diz que um politopo pode ser representado, de forma equivalente, como

- o fecho convexo de um número finito de pontos,

$$\mathcal{L} \equiv \left\{ p \in \mathbb{R}^t \,|\, p = \sum_\lambda q_\lambda d_\lambda, \quad q_\lambda \geq 0, \quad \sum_\lambda q_\lambda = 1 \right\}; \tag{3.23a}$$

- a interseção de um número finito de *semi-espaços*[5],

$$\mathcal{L} \equiv \left\{ p \in \mathbb{R}^t \,|\, b^i p \leq b_0^i, \, \forall\, i \in I \right\}, \tag{3.23b}$$

  onde $\{(b^i, b_0^i), i \in I\}$ denota um conjunto finito de desigualdades; satisfazê-las é condição necessária e suficiente para que uma correlação seja local.

Se (b, b_0) é uma desigualdade do politopo $\mathcal{L}$, então $F = \{p \in \mathcal{L} \,|\, bp = b_0\}$ é uma *face* de $\mathcal{L}$. Faces de dimensão 0 são chamadas *vértices*, e faces de dimensão $dim(L) - 1$ são chamadas *facetas*. Os vértices de um politopo são seus pontos extremais; no caso de $\mathcal{L}$, os vértices são os pontos determinísticos d_λ. As desigualdades associadas às facetas do politopo local são as *desigualdades de Bell*.

[5]Um semi-espaço é uma das duas partes em que um hiperplano divide um espaço afim, neste caso, $\mathbb{R}^t$. Ele pode ser representado por um desigualdade linear, derivada da equação linear que representa o hiperplano.

3.5.3 Representações e dimensões

Correlações locais satisfazem as condições de normalização (3.15) e não-sinalização (3.16). Os vínculos impostos às correlações por estas condições fazem com que a dimensão do politopo local seja menor que a do espaço em que está inserido, $\dim(\mathcal{L}) < t$.

Pode ser conveniente, por isso, representar $\mathcal{L}$ em um subespaço de $\mathbb{R}^t$ cuja dimensão seja a mesma de $\mathcal{L}$, ou seja, projetar p em $\mathbb{R}^{t'} \supset \mathbb{R}^t$, onde $t' = \dim(\mathcal{L})$. Esta projeção pode ser feita de várias formas. Uma delas é introduzindo-se as probabilidades marginais $p_{a|x}$ e $p_{b|y}$ e, então, descartando-se todas as quantidades relacionadas aos resultados $a = v_x - 1$ e $b = v_y - 1$. Em outros termos, passar de

$$p = \left(p_{a,b|x,y}\right) \quad \text{para} \quad p' = \begin{pmatrix} p_{a|x} \\ p_{b|y} \\ p_{a,b|x,y} \end{pmatrix}, \quad \begin{matrix} a \neq v_x - 1 \\ b \neq v_y - 1 \end{matrix}. \tag{3.24}$$

As duas representações são completamente equivalentes. A vantagem da segunda representação, contudo, é que todas componentes de p' são independentes.

Na segunda representação, as desigualdades de Bell podem ser escritas de maneira única. Tome como exemplo a desigualdade CHSH. Na primeira representação, o parâmetro de Bell pode ser escrito como

$$\begin{aligned}\beta_{CHSH} = p_{a=b|0,0} - p_{a\neq b|0,0} + p_{a=b|0,1} - p_{a\neq b|0,1} + \\ + p_{a=b|1,0} - p_{a\neq b|1,0} - p_{a=b|1,1} + p_{a\neq b|1,1},\end{aligned} \tag{3.25}$$

ou, usando-se a condição de normalização $p_{a=b|0,0} = 1 - p_{a\neq b|0,0}$, através da expressão equivalente

$$\begin{aligned}\beta_{CHSH} = 1 - 2p_{a\neq b|0,0} + p_{a=b|0,1} - p_{a\neq b|0,1} + \\ + p_{a=b|1,0} - p_{a\neq b|1,0} - p_{a=b|1,1} + p_{a\neq b|1,1}.\end{aligned} \tag{3.26}$$

Na representação 'linha', a mesma desigualdade pode ser reescrita na forma única

$$p_{a=0|x=0} + p_{b=0|y=0} - p_{0,0|0,0} - p_{0,0|0,1} - p_{0,0|1,0} + p_{0,0|1,1} \leq 0. \tag{3.27}$$

Esta forma da desigualdade CHSH ficou conhecida como *desigualdade CH* [15], devido a John Clause e Michael Horne.

3.5.4 Enumeração de facetas

A tarefa de se encontrar as facetas de um politopo, dados seus vértices, é um problema conhecido como *enumeração de facetas* ou *problema do fecho convexo*. Este problema, no contexto dos politopos locais, corresponde ao problema de se encontrar todas as desigualdades de Bell de um dado cenário.

Nos casos excepcionalmente simples, é possível obter todas as facetas de um politopo através de métodos e códigos computacionais, como PORTA [16] ou HOPDM [17]. No entanto, o tempo de computação cresce rapidamente ao se aumentar os números de partes, medições e resultados, e logo esta estratégia torna-se impraticável. Em [18], Itamar Pitowski analisa a complexidade de se enumerar facetas de politopos de correlações.

Em geral, nem mesmo o número total de desigualdades de Bell de cenários específicos é conhecido. Bárány e Pór [19] mostraram que, para os chamados *politopos 0-1* - politopos cujos vértices são iguais a 0 ou 1, como os politopos locais - , existe uma constante positiva c tal que

$$f > \left(\frac{cD}{\log(D)}\right)^{D/4}, \tag{3.28}$$

onde f é o número de facetas, e D a dimensão do politopo. Este resultado mostra que, em geral, o número de desigualdades de Bell pode crescer superexponecialmente com a dimensão do politopo.

3.5.5 Casos resolvidos

A seguir serão enumerados alguns politopos locais para os quais todas as facetas foram determinadas. Note que as condições de positividade (3.14) são facetas destes politopos; apenas facetas não triviais serão apresentadas. Outra importante observação é que, se uma desigualdade define uma faceta do politopo local, então o mesmo é verdade para todas as desigualdades dela obtidas por mudanças de rótulos das partes, medições e resultados. O que é, assim, escrito como uma desigualdade representa toda a *órbita* de desigualdades dela obtidas por tais operações.

- $(2, 2, 2)$: Este é o cenário mais simples, não trivial[6]; a única desigualdade de Bell é CHSH [14].
- $(2, 2; 2, \ldots, 2)$: Neste caso, assim como no anterior, a desigualdade CHSH é a única, independentemente do número de medições de Bob [20, 21].

[6]Os cenários $(2; 2)$ e $(2; 2, 2)$ são exemplos onde se é possível construir facilmente modelos locais para quaisquer correlações.

- $(v_{x=0}, v_{x=1}; v_{y=0}, v_{y=1})$: Diferentes casos, com v_x, v_y menores que 4, foram investigados computacionalmente em [21]. Em todos eles, as desigualdades CHSH e CGLMP, introduzidas abaixo, foram as únicas encontradas.

- $(2, 3, 2)$: Neste caso, assim como a desigualdade CHSH, a desigualdade

$$P_{a=0|x=0} + p_{b=0|y=0} - p_{0,0|0,0} - p_{0,0|0,1} - p_{0,0|0,2} - \\ - p_{0,0|1,0} - p_{0,0|2,0} - p_{0,0|1,1} + p_{0,0|1,2} + p_{0,0|2,1} \geq -1 \quad (3.29)$$

  define uma faceta do politopo local. Este resultado foi obtido em [22], e reobtido em [20, 21].

- $(2, 2, 2; 2, 2, 2)$: Neste cenário, além de CHSH e a desigualdade (3.29), trás novas desigualdades, apresentadas em [21], são facetas do politopo local.

- $(3, 2, 2)$: Todas as desigualdades foram enumeradas em [23], e agrupadas em 46 órbitas não-equivalentes em [20].

Os cenários $(2, 2, v)$ não foram completamente resolvidos, mas sabe-se que as *desigualdades CGLMP*,

$$\sum_{k}^{\lfloor v/2 \rfloor - 1} \left(1 - \frac{2k}{v-1}\right) (p_{a_0=b_0+k} + p_{b_0=a_1+k+1} + \\ + p_{a_1=b_1+k} + p_{b_1=a_0+k} - p_{a_0=a_0-k-1} - \\ - p_{b_0=a_1-k} - p_{a_1=b_1-k-1} - p_{b_1=a_0-k-1}) \leq 2, \quad (3.30)$$

definem facetas dos politopos locais [24]. O símbolo $\lfloor v/2 \rfloor$ denota a parte inteira de $v/2$, e $p_{a_x=b_y+k} = \sum_{b=0}^{v-1} p_{b\oplus k|x,y}$, onde $\oplus$ denota adição módulo v.

4

Correlações quânticas

> Anyone who is not shocked by quantum theory does not understand it.
>
> - Niels Bohr.

Em seu clássico artigo [11], de 1964, John Bell apresentou uma importante descoberta: existem correlações obtidas de medições em sistemas quânticos que violam as desigualdades de Bell. A grande conseqüência desse resultado, conhecido como teorema de Bell, é que nenhuma teoria realista local é capaz de reproduzir as previsões da mecânica quântica, ao contrário do que acreditavam EPR [9].

Neste capítulo, estudamos as correlações quânticas e suas intrincadas relações com o emaranhamento. Apresentamos também o chamado paradoxo de GHZ e citamos alguns dos mais importantes experimentos realizados no intuito de comprovar o teorema de Bell.

4.1 Correlações quânticas

4.1.1 Definição

Um caso especial de cenário de Bell é aquele em que os sistemas físicos compartilhados entre as partes são sistemas quânticos. Neste *cenário de Bell quântico*, as partes realizam POVMs em seus subsistemas, e, em geral, os resultados obtidos nas medições estarão correlacionados. Serão ditas *correlações quânticas* as correlações observadas em um cenário de Bell quântico.

Considere um cenário de Bell quântico bipartido - todas as definições se estendem trivialmente para cenários multipartidos. O conjunto $\mathcal{Q}$ das correlações quânticas é definido como o conjunto dos vetores $\vec{p}$ para os quais existem

- um estado quântico ρ em um espaço de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$,
- para cada medição x da parte A, um POVM $\left\{\mathbf{E}_{a|x}\right\}$, onde cada efeito $\mathbf{E}_{a|x}$ é associado a um resultado a,
- para cada medição y da parte B, um POVM $\left\{\mathbf{F}_{b|y}\right\}$, onde cada efeito $\mathbf{F}_{b|y}$ é associado a um resultado b,

de forma que suas componentes sejam

$$p_{a,b|x,y} = \mathrm{Tr}\left(\rho\left(\mathbf{E}_{a|x} \otimes \mathbf{F}_{b|y}\right)\right). \tag{4.1}$$

4.1.2 Propriedades

O conjunto das correlações quânticas possui as seguintes propriedades:

- $\mathcal{Q}$ respeita a condição de não-sinalização.

$$\begin{aligned} \sum_b p_{a,b|x,y} &= \sum_b \mathrm{Tr}\left(\rho\left(\mathbf{E}_{a|x} \otimes \mathbf{F}_{b|y}\right)\right) = \\ &= \mathrm{Tr}\left(\rho\left(\mathbf{E}_{a|x} \otimes \mathbf{1}\right)\right) \\ &\equiv p_{a|x}; \end{aligned} \tag{4.2a}$$

$$\begin{aligned} \sum_a p_{a,b|x,y} &= \sum_a \mathrm{Tr}\left(\rho\left(\mathbf{E}_{a|x} \otimes \mathbf{F}_{b|y}\right)\right) = \\ &= \mathrm{Tr}\left(\rho\left(\mathbf{1} \otimes \mathbf{F}_{b|y}\right)\right) \\ &\equiv p_{b|y}. \end{aligned} \tag{4.2b}$$

  Uma vez que todas as correlações quânticas satisfazem as condições de positividade e normalização, tem-se que $\mathcal{Q} \subseteq \mathcal{P}$.

- Qualquer correlação local pode ser obtida em um cenário de Bell quântico. Para todo $\vec{p} \in \mathcal{L}$, existem um operador densidade ρ e POVMs $\left\{E_{a|x}\right\}$ e $\left\{F_{b|y}\right\}$ tais que as probabilidades $p_{a,b|x,y}$ são dadas pela equação (4.1). Contudo, existem correlações quânticas que não admitem modelos locais. Assim, $\mathcal{L} \subset \mathcal{Q}$.

- $\mathcal{Q}$ é um conjunto convexo. Ao contrário de $\mathcal{L}$, porém, o conjunto das correlações quânticas não é um politopo [25].

4.2 O teorema de Bell

O teorema de Bell enuncia a existência de correlações quânticas que não podem ser reproduzidas por nenhuma teoria local. Em outras palavras, este teorema evidencia que a mecânica quântica é incompatível com a hipótese de causalidade local, e correlações não-locais podem ser obtidas em cenários de Bell quânticos.

Considere o cenário de Bell quântico $(2, 2, 2)$. Nele, uma correlação admite interpretação local se, e somente se, satisfaz a desigualdade CHSH e toda a sua órbita de desigualdades dela obtida por mudanças de rótulos. Suponha que as partes estão restritas à realização de medições projetivas, que, por conveniência, estão associadas a observáveis *unitários* - operadores com espectro $\{\pm 1\}$.

Sejam $\mathbf{A}_0$ e $\mathbf{A}_1$ os observáveis unitários correspondentes às medições de Alice e $\mathbf{B}_0$ e $\mathbf{B}_1$ os observáveis unitários correspondentes às medições de Bob. Uma pequena mudança de notação facilitará os cálculos seguintes: os resultados a e b serão identificados com os autovalores de $\mathbf{A}$ e $\mathbf{B}$; para isso, a definição $a, b \equiv \pm 1$ será necessária. O valor esperado de $\mathbf{A}_x \otimes \mathbf{B}_y$, no estado ρ, é

$$\begin{aligned} \langle \mathbf{A}_x \otimes \mathbf{B}_y \rangle_\rho &= \mathrm{Tr}\left(\rho \left(\mathbf{A}_x \otimes \mathbf{B}_y\right)\right) \\ &= \sum_{a=\pm 1} \sum_{b=\pm 1} a\, b\, p_{a,b|x,y} \\ &= p_{-1,-1|x,y} - p_{1,-1|x,y} - p_{-1,1|x,y} + p_{1,1|x,y}. \end{aligned} \tag{4.3}$$

Assim, o parâmetro de Bell da desigualdade CHSH pode ser escrito como

$$\begin{aligned} \beta_{CHSH} &= \langle \mathbf{A}_0 \otimes \mathbf{B}_0 \rangle + \langle \mathbf{A}_1 \otimes \mathbf{B}_0 \rangle + \langle \mathbf{A}_0 \otimes \mathbf{B}_1 \rangle - \langle \mathbf{A}_1 \otimes \mathbf{B}_1 \rangle \\ &= \langle \mathbf{A}_0 \otimes \mathbf{B}_0 + \mathbf{A}_1 \otimes \mathbf{B}_0 + \mathbf{A}_0 \otimes \mathbf{B}_1 - \mathbf{A}_1 \otimes \mathbf{B}_1 \rangle . \end{aligned} \tag{4.4}$$

Desta expressão pode ser definido o *observável de Bell* associado à desigualdade CHSH,

$$\mathcal{B}_{CHSH} \equiv \mathbf{A}_0 \otimes \mathbf{B}_0 + \mathbf{A}_1 \otimes \mathbf{B}_0 + \mathbf{A}_0 \otimes \mathbf{B}_1 - \mathbf{A}_1 \otimes \mathbf{B}_1, \tag{4.5}$$

de forma que o parâmetro de Bell, neste caso, pode ser escrito como o valor esperado deste operador, em um estado quântico.

Suponha que Alice e Bob compartilham um sistema quântico de dois qubits no estado singleto

$$\left|\psi^-\right\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{4.6}$$

A Alice, é permitida a realização de medições dos seguintes observáveis unitários

$$\mathbf{A}_0 = \sigma_1, \quad \mathbf{A}_1 = \sigma_3. \tag{4.7}$$

Por sua vez, os observáveis unitários cujas medições podem ser realizadas por Bob são

$$\mathbf{B}_0 = \frac{\sigma_1 + \sigma_3}{\sqrt{2}}, \quad \mathbf{B}_1 = \frac{\sigma_1 - \sigma_3}{\sqrt{2}}. \tag{4.8}$$

Tomando-se o valor esperado do observável de Bell, construído a partir destes quatro observáveis, no estado singleto, tem-se que

$$\beta_{CHSH} = \langle \mathcal{B}_{CHSH} \rangle_{|\psi^-\rangle} = -2\sqrt{2}. \tag{4.9}$$

As correlações obtidas neste cenário de Bell quântico violam claramente a desigualdade CHSH, e, portanto, são necessariamente não-locais.

4.3 Condições para correlações quânticas não-locais

Ambas as condições abaixo são necessárias para que correlações não-locais sejam obtidas em um cenário de Bell quântico:

1. Os observáveis associados às medições de cada uma das partes não podem comutar entre si. Segundo um teorema enunciado por Arthur Fine [14], as correlações que descrevem um cenário de Bell são locais se, e somente se, existe uma distribuição de probabilidades conjunta para os resultados de todas as possíveis medições realizadas por uma parte. Se os observáveis que descrevem estas medições comutam entre si, então existe uma distribuição com esta característica, e, conseqüentemente, qualquer correlação observada neste cenário é necessariamente local.

2. O estado do sistema quântico compartilhado entre as partes deve ser emaranhado. No artigo de Werner [8], estados separáveis são definidos como os estados quânticos para os quais as correlações deles obtidas são necessariamente locais.

4.3.1 Estados separáveis

Seja ρ o seguinte estado separável de um sistema quântico bipartido

$$\rho = \sum_r q_r \rho_r^A \otimes \rho_r^B. \tag{4.10}$$

Realizados POVMs arbitrários $\left\{E_{a|x}\right\}$ e $\left\{F_{b|y}\right\}$ nas partes A e B, respectivamente, a probabilidade conjunta de se obter os resultados a e b é

$$\begin{aligned} p_{a,b|x,y} &= \mathrm{Tr}\left(\left(\sum_r q_r\, \rho_r^A \otimes \rho_r^B\right)\left(\mathbf{E}_{a|x} \otimes \mathbf{F}_{b|y}\right)\right) \\ &= \sum_r q_r \mathrm{Tr}\left(\rho_r^A \mathbf{E}_{a|x}\right) \mathrm{Tr}\left(\rho_r^B \mathbf{F}_{b|y}\right) \\ &\equiv \sum_r q_r\, p_{a|x}\, p_{b|y}. \end{aligned} \tag{4.11}$$

Fica evidente, assim, que são necessariamente locais todas as correlações obtidas a partir de medições em estados separáveis.

4.3.2 Estados de Werner

Em [8], Werner fez a primeira distinção precisa entre emaranhamento e correlações não-locais. Historicamente, os termos "violação de uma desigualdade de Bell" e "correlações não-clássicas" tinham igual conotação. Neste trabalho, fica evidente que esta relação não é tão clara, pois são apresentadas correlações obtidas de estados emararanhados que admitem modelos locais.

Os estados de Werner são operadores densidade definidos em $\mathcal{H}^d \otimes \mathcal{H}^d$ que são invariantes sob operações unitárias da forma $\mathbf{U} \otimes \mathbf{U}$, *i.e.*, $(\mathbf{U} \otimes \mathbf{U})\, \rho \left(\mathbf{U}^\dagger \otimes \mathbf{U}^\dagger\right) = \rho$. Estes estados constituem uma família a um parâmetro, e podem ser escritos como

$$\rho_W(w) = (1-w)\,\frac{\mathbf{\Pi}_+}{r_+} + (w)\,\frac{\mathbf{\Pi}_-}{r_-}, \tag{4.12}$$

onde $0 \leq w \leq 1$, $\mathbf{\Pi}_+$ é o projetor no subespaço simétrico[1] de $\mathcal{H}^d \otimes \mathcal{H}^d$, $\mathbf{\Pi}_-$ é o projetor no subespaço anti-simétrico, e $r_\pm = \mathrm{Tr}\left(\mathbf{\Pi}_\pm\right) = \left(d^2 \pm d\right)/2$ são suas respectivas dimensões.

Um estado de Werner é separável se, e somente se, $\mathrm{Tr}\left(\mathbf{V}\, \rho_W\right) > 0$, onde $\mathbf{V}$ é o operador de troca. Como função do parâmetro w, esta grandeza é

$$\begin{aligned} \mathrm{Tr}\left(\mathbf{V}\, \rho_W(w)\right) &= \frac{1-w}{d^2+d} - \frac{w}{d^2-d} \\ &= \frac{2\left[d\,(1-2w)-1\right]}{d^3-d}. \end{aligned} \tag{4.13}$$

[1] Sejam $\{|\xi_i\rangle\}$ e $\{|\varphi_j\rangle\}$ bases de $\mathcal{H}_A$ e $\mathcal{H}_B$, respectivamente, ambos de mesma dimensão. Defina o *operador de troca* $\mathbf{V}$, definido em $\mathcal{H}_A \otimes \mathcal{H}_B$, através de sua operação nos elementos da base, $\mathbf{V}\,|\xi_i\rangle\,|\varphi_j\rangle = |\varphi_j\rangle\,|\xi_i\rangle$, e, por linearidade, extenda a definição a todo o espaço. O subespaço simétrico de $\mathcal{H}^d \otimes \mathcal{H}^d$ é formado pelos vetores $|\phi\rangle$ tais que $\mathbf{V}\,|\phi\rangle = |\phi\rangle$; o subespaço anti-simétrico é formado os vetores $|\phi\rangle$ tais que $\mathbf{V}\,|\phi\rangle = -\,|\phi\rangle$.

Assim, independementemente da dimensão d dos espaços de Hilbert, os estados de Werner são separáveis se, e somente se, $w < 1/2$.

Considere que medições projetivas idênticas são realizadas por ambas as partes; $\{\Pi_a\}$ é o conjunto de projetores da medição de Alice e $\{\Pi_b\}$ o conjunto de projetores da medição de Bob[2]. Uma descrição local da correlações obtidas exigiria a existência de uma distribuição q_λ em um espaço Λ, ao qual pertencem variáveis λ, e probabilidades marginais de todos os possíveis resultados tais que

$$\mathrm{Tr}\left(\rho\left(\mathbf{\Pi}_a \otimes \mathbf{\Pi}_b\right)\right) = \int_\Lambda q_\lambda \, p_{a|\lambda} \, p_{b|\lambda} \, d\lambda. \tag{4.14}$$

Se Λ é o conjunto $\left\{\lambda \in \mathbb{C}^d |\ |\lambda| = 1\right\}$ e

$$p_{a|\lambda} = \langle\lambda| \mathbf{\Pi}_a |\lambda\rangle\,, \tag{4.15a}$$

$$p_{b|\lambda} = \begin{cases} 1, & \text{se} \quad \langle\lambda| \mathbf{\Pi}_b |\lambda\rangle < \langle\lambda| \mathbf{\Pi}_{b'} |\lambda\rangle \ \ \forall\ b' \neq b \\ 0, & \text{senão} \end{cases}, \tag{4.15b}$$

pode-se mostrar que as correlações $p_{a,b}$ satisfazem (4.14) para

$$w = 1 - \frac{d+1}{2d^2}. \tag{4.16}$$

Em qualquer caso não-trivial, este valor é maior que $1/2$ e corresponde a um estado emaranhado.

Este resultado evidencia que estados emaranhados não geram, necessariamente, correlações não-locais, apesar de corresponder a um caso particular em que são realizadas medições projetivas idênticas. Modelos locais para correlações obtidas de estados de Werner emaranhados em POVMs foram construídos em [26], e generalizam o resultado acima apresentado.

4.3.3 Teorema de Gisin

O chamado *teorema de Gisin* [27] enuncia que todo estado puro emaranhado de sistemas quânticos bipartidos pode gerar correlações que violam a desigualdade CHSH. Este resultado sugere que as relações entre emaranhamento e não-localidade podem ser estreitas pelo menos para estados puros; no entanto, extensões para outros cenários não são conhecidas.

[2] Os elementos dos conjuntos $\{\Pi_a\}$ e $\{\Pi_a\}$ são iguais; os índices a e b são adicionados para se distinguir as partes.

Seja $|\psi\rangle$ um estado puro emaranhado de um sistema quântico bipartido, *i.e.*, $|\psi\rangle \neq |\xi\rangle \otimes |\varphi\rangle$. Pela decomposição de Schmidt, ele pode ser escrito como

$$|\psi\rangle = \sum_{i=1} c_i \, |\xi_i\rangle \otimes |\varphi_i\rangle, \tag{4.17}$$

onde todos os coeficientes c_i são reais. Como $|\psi\rangle$ é emaranhado, pelo menos $c_1, c_2 \neq 0$. Defina

$$\left|\psi_{/}\right\rangle = c_1 \, |\xi_1\rangle \otimes |\varphi_1\rangle + c_2 \, |\xi_2\rangle \otimes |\varphi_2\rangle \tag{4.18}$$

e

$$|\psi_{\perp}\rangle = \sum_{i>2} c_i \, |\xi_i\rangle \otimes |\varphi_i\rangle. \tag{4.19}$$

Assim, $|\psi\rangle = \left|\psi_{/}\right\rangle + |\psi_{\perp}\rangle$.

O estado $\left|\psi_{/}\right\rangle$ é, essencialmente, um estado de dois qubits. Por conveniência de notação, uma operação $\mathbf{U}_A \otimes \mathbf{U}_B$, onde $\mathbf{U}_A$ e $\mathbf{U}_B$ são operadores unitários, será aplicada em $\left|\psi_{/}\right\rangle$ de forma que

$$\left|\psi_{/}\right\rangle = c_1 \, |01\rangle + c_2 \, |10\rangle \, . \tag{4.20}$$

Esta operação corresponde a mudanças locais de referencial e não alteram as propriedades do estado quântico.

Sejam $\mathbf{A}_x$ e $\mathbf{B}_y$ observáveis unitários definidos em $\mathcal{H}^2$, que podem ser escritos como

$$\mathbf{A}_x = \vec{a}_x.\vec{\sigma}, \quad \mathbf{B}_y = \vec{b}_y.\vec{\sigma}, \tag{4.21}$$

onde $\vec{a}_x, \vec{b}_y \in \mathbb{R}^3$, tais que $|\vec{a}_x| = \left|\vec{b}_y\right| = 1$. Se

$$\begin{aligned} \vec{a}_x &= \left(\text{sen}\left(\alpha_x\right), 0, \cos\left(\alpha_x\right)\right), \\ \vec{b}_y &= \left(\text{sen}\left(\gamma_y\right), 0, \cos\left(\gamma_y\right)\right); \end{aligned} \tag{4.22a}$$

onde, ainda, $\alpha_0 = 0$, e $\alpha_1 = \pm\pi/2$ - o sinal sendo o oposto do sinal de $c_1 c_2$ - , o parâmetro de Bell da desigualdade CHSH é

$$\beta_{CHSH} = \cos\left(\gamma_0\right) - \cos\left(\gamma_1\right) + 2\left|c_1 c_2\right| \left(\text{sen}\left(\gamma_0\right) + \text{sen}\left(\gamma_1\right)\right). \tag{4.23}$$

Este valor é máximo para $\cos\left(\gamma_0\right) = -\cos\left(\gamma_1\right) = \left(1 + 4\left|c_1 c_2\right|^2\right)^{-\frac{1}{2}}$, onde $\text{sen}\left(\gamma_0\right) > 0$, $\text{sen}\left(\gamma_1\right) > 0$, e, para este valor, tem-se

$$\beta_{CHSH} = 2\sqrt{1 + 4\left|c_1 c_2\right|^2}. \tag{4.24}$$

Este valor é estritamente maior que 2 para quaisquer c_1 e c_2 diferentes de zero, ou seja, para todo $|\psi\rangle$ emaranhado.

4.4 Máxima violação de CHSH para 2 qubits

Dado um estado quântico de dois qubits, é possível determinar, de forma analítica, qual a máxima violação da desigualdade CHSH que correlações dele obtidas em medições projetivas são capazes de atingir. Este é um importante resultado da família Horodecki [28], que permite, ainda, encontrar as medições projetivas ótimas que podem ser realizadas pelas partes, dado o estado de dois qubits no qual elas farão as medições.

Qualquer estado quântico definido em $\mathcal{H}^2 \otimes \mathcal{H}^2$ pode ser escrito como

$$\rho = \frac{1}{4}\left(\mathbf{1}\otimes\mathbf{1} + \vec{r}.\vec{\sigma}\otimes\mathbf{1} + \mathbf{1}\otimes\vec{s}.\vec{\sigma} + \sum_{m,n=1}^{3} t_{mn}\sigma_m\otimes\sigma_n\right), \tag{4.25}$$

onde $\vec{r},\vec{s}\in\mathbb{R}^3$, tais que $|\vec{r}|\leq 1$, $|\vec{s}|\leq 1$, e $t_{mn} = \mathrm{Tr}\left(\rho\left(\sigma_m\otimes\sigma_n\right)\right)$; é conveniente definir uma matriz 3×3 $\mathcal{T}_\rho$, tal que t_{mn} são seus elementos. Sejam $\mathbf{A}_x = \vec{a}_x.\vec{\sigma}$ e $\mathbf{B}_y = \vec{b}_y.\vec{\sigma}$ os observáveis unitários de medição de Alice e Bob, respectivamente. O valor esperado do operador de Bell da desigualdade CHSH, avaliado em um estado ρ, escrito na forma (4.25), é

$$\langle\mathcal{B}_{CHSH}\rangle_\rho = \vec{a}_0.\left(T_\rho\left(\vec{b}_0+\vec{b}_1\right)\right) + \vec{a_1}.\left(T_\rho\left(\vec{b}_0-\vec{b}_1\right)\right). \tag{4.26}$$

Os vetores $\vec{b}_0$ e $\vec{b}_1$ podem ser decompostos em uma base ortonormal $\{\vec{c}_0,\vec{c}_1\}$,

$$\vec{b}_0+\vec{b}_1 = 2\cos(\theta)\,\vec{c}_0, \quad \vec{b}_0-\vec{b}_1 = 2\mathrm{sen}(\theta)\,\vec{c}_1, \tag{4.27}$$

onde $\theta\in[0,\pi/2]$. É avaliada, então, a maximização de $\langle\mathcal{B}_{CHSH}\rangle$ com respeito a θ e aos vetores $\vec{a}_0,\vec{a}_1,\vec{c}_0,\vec{c}_1$:

$$\begin{aligned}
\max\langle\mathcal{B}_{CHSH}\rangle_\rho &= \max_{(\theta,\vec{a}_0,\vec{a}_1,\vec{c}_0,\vec{c}_1)} 2\left[\vec{a}_0.\left(T_\rho\vec{c}_0\right)\cos(\theta) + \vec{a}_1.\left(T_\rho\vec{c}_1\right)\mathrm{sen}(\theta)\right] \\
&= \max_{(\theta,\vec{c}_0,\vec{c}_1)} 2\left[\left|T_\rho\vec{c}_0\right|\cos(\theta) + \left|T_\rho\vec{c}_1\right|\mathrm{sen}(\theta)\right] \\
&= \max_{(\vec{c}_0,\vec{c}_1)} 2\sqrt{\left|T_\rho\vec{c}_0\right|^2 + \left|T_\rho\vec{c}_1\right|^2}.
\end{aligned} \tag{4.28}$$

Sejam a matriz $U = \mathcal{T}_\rho^T\mathcal{T}_\rho$, diagonalizável, e u_0 e u_1 seus dois maiores autovalores. A avaliação do último máximo resulta em

$$\max\langle\mathcal{B}_{CHSH}\rangle_\rho = 2\sqrt{u_0+u_1}. \tag{4.29}$$

Estados puros, escritos em sua forma de Schmidt $|\psi\rangle = \cos(\varphi)\,|00\rangle + \mathrm{sen}(\varphi)\,|11\rangle$ têm, através do resultado acima, máxima violação

$$\max\langle\mathcal{B}_{CHSH}\rangle_{|\psi\rangle} = 2\sqrt{1+\sin^2(2\varphi)}. \tag{4.30}$$

4.5 O paradoxo de GHZ

Considere um cenário de Bell $(3, 2, 2)$. Três partes dividem um sistema quântico de três qubits no estado

$$|\psi_{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}, \tag{4.31}$$

e podem realizar, cada uma, duas diferentes medições projetivas em seu subsistema. As possíveis medições de Alice, Bob e Charlie são exatamente iguais, dadas por $\left\{\left|\psi_{0|0}\right\rangle\left\langle\psi_{0|0}\right|, \left|\psi_{1|0}\right\rangle\left\langle\psi_{1|0}\right|\right\}$ e $\left\{\left|\psi_{0|1}\right\rangle\left\langle\psi_{0|1}\right|, \left|\psi_{1|1}\right\rangle\left\langle\psi_{1|1}\right|\right\}$, onde

$$\begin{aligned} \left|\psi_{0|0}\right\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \left|\psi_{1|0}\right\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \\ \left|\psi_{0|1}\right\rangle &= \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}, \quad \left|\psi_{1|1}\right\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}. \end{aligned} \tag{4.32}$$

Algumas distribuições específicas são de especial interesse. Elas são as probabilidades conjuntas relacionadas às medições $xyz = 000$,

$$p_{a,b,c|0,0,0} = \begin{cases} 1/4, & \text{se} \quad a \oplus b \oplus c = 1 \\ 0, & \text{senão} \end{cases}, \tag{4.33}$$

e às medições $xyz \in \{011, 101, 110\}$, que podem ser escritas de forma compacta como

$$p_{a,b,c|x,y,z} = \begin{cases} 1/4, & \text{se} \quad a \oplus b \oplus c = 0 \\ 0, & \text{senão} \end{cases}, \tag{4.34}$$

onde $\oplus$ denota adição módulo 2.

Sejam $a_x, b_y, c_z \in \{0, 1\}$ os resultados obtidos quando as medições x, y, z são realizadas. Então, para cada uma das quatro configurações de medição consideradas acima, com probabilidade 1 os resultados obtidos satisfazem

$$\begin{aligned} a_0 \oplus b_0 \oplus c_0 &= 1, \\ a_0 \oplus b_1 \oplus c_1 &= 0, \\ a_1 \oplus b_0 \oplus c_1 &= 0, \\ a_1 \oplus b_1 \oplus c_0 &= 0. \end{aligned} \tag{4.35}$$

Nenhum modelo local é capaz de reproduzir as correlações quânticas (4.33) e (4.34). A prova é a seguinte *reductio ad absurdum*. Suponha que as correlações (4.33) e (4.34) sejam locais, combinações convexas de pontos locais determinísticos d_λ que designam resultados $\chi_A(x) = a_x, \chi_B(y) =$

$b_y, \chi_C(z) = c_z$ para as várias medições x, y e z. Como as relações (4.35) são satisfeitas com probabilidade 1, existe pelo menos um ponto d_λ tal que os resultados $\chi_A(x)$, $\chi_B(y)$ e $\chi_C(z)$ por ele designados satisfazem estas relações. Porém, cada a_x, b_y e c_z aparece em duas das quatro relações, e qualquer resultado localmente designado em uma equação deve ser exatamente igual ao resultado correspondente na equação seguinte. Assim, a soma das quatro equações resulta em $0 = 1$, uma contradição.

Este é o chamado *paradoxo de GHZ*, uma prova do teorema de Bell sem o uso de desigualdades, que deve seu nome a Daniel Greenberger, Michael Horne e Anton Zeilinger [29, 30]. Em certo sentido, este resultado é mais forte que qualquer violação de desigualdades, pois basta uma realização apenas de cada medição para evidenciar as correlações não-locais da mecânica quântica.

A este paradoxo é possível associar uma desigualdade de Bell, conhecida como *desigualdade de Mermin* [31],

$$p_{a\oplus b\oplus c=1|0,0,0} + p_{a\oplus b\oplus c=0|0,1,1} + p_{a\oplus b\oplus c=0|1,0,1} + p_{a\oplus b\oplus c=0|a\oplus b\oplus c=0} \leq 3, \quad (4.36)$$

onde $p_{a\oplus b\oplus c=k|x,y,z} = \sum_{a,b,c} \delta_{a\oplus b\oplus c,k} p_{a,b,c|x,y,z}$. As correlações apresentadas, obtidas dos *estados GHZ* (4.31), violam maximamente esta desigualdade até seu limite algébrico. A cota local é facilmente obtida se observado que qualquer modelo local é capaz de satisfazer, no máximo, três das quatro relações acima.

4.6 Emaranhamento

Emaranhamento, muitas vezes definido como "correlações não-clássicas", tem íntimas e intrincadas relações com a noção de não-localidade, ou correlações não-locais, como pode ser observado na seção 4.3. Com o advento da teoria quântica da informação, o emaranhamento foi identificado como um importante recurso, responsável por tarefas como teleportação de estados [32] e distribuição quântica de chaves criptográficas [33]. Neste sentido, é importante caracterizar e quantificar este recurso de forma eficiente, embora não seja, ainda, completamente claro o papel do emaranhamento na computação quântica. Nesta seção, alguns critérios de caracterização e quantificação de emaranhamento serão brevemente apresentados; as referências [5, 34, 35] são indicadas para aqueles que desejam se aprofundar neste tema.

4.6.1 Caracterização

Um estado emaranhado é um estado quântico de um sistema composto que não pode ser decomposto na forma [8]

$$\rho = \sum_{r=1} q_r \rho_r^A \otimes \rho_r^B, \quad q_r \geq 0, \quad \sum_{r=1}^{n} q_r = 1. \tag{4.37}$$

Esta definição, porém, é pouco útil quando se deseja saber se um dado estado tem ou não emaranhamento.

Sejam ρ o operador densidade de um sistema quântico e $\{|\xi_i\rangle\}$ uma base ortonormal de $\mathcal{H}$, o espaço de Hilbert associado ao sistema. Nesta base, ρ pode ser escrito como

$$\rho = \sum_{i,j} \rho_{i,j} \left|\xi_i\right\rangle \left\langle\xi_j\right| . \tag{4.38}$$

A *transposta* de ρ, denotada ρ^T, é definida, com respeito à base escolhida, como

$$\rho^T = \sum_{i,j} \rho_{i,j} \left|\xi_j\right\rangle \left\langle\xi_i\right| . \tag{4.39}$$

A *transposição* de um operador densidade preserva as três propriedades que o definem: hermiticidade, positividade e normalização. Por isso, uma importante observação é que a transposta de um operador densidade é, também, um operador densidade.

Em um sistema composto, a operação de transposição pode ser realizada em um subsistema apenas. As matrizes resultantes são chamadas *transpostas parciais*, e são denotadas ρ^{T_A} caso a transposição seja feita no subsistema A e ρ^{T_B} caso seja feita em B. São assim definidas: sejam $\{|\xi_i\rangle\}$ e $\{|\varphi_\mu\rangle\}$ bases de $\mathcal{H}_A$ e $\mathcal{H}_B$, respectivamente, e ρ o estado de um sistema cujo espaço de Hilbert é $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ que, nas bases acima definidas, é escrito como

$$\rho = \sum_{i,\mu,j,\nu} \rho_{i,\mu,j,\nu} \left(\left|\xi_i\right\rangle \left\langle\xi_j\right| \otimes \left|\varphi_\mu\right\rangle \left\langle\varphi_\nu\right|\right). \tag{4.40}$$

As transpostas parciais deste estado, definidas com respeito às bases apresentadas, são

$$\rho^{T_A} = \sum_{i,\mu,j,\nu} \rho_{i,\mu,j,\nu} \left(\left|\xi_j\right\rangle \left\langle\xi_i\right| \otimes \left|\varphi_\mu\right\rangle \left\langle\varphi_\nu\right|\right); \tag{4.41a}$$

$$\rho^{T_B} = \sum_{i,\mu,j,\nu} \rho_{i,\mu,j,\nu} \left(\left|\xi_i\right\rangle \left\langle\xi_j\right| \otimes \left|\varphi_\nu\right\rangle \left\langle\varphi_\mu\right|\right). \tag{4.41b}$$

Assim como a operação de transposição, a *transposição parcial* preserva as propriedades de hermiticidade e normalização de um operador densidade;

a positividade do operador, porém, não é necessariamente preservada. Considere, *e.g.*, um estado separável ρ. Suas transpostas parciais são

$$\rho^{T_A} = \sum_r q_r \left(\left(\rho_r^A\right)^T \otimes \rho_r^B \right); \tag{4.42a}$$

$$\rho^{T_B} = \sum_r q_r \left(\rho_r^A \otimes \left(\rho_r^B\right)^T \right). \tag{4.42b}$$

A transposição total dos operadores ρ_r^A e ρ_r^B resulta em novos operadores hermitianos, normalizados e positivos, possíveis operadores densidade relacionados às partes do sistema quântico composto. Por isso, as transpostas parciais de estados separáveis são necessariamente positivas.

Esta é a essência do chamado *critério de Peres* [36]: uma vez que as transpostas parciais de todos os estados separáveis são necessariamente positivas, é suficiente que uma transposta parcial do estado ρ seja não-positiva para que ρ seja emaranhado.

Em sistemas bipartidos cujo espaço de Hilbert tenha dimensão inferior a 6, apenas os estados separáveis têm transpostas parciais positivas [37]. Este resultado permite que, para tais sistemas, seja possível enunciar uma versão mais forte do critério de Peres, que ficou conhecida como *critério de Peres-Horodecki*: para que estados quânticos de sistemas cujos espaços de Hilbert são $\mathcal{H}_A^2 \otimes \mathcal{H}_B^2$ e $\mathcal{H}_A^2 \otimes \mathcal{H}_B^3$ sejam emaranhados, é necessário e suficiente que suas transpostas parciais sejam não-positivas.

A validade do critério de Peres-Horodecki é limitada, essencialmente, porque sistemas compostos cujos espaços de Hilbert tenham dimensões maiores que 6 admitem estados emaranhados cujas transpostas parciais são positivas. Estes estados são conhecidos como *estados emaranhados PPT*[3] [38].

As *testemunhas de emaranhamento* [37] constituem mais um importante critério de separabilidade. Uma conclusão do teorema de Hahn-Banach, de análise convexa em dimensão finita, garante que, dados um conjunto convexo fechado e um ponto fora dele, existe um funcional W que os separa. O conjunto dos estados separáveis de um sistema quântico é convexo e fechado; segundo este teorema, para todo estado emaranhado existe um funcional que o separa de todos os estados separáveis. Este funcional é um operador hermitiano $\mathbf{W}$, que, geometricamente, determina o hiperplano no espaço de estados definido como o conjunto de operadores densidade ρ que satisfazem

$$\mathrm{Tr}\left(\rho\mathbf{W}\right) = 0. \tag{4.43}$$

[3] Do inglês *positive partial transpose*.

Dado um estado emaranhado ρ_{Ent}, existe $\mathbf{W}$ tal que $\mathrm{Tr}\left(\mathbf{W}\rho_S\right) \geq 0$ para todo estado separável $\rho_S \in \mathcal{S}$ e $\mathrm{Tr}\left(\mathbf{W}\rho_{Ent}\right) < 0$. Este critério inspirou uma segunda definição de emaranhamento [37]: um estado ρ é emaranhado se, e somente se, existe um operador hermitiano $\mathbf{W}$ tal que $\mathrm{Tr}\left(\mathbf{W}\rho\right) < 0$, sendo que $\mathrm{Tr}\left(\mathbf{W}\rho_S\right) \geq 0$ para todo estado separável ρ_S.

A violação de uma desigualdade de Bell, em um cenário de Bell quântico, pode ser traduzida como uma testemunha de emaranhamento [39]. Suponha que $\left\{\mathbf{E}_{a|x}\right\}$ e $\left\{\mathbf{F}_{b|y}\right\}$ POVMs que, realizados nas partes de um sistema cujo estado é ρ, emaranhado, produzem correlações não-locais p, cujas componentes são

$$p_{a,b|x,y} = \mathrm{Tr}\left(\rho\left(\mathbf{E}_{a|x} \otimes \mathbf{F}_{b|y}\right)\right). \tag{4.44}$$

Então, neste cenário, existe uma desigualdade de Bell representada por $(b, 0)$ tal que

$$b.p = \sum_{a,b,x,y} b_{a,b|x,y}\, p_{a,b|x,y} \leq 0. \tag{4.45}$$

Considere o seguinte operador, construído a partir dos POVMs acima definidos:

$$\mathbf{W} = -\sum_{a,b,x,y} b_{a,b|x,y}\mathbf{E}_{a|x} \otimes \mathbf{F}_{b|y}. \tag{4.46}$$

Este operador é hermitiano, pois os efeitos são operadores hermitianos e o espaço destes operadores é fechado sob combinações lineares reais. O valor médio deste operador tomado em qualquer estado separável é maior ou igual a zero, uma vez que as correlações obtidas de sua medição são locais e satisfazem (4.45). No entanto, para o estado ρ, o valor médio deste operador é negativo, o que mostra que $\mathbf{W}$ é uma testemunha de emaranhamento.

Em geral, as testemunhas de emaranhamento obtidas de desigualdades de Bell não são ótimas[40], no sentido de que, dado um estado quântico emaranhado, pode existir uma testemunha de emaranhamento que é não é obtida de uma desigualdade de Bell que tenha um valor médio negativo maior, em módulo, do que os de quaisquer testemunhas obtidas de desigualdades de Bell, em relação ao estado dado. Por outro lado, as desigualdades de Bell são as únicas ferramentas conhecidas que evidenciam o emaranhamento presente em um estado que não dependem de pressuposições quanto à dimensão do espaço de Hilbert do sistema quântico [41].

4.6.2 Quantificação

O emaranhamento presente em um estado quântico pode ser quantificado através de funções conhecidas como *monótonos de emaranhamento* [42, 43]. Um monótono de emaranhamento é uma função $E\left(\rho\right)$ que não cresce, em

média, sob *operações locais e comunicação clássica* (LOCC). Esta classe de operações representa todas as possíveis intervenções que podem ser realizadas pelas partes em seus subsistemas apenas, permitindo, ainda, que se comuniquem classicamente durante as intervenções. Exemplos de LOCC são:

- Operações unitárias locais correlacionadas

$$\rho \mapsto \sum_i \mathbf{U}_i \rho \mathbf{U}_i^\dagger, \tag{4.47}$$

  onde $\mathbf{U}_i = \mathbf{U}_i^A \otimes \mathbf{U}_i^B$.

- Adição de um sistema auxiliar,

$$\rho \mapsto \rho \otimes \sigma, \tag{4.48}$$

  onde σ é o estado do sistema adicional.

- Descarte de uma parte do sistema,

$$\rho \mapsto \mathrm{Tr}_A(\rho). \tag{4.49}$$

LOCC não podem aumentar, em média, o emaranhamento de um estado quântico, mas podem ser utilizadas para diluir o emaranhamento presente em um estado quântico em cópias de um segundo estado, menos emaranhado. Da mesma forma, essa classe de operações pode ser utilizada para concentrar o emaranhamento de várias cópias de um estado em um número menor de cópias de um segundo estado mais emaranhado. Um primeiro quantificador é o *custo de emaranhamento* [44], relacionado ao primeiro processo. Se existe um protocolo de LOCC, $\mathcal{M}_{LOCC}$, capaz de transformar m cópias de *pares EPR*[4] em n cópias de um estado ρ, no limite $n \to \infty$, pode-se dizer que a razão $\frac{m}{n}$ quantifica - ou, pelo menos, estipula um teto para - o investimento do recurso emaranhamento necessário nesta preparação das cópias de ρ. O custo de emaranhamento E_C é definido como o ínfimo dessa razão sobre todos os possíveis protocolos LOCC,

$$E_C(\rho) = \inf_{\mathcal{M}_{LOCC}} \lim_{n\to\infty} \frac{m}{n}. \tag{4.50}$$

O *emaranhamento destilável*, denotado E_D, toma o caminho oposto: é um quantificador de emaranhamento relacionado ao número m de estados

[4]Um par EPR é um estado de dois qubits da forma $|\psi_{EPR}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

maximanente emaranhados que podem ser criados, através de LOCC apenas, a partir de n de cópias de um estado quântico. Ele é definido como

$$E_D = \sup_{\mathcal{M}_{LOCC}} \lim_{m\to\infty} \frac{n}{m}. \tag{4.51}$$

Há estados emaranhados para os quais não existe nenhum protocolo LOCC capaz de destilar seu emaranhamento. Sabe-se que este é o caso de todos os estados que apresentam transpostas parciais positivas, ou seja, estados emaranhados PPT [38]. Em geral, diz-se que apresentam *emaranhamento preso*[5] os estados emaranhados que não podem ter seu emaranhamento destilado. Não se sabe se existem estados que apresentam emaranhamento preso que não sejam estados emaranhados PPT.

4.6.3 Relações com não-localidade

Existem estados quânticos emaranhados que, em alguns cenários, sempre exibem correlações locais para quaisquer possíveis escolhas de medições como, *e.g.*, os estados de Werner [8]. Alguns desses estados, no entanto, podem apresentar correlações não-locais após a realização de LOCC apropriadas, exibindo, assim, um tipo de "não-localidade oculta", como evidenciado por Popescu em [51]. Por um lado, esse resultado evidenciou que a máxima violação de uma desigualdade de Bell não é um monótono de emaranhamento, e portanto, não deve ser utilizado como um quantificador deste recurso. Isso corrobora com o resultado obtido em [24], onde observa-se que as desigualdades CGLMP, apresentadas no capítulo 3, seção 3.5, são maximamente violadas por estados não-maximamente emaranhados[6]. Por outro lado, a observação de Popescu levantou a hipótese de que a não-localidade de um estado quântico deveria ser avaliada após sua preparação e manipulação através de LOCC, o que, possivelmente, evidenciaria que todos os estados emaranhados apresentam não-localidade.

No entanto, em 2006 [52], Lluis Masanes provou que, no cenário $(2, 2, 2)$, a violação da desigualdade CHSH após pós-processamento, no regime assintótico de infinitas cópias, somente é possível se o estado inicial pode ser destilado. Assim, os estados emaranhados PPT, que não podem ter seu emaranhamento destilado, não apresentam correlações não-locais neste cenário nem mesmo após manipulações locais.

[5] Do inglês *bound entanglement*.

[6] Em sistemas bipartidos, estados maximamente emaranhados são estados tais que todos os coeficientes de Schmidt são iguais a $\frac{1}{\sqrt{d}}$, onde d é a dimensão do espaço de Hilbert do sistema de menor dimensão.

4.7 Testes experimentais de não-localidade

Desde meados dos anos 70, várias demonstrações experimentais da não-localidade quântica foram realizadas. Na vasta maioria destes experimentos, os resultados observados concordavam, em grande precisão, com as previsões da mecânica quântica. Apesar disso, não é possível, em nenhum deles, afirmar que as correlações observadas são de fato não-locais. Isso porque existem "falhas" nas configurações experimentais, conhecidas como *loopholes*, que abrem espaço para que correlações aparentemente não-locais sejam explicadas dentro da hipótese de causalidade local.

Dois são os *loopholes* mais importantes: o *loophole de localidade* e o *loophole de detecção*. O *loophole* de localidade está relacionado à condição de que os eventos de medição em um cenário de Bell devem, necessariamente, ter separação espacial. Se esta condição não é satisfeita, é possível que as partes troquem informações durante os eventos de medição, o que seria suficiente para que fortes correlações entre os resultados fossem observadas, que poderiam, inclusive, violar uma desigualdade de Bell. Observe que, segundo a definição apresentada no capítulo 3, seção 3.2, um evento de medição tem início com a escolha da medição a ser realizada. Para que os eventos de medição sejam espacialmente separados, as escolhas de medição devem ser aleatórias e independentes; caso contrário, se o mecanismo responsável por tais escolhas tem funcionamento determinístico ou correlacionado a alguma outra variável, é possível, a princípio, que informações sobre a medição a ser escolhida estejam indiretamente disponíveis às outras partes.

O *loophole de detecção*, por sua vez, é particularmente importante nos experimentos que utilizam contagens de fótons. Sistemas ópticos são fontes bem conhecidas e controladas de estados emaranhados. Por isso, a vasta maioria dos experimentos de não-localidade realizados estão sujeitos a este *loophole*. Ele se baseia na premissa de que a baixa eficiência dos detectores resulta do fato de que as detecções são governadas pelas variáveis λ. Os fótons detectados seriam uma amostragem desonesta do *ensemble* de fótons produzidos, exatamente aqueles para os quais os resultados, pré-determinados por λ, exibiriam, nas medições escolhidas, correlações aparentemente não-locais. Se todos os fótons produzidos fossem detectados, somente correlações locais seriam observadas. Por outro lado, caso os detectores tenham boa eficiência, este argumento não pode ser invocado.

O primeiro teste experimental de não-localidade foi realizado por Freedman e Clauser, em 1972 [45]. Pares de fótons emaranhados em polarização eram criados a partir de transições eletrônicas em átomos de cálcio e enviados à medição. Com os dados obtidos, foi observada a violação da desigualdade CHSH. No entanto, como os aparatos de medição eram estáticos

e os detectores pouco eficientes, este experimento estava aberto a ambos os *loopholes*.

Dez anos depois, Aspect, Dalibard e Roger [46] realizaram o primeiro experimento em que a escolha das medições variavam no tempo, na tentativa de se fechar o *loophole* de localidade. Mecanismos opto-acústicos simulavam escolhas aleatórias das medições locais, realizadas na polarização de fótons criados em fontes de átomos de cálcio similares às utilizadas por Freedman e Clauser [45]. Porém, o mecanismo apresentava caráter quase-periódico, o que não permitiu fechar o *loophole* de localidade por completo.

A partir de 1988, as fontes de átomos de cálcio passaram a ser substituídas por cristais não-lineares que, através do processo de conversão paramétrica descendente, são capazes de criar fótons emaranhados de forma mais eficaz. Os primeiros experimentos de não-localidade com estas fontes foram realizados por Ou e Mandel [47], e, independentemente, por Alley e Shih [48], ambos abertos aos *loopholes* de localidade e detecção.

Considera-se que o *loophole* de localidade tenha sido fechado em 1998, em um experimento realizado por Weihs e colaboradores [49]. Nele, mecanismos aleatórios e independentes foram utilizados para a escolha das medições.

O *loophole* de detecção não é problema em experimentos realizados em íons armadilhados, nos quais a eficiência de detecção é próxima de 100%. Considera-se que o experimento realizado por Rowe e colaboradores [50], em 2001, tenha fechado este *loophole*. Como os íons têm separação espacial de micrômetros, o *loophole* de localidade permanece.

5

Correlações não-sinalizadoras

> Quantum phenomena do not occur in a Hilbert space, they occur in a laboratory.
>
> - Asher Peres.

Em 1994, Sandu Popescu e Daniel Rohrlich [54] apresentaram os primeiros exemplos de correlações não-locais mais fortes que as presentes em qualquer sistema quântico, e que, apesar disso, respeitam a condição de não-sinalização. Esse resultado inspirou o levantamento da seguinte questão: por que a mecânica quântica é incapaz de reproduzir tais correlações? Existiria um princípio físico que impediria sua existência?

Neste capítulo abordamos as correlações não-sinalizadoras em sua totalidade. Apresentamos sua estrutura matemática e possíveis aplicações na teoria da informação, onde, particularmente em criptografia, correlações não-locais são responsáveis pela segurança incondicional em protocolos de distribuição quântica de chaves. Ainda, introduzimos a causalidade da informação, candidata a princípio físico responsável pela não-localidade limitada das correlações quânticas.

5.1 Além das correlações quânticas

5.1.1 A cota de Tsirelson

A cota de Tsirelson [53] é uma evidência de que as correlações quânticas não podem ser arbitrariamente não-locais. No capítulo 4, seção 4.4, mostrou-se que a máxima violação da desigualdade CHSH para um estado puro de 2 qubits, escrito em sua forma de Schmidt como $|\psi\rangle = \cos(\varphi)|00\rangle + \text{sen}(\varphi)|11\rangle$, é

$$\max \left| \langle \mathcal{B}_{CHSH} \rangle_{|\psi\rangle} \right| = 2\sqrt{1 + \sin^2(2\varphi)}. \tag{5.1}$$

Desta equação, conclui-se que

$$\left|\langle \mathcal{B}_{CHSH} \rangle_{|\psi\rangle}\right| \leq 2\sqrt{2}. \tag{5.2}$$

Qualquer estado misto pode ser escrito como combinação convexa de estados puros. Por isso, a cota acima é verdadeira para qualquer estado de dois qubits. Na verdade, esta cota vale para qualquer estado de sistemas quânticos bipartidos. Para a prova, é suficiente considerar apenas medições projetivas - um resultado obtido em [68] prova que, em cenários de Bell quânticos bipartidos, as maiores violações são obtidas através de medições projetivas. Sejam observáveis unitários $\mathbf{A}_0, \mathbf{A}_1, \mathbf{B}_0, \mathbf{B}_1$ associados às medições projetivas de Alice e Bob, e tome o quadrado do observável de Bell, que pode ser escrito como

$$\mathcal{B}^2_{CHSH} = 4.\mathbf{1} - [\mathbf{A}_0, \mathbf{A}_1] \otimes [\mathbf{B}_0, \mathbf{B}_1]\,. \tag{5.3}$$

Utilizando a desigualdade $||[\mathbf{V}, \mathbf{W}]|| \leq 2\,||\mathbf{V}||\,||\mathbf{W}||$, onde $||\mathbf{O}||$ é definido como o maior autovalor, em módulo, do operador $\mathbf{O}$, tem-se

$$\left|\left|\mathcal{B}^2_{CHSH}\right|\right| \leq 4 + 4\,||\mathbf{A}_0||\,||\mathbf{A}_1||\,||\mathbf{B}_0||\,||\mathbf{B}_1||\,. \tag{5.4}$$

Uma vez que todos os observáveis são unitários, suas normas são iguais a 1, o que resulta na cota

$$\left|\left|\mathcal{B}^2_{CHSH}\right|\right| \leq 8. \tag{5.5}$$

A maior violação quântica de uma desigualdade de Bell corresponde ao maior autovalor possível do observável de Bell correspondente à igualdade. Como $||\mathbf{O}^2|| = ||\mathbf{O}||^2$, tem-se a cota de Tsirelson,

$$\mathrm{Tr}\,(\rho \mathcal{B}_{CHSH}) \leq 2\sqrt{2}. \tag{5.6}$$

5.1.2 Caixas não-sinalizadoras

Fixado um cenário de Bell, o foco é voltado exclusivamente para as probabilidades conjuntas que o descrevem. A imagem de experimentos sendo realizados de forma sincronizada em laboratórios distantes, apesar de didática e inspiradora, é desnecessária e, talvez, capciosa, no sentido em que pode induzir o leitor a crer que todas as correlações não-sinalizadoras de um cenário de Bell podem ser obtidas através de medições em sistemas físicos.

Até o presente ponto, nesta dissertação, esta perspectiva foi inofensiva. Todas as correlações não-locais apresentadas até o momento podem ser obtidas por meio de medições em sistemas quânticos. Porém, serão apresentadas correlações que, violando a cota de Tsirelson, não gozam desta

propriedade. Por isso é conveniente introduzir uma nova perspectiva, mais abstrata, que resulta em uma linguagem fácil para se falar de correlações não-locais sem que seja necessário recorrer a experimentos hipotéticos de medições em sistemas físicos.

De maneira abstrata, um cenário de Bell de duas partes é completamente equivalente a *caixas pretas*[1] compartilhadas entre as partes, cujo mecanismo de funcionamento é desconhecido. Cada uma das partes alimenta sua divisão da caixa com *entradas* x e y, respectivamente, escolhidas de conjuntos pré-fixados. A caixa retorna *saídas* a e b com probabilidades conjuntas $p_{a,b|x,y}$, que obedecem à condição de não-sinalização. Os termos 'caixa' e 'correlação' serão utilizados como sinônimos. Essa perspectiva é especialmente conveniente do ponto de vista da teoria da informação, em que correlações não-locais são recursos que, assim, podem ser identificados com as caixas em questão.

5.2 O conjunto das correlações não-sinalizadoras

Introduzido no capítulo 3, o conjunto $\mathcal{P}$ das correlações não-sinalizadoras é definido como os pontos $p \in \mathbb{R}^t$ que satisfazem às condições de positividade

$$p_{a,b|x,y} \geq 0, \quad \forall\ a, b, x, y; \tag{5.7}$$

normalização,

$$\sum_{a=0}^{v_x-1} \sum_{b=0}^{v_y-1} p_{a,b|x,y} = 1, \quad \forall\ x, y; \tag{5.8}$$

e não-sinalização,

$$\begin{aligned} \sum_{b=0}^{v_y-1} p_{a,b|x,y} &= p_{a|x}, \quad \forall\ a, x, y; \\ \sum_{a=0}^{v_x-1} p_{a,b|x,y} &= p_{b|y}, \quad \forall\ b, x, y. \end{aligned} \tag{5.9}$$

As equações (5.8) e (5.9) determinam o *fecho afim* de $\mathcal{P}$, o menor subconjunto afim de $\mathbb{R}^t$ que contém $\mathcal{P}$. A dimensão deste espaço, que é a mesma de $\mathcal{P}$ (*vide* [12], cap. 3), é

$$t' = \Pi_{i=1}^{n} \left[\sum_{j=0}^{m_i} (v_{ij} - 1) + 1 \right] - 1, \tag{5.10}$$

[1] Do inglês *black boxes*.

onde n é o número de partes, m_i o número de possíveis medições da i-ésima parte e v_{ij} o número de resultados da j-ésima medição da i-ésima parte. O fecho afim de $\mathcal{P}$ é também o fecho afim de $\mathcal{L}$ e $\mathcal{Q}$, portanto, $dim\,(\mathcal{Q}) = dim\,(\mathcal{L}) = dim\,(\mathcal{P}) = t'$.

Assim como $\mathcal{L}$, o conjunto $\mathcal{P}$ é um politopo convexo. Seus pontos extremais podem ser divididos em duas classes: os pontos locais, que são pontos extremais de $\mathcal{L}$, e pontos não-locais. No cenário $(2, 2, 2)$, o politopo de não-sinalização tem dimensão $t' = 8$ e 24 pontos extremais. Os 16 vértices locais podem ser escritos como

$$p_{a,b|x,y} = \begin{cases} 1, & \text{se} \quad a = \alpha x \oplus \beta, \quad b = \gamma y \oplus \delta \\ 0, & \text{senão} \end{cases}, \tag{5.11}$$

onde $\alpha, \beta, \gamma, \delta \in \{0, 1\}$. Aqui e adiante, o símbolo $\oplus$ denota adição módulo 2. Os 8 vértices não-locais são

$$p_{a,b|x,y} = \begin{cases} 1/2, & \text{se} \quad a \oplus b = xy \oplus \alpha x \oplus \beta y \oplus \gamma \\ 0, & \text{senão} \end{cases}, \tag{5.12}$$

onde $\alpha, \beta, \gamma \in \{0, 1\}$.

Usando renomeações locais, cada parte pode converter um vértice em qualquer outro da mesma classe. Alice, por exemplo, pode renomear suas entradas $x \mapsto x \oplus 1$, ou suas saídas, de forma condicionada à entrada, $a \mapsto a \oplus \alpha x \oplus \beta$. Assim, cada vértice local 'd equivalente a

$$p_{a,b|x,y} = \begin{cases} 1, & \text{se} \quad a = 0, b = 0 \\ 0, & \text{senão} \end{cases}, \tag{5.13}$$

a menos de renomeações locais. Da mesma forma, cada vértice não-local é equivalente a

$$p_{a,b|x,y} = \begin{cases} 1/2, & \text{se} \quad a \oplus b = xy \\ 0, & \text{senão} \end{cases}. \tag{5.14}$$

A órbita de desigualdades obtidas de CHSH por renomeações de resultados tem 8 elementos, que representam as facetas não-triviais do politopo local $\mathcal{L}$ do cenário $(2, 2, 2)$ (*vide* cap. 3, seção 3.5). Existe uma importante relação entre estas desigualdades e os vértices não-locais do politopo $\mathcal{P}$. Considere a seguinte notação

$$\langle ij \rangle \equiv \sum_{a,b=0}^{1} (-1)^{a+b} p_{a,b|x=i,y=j}. \tag{5.15}$$

As 8 desigualdades podem ser escritas como

$$\beta_{CHSH}^{\alpha\beta\gamma} = (-1)^{\gamma} \langle 00 \rangle + (-1)^{\beta+\gamma} \langle 01 \rangle + (-1)^{\alpha+\gamma} \langle 10 \rangle + (-1)^{\alpha+\beta+\gamma} \langle 11 \rangle \leq 2, \tag{5.16}$$

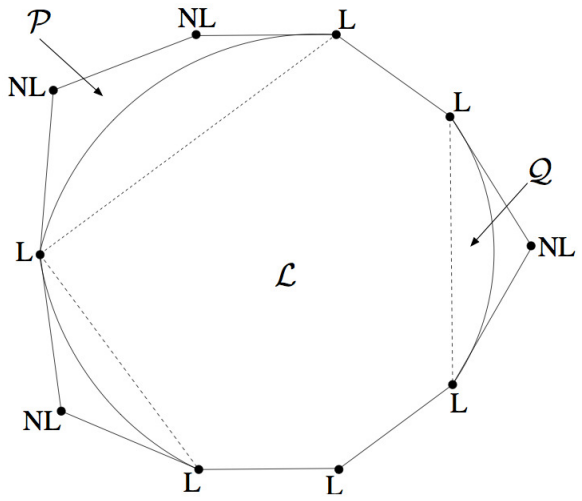

Figura 5.1: Representação do espaço de caixas não-sinalizadoras. Os vértices locais são rotulados L e os vértices não-locais são rotulados NL. As desigualdades de Bell são as facetas representadas por linhas tracejadas.

onde $\alpha, \beta, \gamma \in \{0, 1\}$. Cada um dos parâmetros tem a cota algébrica $\left|\beta_{CHSH}^{\alpha\beta\gamma}\right| \leq 4$. Existe uma correspondância 1-para-1 entre os vértices não-locais de $\mathcal{P}$ e as facetas de $\mathcal{L}$, com cada desigualdade sendo violada até seu limite algébrico pelas correlações com α, β, γ correspondentes na equação (5.12). Essas caixas extremamente não-locais ficaram conhecidas como *caixas PR*, devido a Sandu Popescu e Daniel Rohrlich [54].

As condições de positividade (5.7) definem facetas de $\mathcal{P}$. Elas também definem facetas triviais de $\mathcal{L}$, mas o politopo local também possui facetas não-triviais que são as desigualdades de Bell. Como as correlações quânticas podem violar as desigualdades de Bell, tem-se que $\mathcal{L} \subset \mathcal{Q}$. No entanto, elas violam CHSH até a cota de Tsirelson, e constituem um subconjunto próprio de $\mathcal{P}$. Assim $\mathcal{L} \subset \mathcal{Q} \subset P$.

5.3 Complexidade da comunicação

Nas ciências da computação, diferentes tarefas são comparadas de acordo com sua *complexidade*. A complexidade de determinada tarefa pode ser avaliada através dos recursos necessários para sua execução, como a quantidade de memória ou o número de operações lógicas realizadas. Em computação distribuída, a *complexidade de comunicação* é particularmente im-

portante: ela é a quantidade de comunicação necessária entre duas partes para que se possa avaliar uma *função distribuéda*, que tem seus argumentos divididos entre as duas partes. Considere que as variáveis sejam *bits* e a função distribuída receba como argumentos duas seqüências de n bits, $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$; a seqüência de Alice será denotada $\vec{x}$ e a de Bob $\vec{y}$. A complexidade de comunicação de uma função $f = f(\vec{x}, \vec{y})$ é o menor número de bits que devem ser transmitidos entre as partes para que a função seja corretamente avaliada. Considere, por exemplo, a função produto interno[2],

$$f(\vec{x}, \vec{y}) = \sum_{i}^{n} x_i.y_i. \tag{5.17}$$

É fácil ver que esta função tem complexidade de comunicação n, a maior possível, uma vez que, na melhor estratégia possível, uma das partes deve conhecer toda a seqüência em posse da outra para que possa calculá-la.

Em 2000, Win van Dam [56] provou que, se duas partes têm acesso a caixas PR, a complexidade de comunicação de qualquer função distribuída entre elas é trivial, *i.e.*, o envio de 1 único bit é suficiente. O primeiro passo da prova deste importante resultado é a observação de que qualquer função $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ pode ser escrita como um polinômio, em várias variáveis. Isso pode ser melhor visualidado se observado, primeiramente, que qualquer função elementar de dois bits pode ser implementada com as operações soma e produto, e, funções mais complexas, implementadas através de funções elementares. Ainda, estes polinômios podem ser reescritos como

$$f(\vec{x}, \vec{y}) = \sum_{i}^{2^n} P_i(\vec{x}).Q_i(\vec{y}), \tag{5.18}$$

onde $P_i(\vec{x})$ são polinômios em $\vec{x} \in \{0,1\}^n$ e $Q_i(y)$ são monômios em $\vec{y} \in \{0,1\}^n$. No total, existem 2^n diferentes monômios

$$Q_i(\vec{y}) = \Pi_{j \in J} y_j$$

- um para cada $J \in \{0, \ldots, n\}$ - , e, por isso, o índice i é limitado a $1 \leq i \leq 2^n$.

Assim, qualquer função $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ pode ser reescrita como uma função produto interno de seqüências de 2^n bits, pois cada polinômio $P_i(\vec{x})$ pode ser localmente calculado por Alice sem necessidade de comunicação com Bob, resultando em um bit x'_i de uma nova seqüência $\vec{x}' = (x'_1, \ldots, x'_{2^n})$; o mesmo valendo para Bob e seus monômios, que resulta

[2] As operações produto (.) e adição ($\oplus$) são avaliadas em aritmética módulo 2.

em uma nova seqüência $\vec{y}' = (y'_1, \ldots, y'_{2^n})$. Portanto, se as partes conseguem avaliar a função "produto interno" de seqüências de 2^n bits com o envio de um único bit, elas são capazes de avaliar qualquer função de pares de seqüências de n bits também com o envio de um bit.

Suponha que Alice e Bob compartilham partes de uma caixa PR, que, respectivamente, são alimentadas com entradas x e y e retornam saídas a e b, que sempre satisfazem $a \oplus b = x.y$. Para avaliar o função produto interno de seqüências $\vec{x}'$ e $\vec{y}'$ de N bits Alice e Bob podem utilizar a caixa PR N vezes, colocando como entradas os elementos de suas respectivas seqüências, e obtendo como saídas, ao final do processo, duas seqüências $\vec{a'}$ e $\vec{b'}$ que satisfazem, termo a termo, a relação $a'_i \oplus b'_i = x'_i.y'_i$. Se $N = 2^n$, tem-se que

$$\begin{aligned} f(\vec{x}, \vec{y}) &= \sum_i^{2^n} x'_i.y'_i \\ &= \sum_i^{2^n} (a' + b') \\ &= \left(\sum_i^{2^n} a'_i \right) + \left(\sum_i^{2^n} b'_i \right). \end{aligned} \tag{5.19}$$

O primeiro termo do produto é a soma das saídas obtidas por Alice, e, o segundo, a soma das saídas obtidas por Bob; ambos podem ser calculados localmente. Basta, portanto, que um deles comunique um único bit, o total de sua soma, para que o outro seja capaz de avaliar a função produto interno, e, conseqüentemente, qualquer função booleana. Assim é provada a trivialização da complexidade de comunicação se recursos não-locais fortes são permitidos.

5.4 Causalidade da informação

A mecânica quântica é a única teoria física que prevê a existência de correlações não-locais. Este fato chamou a atenção de Popescu e Rohrlich [54], que apontaram a não-localidade como um axioma da teoria quântica, um princípio físico que destacaria esta teoria frente às demais. No entanto, correlações como as caixas PR, que violam a cota de Tsirelson e, ao mesmo tempo, obedecem à condição de não-sinalização, evidenciam a possibilidade de outras teorias que, assim como a mecânica quântica, são não-locais e não-sinalizadores. Ganhou importância, assim, a busca por um princípio físico que explicaria as limitações na não-localidade quântica.

Recentemente proposta, a *causalidade da informação* [57] é forte candidata a tal princípio. Ela generaliza a idéia de não-sinalização e é respeitada pelas teorias clássica e quântica, ao passo que é violada por teorias que admitem correlações mais não-locais que as quânticas. Seu enunciado diz que a transmissão de m bits clássicos pode causar um ganho de informação de, no máximo, m bits. A condição de não-sinalização é, assim, causalidade da informação para $m = 0$.

Considere a seguinte situação, uma tarefa cuja eficiência de execução é limitada por causalidade da informação. Alice recebe N bits aleatórios e independentes, organizados no vetor $\vec{x} = (x_0, \ldots, x_{N-1})$. Em um lugar distante, Bob recebe uma variável aleatória $i \in \{0, \ldots, N-1\}$. Alice pode enviar q bits clássicos para Bob, com a ajuda dos quais Bob deve advinhar o valor do i-ésimo bit na lista de Alice, x_i. Bob pode responder corretamente o valor de q bits. Se Alice o envia uma mensagem $\vec{m} = (x_0, \ldots, x_{q-1})$, Bob responderá corretamente sempre que $i \in \{0, \ldots, q-1\}$. No entanto, se $i \in \{q, \ldots, N-1\}$, não resta a Bob opção senão arriscar o resultado. Alice e Bob podem compartilhar e utilizar recursos não-sinalizadores, mas como eles contém informação a respeito de $\vec{x}$, em toda estratégia haverá um compromisso entre as probabilidades de Bob advinhar os diferentes bits de Alice.

Denote a saída de Bob por β. A eficiência da estratégia de Alice e Bob é quantificada por

$$\mathcal{I} \equiv \sum_{K=0}^{N-1} I\left(x_k : \beta | i = K\right), \tag{5.20}$$

onde $I\left(x_k : \beta | i = K\right)$ é a *informação mútua* entre x_K e β, *condicionada* ao recebimento da variável $i = K$ por Bob. A *informação mútua* quantifica a dependência mútua entre duas variáveis aleatórias, e pode ser definida como

$$I\left(x : y\right) = \sum_x \sum_y p_{x,y} \log\left(\frac{p_{x,y}}{p_x p_y}\right). \tag{5.21}$$

A informação mútua condicional satisfaz

$$I\left(x : y, z\right) = I\left(x : y, z\right) - I\left(x : z\right). \tag{5.22}$$

Em [57], é provado que

$$\mathcal{I} \geq N - \sum_{K=0}^{N-1} S\left(P_K\right), \tag{5.23}$$

onde $S\left(x\right) = -x\log\left(x\right) - \left(1-x\right)\log\left(1-x\right)$ é a entropia de Shannon de uma distribuição de probabilidades de dois elementos, e P_K é a probabilidade

de $x_K = \beta$. Para se chegar a esta desigualdade, assumiu-se que x_K é independentemente distribuído com probabilidades iguais. Causalidade da informação é respeitada se

$$\mathcal{I} \leq m. \tag{5.24}$$

O parâmetro $\mathcal{I}$ é inteiramente determinado pelas entradas de Alice e Bob e a saída de Bob.

Para se entender como correlações não-sinalizadores podem violar o princípio de causalidade local, considere o caso mais simples, em que Alice recebe dois bits, e pode enviar apenas um bit a Bob. Ambos compartilham recursos não-locais através de caixas PR, e podem utilizá-los para cumprir a tarefa proposta. Tome a seguinte estratágia: Alice alimenta sua parte da caixa com a entrada $x = x_0 + x_1$ e Bob, por sua vez, alimenta sua parte da caixa com a entrada $y = i$, se ele deseja saber o bit x_i de Alice. Eles obtém, respectivamente, a saída a, utilizada por Alice na computação do bit que enviará a Bob, $r = x_0 + a$, e b. Ao receber o bit r de Alice, Bob computa seu palpite

$$\begin{aligned} \beta &= r \oplus b & (5.25)\\ &= x_0 \oplus a \oplus b & (5.26)\\ &= x_0 \oplus (x_0 \oplus x_1)\,.i & (5.27)\\ &= x_i. & (5.28) \end{aligned}$$

Se Alice e Bob compartilham uma caixa PR, com a estratégia acima descrita Bob sempre acerta o valor do bit por ele escolhido, independente de qual seja. Tem-se, assim,

$$\mathcal{I} = 2, \quad \text{para} \quad q = 1; \tag{5.29}$$

Com o envio de um único bit, por Alice, Bob tem acesso a 2 bits de informação.

Em [57], Marcin Pawlowski e colaboradores provam que qualquer correlação que satisfaz a cota de Tsirelson obedece à causalidade da informação, enquanto que correlações mais não-locais que as quânticas, neste cenário, violam este princípio, como no exemplo acima. No entanto, não se sabe se o mesmo vale em outros cenários.

5.5 Criptografia

Criptografia é a prática e a ciência de se esconder, transmitir e reobter informação de forma segura. Em seus terrenos, a mecânica quântica encontrou uma vasta gama de aplicações, o que resultou na chamada *criptografia*

quântica, o uso de sistemas quânticos com o intuito de realizar tarefas criptográficas.

A principal tarefa atribuída à criptografia quântica é a *distribuição quântica de chaves (QKD)*[3]. Em uma importante classe de protocolos criptográficos, duas partes interessadas em estabelecer um canal seguro de comunicação devem possuir *chaves criptográficas* - coleções de bits aleatórios - correlacionadas entre si, somente. Uma das partes, suponha, Alice, utiliza sua chave para *codificar* a mensagem a ser transmitida, de forma que somente Bob, que possui uma chave correspondente, pode *decodificá-la*. A mensagem codificada, então, pode ser enviada através de um canal público de comunicação - rádio, tv, internet - pois mesmo uma terceira parte - Eva, como é comumente chamada na literatura - , possivelmente mal intencionada, interceptando a mensagem codificada, não será capaz de obter dela informação alguma[4]. A única dificuldade nos chamados *protocolos criptográficos de chave privada* é a distribuição das chaves criptográficas: Eva concentra seus *ataques* neste estágio com o objetivo de obter informação sobre as chaves.

Uma grande vantagem da utilização de sistemas quânticos em tarefas de distribuição de chaves é que, em geral, intervenções realizadas por Eva durante o processo danificam a chave obtida, e, assim, podem ser detectadas, *a posteriori*, por Alice e Bob. Esta habilidade permite a eles distingüir entre chaves seguras e chaves não-seguras, e utilizar somente aquelas provadamente confiáveis.

5.5.1 O protocolo BB84

O primeiro protocolo de QKD foi criado por Charles Bennett e Giles Brassard em 1984, e ficou conhecido pela sigla BB84 [58].

Alice começa com o sorteio de dois bits, α e a. A partir destes valores,

[3]Do inglês *quantum key distribution*.

[4]Um tipo de codificação chamado *one-time pad* é impossível de se quebrar, caso utilizado corretamente. Seu uso correto depende de chaves verdadeiramente aleatórias, necessariamente tão longas quanto a mensagem, que devem ser sumariamente descartadas após o uso.

Alice prepara um qubit no estado $|\psi\rangle = |\psi_{\alpha,a}\rangle$, onde

$$\begin{aligned} |\psi_{0,0}\rangle &= |0\rangle\,, \\ |\psi_{0,1}\rangle &= |1\rangle\,, \\ |\psi_{1,0}\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \\ |\psi_{1,1}\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned} \tag{5.30}$$

O bit α determina a escolha de uma base de $\mathcal{H}^2$: $\alpha = 0$ implica a escolha da base $\mathcal{Z} = \{|0\rangle\,, |1\rangle\}$, e $\alpha = 1$ implica a escolha da base $\mathcal{X} = \{|+\rangle\,, |-\rangle\}$, onde

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}. \tag{5.31}$$

O bit a determina o elemento da base escolhida em que Alice prepara o qubit. Alice, então, envia o qubit preparado para Bob, que sorteia um bit β e, de acordo com o valor obtido, realiza uma medição projetiva na base correspondente: $\beta = 0$ implica medição na base $\mathcal{Z}$; $\beta = 1$ implica medição na base $\mathcal{X}$. O resultado obtido por Bob é um bit, denotado b.

Esse processo é reiterado um grande número de vezes; ao final, Alice tem duas seqüências de bits, $\{\alpha_i\}$ e $\{a_i\}$, assim como Bob, que possui as seqüências $\{\beta_i\}$ e $\{b_i\}$. De acordo com a mecânica quântica, se $\alpha_i = \beta_i$, então $a_i = b_i$; se $\alpha_i \neq \beta_i$, então $a_i = b_i$ com probabilidade $1/2$ e $a_i \neq b_i$ com igual probabilidade.

No passo seguinte, Alice e Bob divulgam publicamente suas seqüências $\{\alpha_i\}$ e $\{\beta_i\}$. Comparando cada uma das entradas, eles descartam todos os bits a_j e b_j para os quais $\alpha_j \neq \beta_j$. Desta forma eles terão um par de seqüências reduzidas $\{a'_i\}$ e $\{b'_i\}$ tais que $a'_i = b'_i \;\forall\, i$.

A segurança do protocolo depende dos possíveis ataques que Eva poderia fazer à comunicação de Alice e Bob. O *teorema de não-clonagem* (*vide* [5] pg. 532) garante que Eva não pode interceptar os qubits enviados por Alice, fazer cópias deles, e reenviá-los para Bob, esperando pela divulgação das bases em que deve realizar as medições projetivas. O que Eva poderia fazer é a substituição do sistema original por um segundo sistema preparado por ela. No entanto, esta intervenção, em geral, destruiria a correlação perfeita entre as seqüências $\{a'_i\}$ e $\{b'_i\}$. Comparando parte dessas seqüências, Alice e Bob poderiam detectar a presença da terceira parte espiã, às custas de perder alguns bits de suas chaves.

5.5.2 O protocolo E91

Uma importante variação do protocolo BB84 foi criada em 1991 por Artur Ekert [33]. Neste protocolo, uma fonte prepara sistemas de dois qubits no estado singleto,

$$\left|\psi^{-}\right\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \tag{5.32}$$

e cada partícula é enviada a cada uma das partes, Alice e Bob. Cada um deles, então, realiza uma de três possíveis medições em sua partícula: Alice pode realizar a medição dos observáveis $\mathbf{A}_\alpha$

$$\begin{aligned} \mathbf{A}_0 &= \sigma_3, \\ \mathbf{A}_1 &= \frac{1}{\sqrt{2}}\left(\sigma_1 + \sigma_3\right), \\ \mathbf{A}_2 &= \sigma_1; \end{aligned} \tag{5.33}$$

Bob, por sua vez, pode medir os observáveis $\mathbf{B}_\beta$

$$\begin{aligned} \mathbf{B}_0 &= \frac{1}{\sqrt{2}}\left(\sigma_1 - \sigma_3\right), \\ \mathbf{B}_1 &= \frac{1}{\sqrt{2}}\left(\sigma_1 + \sigma_3\right), \\ \mathbf{B}_2 &= \sigma_1. \end{aligned} \tag{5.34}$$

O processo é reiterado um grande número de vezes. Ao final, Alice tem uma seqüência $\{\alpha_i\}$, com os rótulos das medições realizadas, e $\{a_i\}$, uma seqüência de bits com os respectivos resultados. Analogamente, Bob tem uma seqüência $\{\beta_i\}$, com os rótulos das medições, e uma seqüência de bits $\{b_i\}$ com os resultados obtidos. Então, as seqüências $\{\alpha_i\}$ e $\{\beta_i\}$ são divulgadas publicamente; sua comparação, termo a termo, permite que os elementos das seqüências $\{a_i\}$ e $\{b_i\}$ sejam organizados em duas coleções: a coleção dos resultados a_i e b_i tais que $\alpha_i = \beta_i$, para $\beta_i \in \{1, 2\}$, e a coleção dos resultados restantes. Esta última coleção é divulgada, o que permite que Alice e Bob possam estimar o valor de $\langle \mathbf{A}_0 \otimes \mathbf{B}_0 \rangle$, $\langle \mathbf{A}_0 \otimes \mathbf{B}_1 \rangle$, $\langle \mathbf{A}_2 \otimes \mathbf{B}_0 \rangle$, $\langle \mathbf{A}_2 \otimes \mathbf{B}_1 \rangle$. A chave criptográfica é formada pelos resultados organizados na outra coleção[5].

A segurança deste protocolo é baseada na violação da desigualdade CHSH. Se o estado compartilhado entre as partes é o estado (5.32), então (*vide* capítulo 4, seção 4.2)

$$\langle \mathbf{A}_0 \otimes \mathbf{B}_0 \rangle - \langle \mathbf{A}_0 \otimes \mathbf{B}_1 \rangle - \langle \mathbf{A}_2 \otimes \mathbf{B}_0 \rangle - \langle \mathbf{A}_2 \otimes \mathbf{B}_1 \rangle = 2\sqrt{2}. \tag{5.35}$$

[5]Observe que, nesta coleção, $a_i = \beta_i \oplus 1$.

Se a equação (5.35) é verificada, então as correlações observadas são necessariamente não-locais, o que implica que os resultados das medições realizadas não podem ser localmente pré-determinados. Suponha o contrário: todos os resultados obtidos por Alice podem ser determinados por Eva caso ela conheça variáveis locais λ e as medições realizadas, $\{\alpha_i\}$; da mesma forma, os resultados de Bob podem ser determinados através de λ e $\{\beta_i\}$. A informação sobre as medições realizadas é divulgada publicamente, portanto, basta que Eva tenha acesso a λ para que possa determinar a chave criptográfica. A verificação de (5.35) impede a existência de uma estratégia como a descrita e garante a segurança da chave nesse sentido.

5.5.3 Criptografia independente de dispositivos

As provas de segurança usuais de protocolos QKD são baseadas na premissa de que as partes legítimas, Alice e Bob, têm conhecimento e controle completos sobre seus sistemas e aparatos quânticos. Em [59], Acín, Gisin e Masanes apresentam um exemplo que mostra claramente quão crucial é esta condição.

O protocolo BB84 é considerado, em uma versão um pouco diferente da aqui apresentada. A diferença é que as partes, assim como no protocolo E91, compartilham qubits no estado singleto. Por isso, Alice deve realizar medições em suas partículas, ao invés de prepará-las; todos os demais passos do protocolo são iguais. Sabe-se que este protocolo é seguro desde que a taxa de erro seja inferior a certo limiar [60]. No entanto, este resultado é verdadeiro para 2 qubits apenas, e existem estados de 4 qubits para os quais a taxa de erro é zero mesmo quando Eva tem conhecimento completo a respeito da chave.

O ponto crítico é que, na prática, é muito difícil garantir a dimensionalidade de um sistema quântico. Este problema pode ser evitado em uma nova abordagem, recentemente proposta: *criptografia independente de dispositivos*[6]. Nesta abordagem, a segurança dos protocolos é baseada na violação de desigualdades de Bell, no espírito do protocolo E91. Em [59], é provado que, se as correlações obtidas no processo de distribuição de chaves violam a desigualdade CHSH, então o conhecimento de Eva sobre a chave criptográfica é limitado, mesmo que, em seus ataques, Eva disponha de recursos não-locais limitados apenas pela condição de não-sinalização. Neste contexto, é interessante que a Eva é permitido, inclusive, fabricar os dispositivos que serão utilizados por Alice e Bob para a QKD; caso as correlações obtidas sejam não-locais, a chave é segura, indepententemente

[6]Do inglês *device independent cryptography*.

do dispositivo utilizado. Em 2009 [61], Lluis Masanes estende essa prova ao melhor e mais rigoroso critério de segurança conhecido, o chamado *universally composable security*.

Considerações finais

Nesta dissertação, apresentamos a definição e as mais importantes propriedades da não-localidade, além de destacar sua importância tanto para uma compreensão fundamental da Natureza quanto para aplicações práticas na teoria quântica da informação. Antes de concluí-la, porém, vale citar alguns possíveis caminhos para se seguir, a partir daqui.

Um importante problema a se entender é a intrincada relação entre não-localidade e emaranhamento. Há estados emaranhados que não apresentam correlações não-locais em nenhum dos cenários de Bell conhecidos. Eles apresentariam não-localidade em outros cenários, mais complexos? Em particular, um problema relacionado que despertou interesse nos últimos anos envolve os estados emaranhados PPT. Conjecturou-se que estes estados não podem apresentar correlações não-locais, mas não existe prova nem contra-exemplo.

Para ambos os conceitos, os casos bipartidos foram extensamente estudados, mas pouco se sabe sobre os casos multipartidos. Nesses cenários, a rica estrutura do emaranhamento inspira o conceito de não-localidade genuína multipartida, que, apesar de alguns resultados conhecidos, necessita de mais investigação.

Com a observação de que não-localidade pode ser um recurso, a busca por aplicações é imediata. Aplicações conhecidas envolvem protocolos de distribuição de chaves criptográficas, mas seu uso como recurso fora da criptografia ainda é pouco explorado, e oferece inúmeras possibilidades. Neste contexto, a quantificação da não-localidade como recurso torna-se uma questão de igual importância.

Por fim, vale ressaltar que o conjunto das correlações quânticas carece de caracterização inclusive no cenário mais simples. Ao contrário do conjunto de correlações locais, o conjunto de correlações quânticas não é um politopo convexo, e sua fronteira não é plenamente conhecida. Essa questão está intimamente ligada à busca por um princípio físico que destaque a fronteira

do conjunto de correlações quânticas e justifique sua distinção dentro do conjunto de correlações não-sinalizadoras.

Bibliografia

[1] A. Peres; *"Quantum theory: concepts and methods"*, Kluwer Academic Publishers (1995).

[2] J. von Neumann; *"Mathematical foundations of quantum mechanics"*, Princeton University Press (1955).

[3] R.P. Feynman, R.B. Leighton, M. Sands; *"The Feynman lectures on Physics, vol.3"*, Addison-Wesley publishing company (1965).

[4] C. Cohen-Tannoudji, B. Diu, F. Lalöe; *"Quantum mechanics"*, Wiley-Interscience (2006).

[5] M.A. Nielsen, I.L. Chuang; *"Quantum computation and quantum information"*, Cambridge University Press (2000).

[6] M. O. Terra Cunha; *"Noções de informação quântica"*, IMPA (2007).

[7] E. Schrödinger; *Naturwissenschaften* **23**, 807 (1935).

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

[9] A. Einstein, B. Podolski, N. Rosen; "Can quantum-mechanical description of physical reality be considered complete?", *Phys. Rev.* **47**, 777 (1935).

[10] D. Bohm; *"Quantum Theory"*, Prentice-Hall (1951).

[11] J. S. Bell, "On the Einstein Podolsky Rosen paradox", *Physics* **1**, 3, 195 (1964).

[12] S. Pironio; *"Aspects of quantum nonlocality"*, tese de doutorado, Université Libre de Bruxelles (2004).

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

[14] A. Fine; "Hidden variables, joint probability, and the Bell inequalities", *Phys. Rev. Lett.* **48**, 291 (1982).

[15] J. F. Clauser and M. A. Horne; "Experimental consequences of objective local theories", *Phys. Rev. D.* **10**, 526 (1074).

[16] http://www.zib.de/Optimization/Software/Porta.

[17] http://www.maths.ed.ac.uk/ gondzio/software/hopdm.html.

[18] I. Pitowski; "Correlation polytopes: their geometry and complexity", *Mathematical Programming* **50**, 395 (1991).

[19] I. Bárány, A. Pór; "On 0-1 polytopes with many facets", *Adv. Math.* **161**, 209 (2001).

[20] C. Sliwa; "Symmetries of the Bell correlation inequalities", *Phys. Lett. A.* **317**, 165 (2003).

[21] D. Collins, N. Gisin; "A relevant two qubit Bell inequality inequivalent to the CHSH inequality",*J. Phys. A: Math. Gen.* **35**, 1775 (2004).

[22] M. Froissard;"Nuovo Cimento B" **64**, 241 (1981).

[23] I. Pitowski, K. Svozil; "Optimal tests of quantum nonlocality", *Phys. Rev. A.* **64**, 014102 (2001).

[24] D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu; "Bell inequalities for arbitrarily high-dimensional systems", *Phys. Rev. Lett.* **88**, 040404 (2002).

[25] M. Navascués, S. Pironio, A. Acín; "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations", *New Journal of Physics* **10**, 073013 (2008).

[26] J. Barrett; "Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality", *Phys. Rev. A.* **65**, 042302 (2002).

[27] N. Gisin; "Bell's inequality holds for all non-product states", *Phys. Lett. A.* **154**, 201 (1991).

[28] R. Horodecki, P. Horodecki, M. Horodecki; "Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition", *Phys. Lett. A.* **200**, 340 (1995).

[29] D. M. Greenberger, M. A. Horne, A. Zeilinger; em "Bell's theorem, quantum theory, and conceptions of the Universe", Kluwer Academic Publishers (1989).

[30] D. M. Greenberger, M. A. Horne, A. Shimony, A. Zeilinger; "Bell's theorem without inequalities", *Am. J. Phys.* **58**, 1131 (1990).

[31] D. Mermin; "Extreme quantum entanglement in a superposition of macroscopically distinct states", *Phys. Rev. Lett.* **65**, 1838 (1990).

[32] C. H. Bennett, G. Brassard, C. Crápeau, R. Jozsa, A. Peres, W. K. Wootters ; "Teleporting an unknown quantum state via dual classical and Einstein-Podolski-Rosen channels", *Phys. Rev. Lett.* **70**, 1895 (1993).

[33] A. K. Ekert; "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.* **67**, 661 (1991).

[34] M. O. Terra Cunha; *"Emaranhamento: caracterização, manipulação e conseqüências"*, tese de doutorado, Universidade Federal de Minas Gerais (2005).

[35] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki; "Quantum entanglement", *Rev. Mod. Phys.* **81**, 865 (2009).

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

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

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

[39] B. M. Terhal; "Bell inequalities and the separability criterion", *Phys. Lett. A.* **221**, 319 (2000).

[40] P. Hyllus, O. Gühne, D. Bruss, M. Lewenstein; "Relations between entanglement witnesses and Bell inequalities", *Phys. Rev. A.* **72**, 012321 (2005).

[41] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani; "Device-independent security of quantum cryptography against collective attacks", *Phys. Rev. Lett.* **98**, 230502 (2007).

[42] G. Vidal; "Entanglemente monotones", *J. Mod. Opt.* **47**, 335 (2000).

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

[44] P. M. Hayden, M. Horodecki, B. M. Terhal; "The asymptotic entanglement cost of preparing a quantum state", *J. Phys. A: Math. Gen.* **34**, 6891 (2001).

[45] S. J. Freedman, J. F. Clauser; "Experimental test of local hidden-variable theories", *Phys. Rev. Lett.* **28**, 938 (1972).

[46] A. Aspect, J. Dalibard, G. Roger; "Experimental test of Bell's inequalities using time-varying analyzers", *Phys. Rev. Lett.* **49**, 1804 (1982).

[47] Z. Y. Ou, L. Mandel; "Violation of Bell's inequality and classical probability in a two-photon correlation experiment", *Phys. Rev. Lett.* **61**, 50 (1988).

[48] Y. H. Shih, C. O. Alley; "New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion", *Phys. Rev. Lett.* **61**, 2921 (1988).

[49] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger; "Violation of Bell's inequality under strict Einstein locality conditions", *Phys. Rev. Lett.* **81**, 5039 (1998).

[50] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, D. J. Wineland; "Experimental violation of a Bell's inequality with efficient detection", *Nature* **409**, 791 (2001).

[51] S. Popescu; "Bell's inequalities and density matrices: Revealing hidden nonlocality", *Phys. Rev. Lett.* **74**, 2619 (1995).

[52] L. Masanes; ""Asymptotic violation of Bell inequalities and distillability"", *Phys. Rev. Lett.* **97**, 050503 (2006)

[53] B. S. Cirel'son; "Quantum generalizations of Bell's inequality", *Lett. Math. Phys.* **4**, 93 (1980).

[54] S. Popescu, D. Rohrlich; "Nonlocality as an axiom", *Found. Phys.* **24**, 379, (1994).

[55] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts; "Non-local correlations as an information theoretic resource", *Phys. Rev. A.* **71**, 022101 (2005).

[56] W. van Dam,"Nonlocality and communication complexity", tese de doutorado, University of Oxford, (2000).

[57] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Zukowski; "Information causality as a physical principle", *Nature* **461**, 1101 (2009).

[58] C. H. Bennett, G. Brassard; *Proceedings of the international conference on computers, systems, and signal processing*, India (1984).

[59] A. Acín, N. Gisin, L. Masanes; "From Bell's theorem to secure quantum key distribution", *Phys. Rev. Lett.* **97**, 120405 (2006).

[60] P.W. Shor, J. Preskyll; "Simple proof of security of the BB84 quantum key distribution protocol", *Phys. Rev. Lett.* **85**, 441 (2000).

[61] L. Masanes; "Universable composable privacy amplification from causality constraints", *Phys. Rev. Lett.* **102**, 140501 (2009).

[62] Y.-C. Liang, N. Harrigan, S. D. Bartlett, T. Rudolph; "Nonclassical correlations from randomly chosen local measurements", *Phys. Rev. Lett.* **104**, 050401 (2010).

[63] L. Aolita, S. Walborn; "Quantum communication without alignment using multiple-qubit single-photon states", *Phys. Rev. Lett.* **98**, 100501 (2007).

[64] R. R. Werner, M. M. Wolf; "All-multipartite Bell-correlation inequalities for two dichotomic observables per site", *Phys. Rev. A.* **64**, 032112 (2001).

[65] M. Zukowski, C. Brukner; "Bell's theorem for general N-qubit states", *Phys. Rev. Lett.* **88**, 210401 (2002).

[66] M. Ardehali; "Bell inequalities with a magnitude of violation that grows exponentially with the number of particles", *Phys. Rev. A.* **46**, 5375 (1992).

[67] A. V. Belinski, D. N. Klychko; "Interference of light and Bell's theorem", *Phys. Usp.* **36**, 653 (1993).

[68] R. Cleve, P. Hoyer, B. Toner, J. Watrous; "Consequences and limits of nonlocal strategies", arXiv:quant-ph/0404076.