Não-localidade como recurso para comunicação

Autor: Marco Túlio Coelho Quintino
Orientador: Marcelo O. Terra Cunha

Setembro, 2010

Sumário

Resumo

Em 1935, durante suas investigações sobre fundamentos da mecânica quântica, Einstein, Podolsky e Rosen levantaram perguntas sobre a realidade das propriedades físicas de um sistema que possui suas partes espacialmente separadas. Estas perguntas ficaram por muito tempo amarradas a discussões filosóficas sem rigor matemático ou evidências experimentais. Foi apenas em 1964 que John S. Bell mostrou que exigir que uma variável seja capaz de prever o resultado das medições feitas em duas partes separadas de um sistema impõe restrições nas correlações entre essas. Em especial, a mecânica quântica prevê correlações que não podem ser atingidas por teorias ditas realistas locais.

Mesmo com o teorema de Bell, a não-localidade quântica ficou por muito tempo sendo tratada apenas como uma ferramenta para interpretar os postulados da teoria quântica. Hoje, compreendemos melhor esta não-localidade, e sabemos que ela pode ser usada como recurso para comunicação. Este trabalho vai abordar a mecânica quântica como uma teoria de informação para explorar os limites e consequências da não-localidade.

Abstract

In 1935 during investigations about the foundations of quantum mechanics, Einstein, Podolsky and Rosen raised some questions about the physical reality of properties of a system that has spatial separated parts. These questions where, for a long time, attached to philosophical discussions without any mathematical rigour or experimental evidences. It was only in 1964 that John S. Bell showed that predict the measurements made in two separated party system put some restrictions into their correlations. In special, quantum mechanics predicts correlations that can't be reached by local realist theories.

But, even with Bell's theorem, the quantum non-locality were for a very long time treated as just a tool to understand quantum mechanics postulates. Today, we have a better understanding of this non-locality, and know that it can be used as a resource for communication. This work treat quantum mechanics as an information theory to explore the limits and consequences of non-locality.

Prólogo

O emaranhamento quântico é o grande foco desta monografia, suas propriedades são tão particulares que Erwin Scrödinger chegou a afirmar *"I would not call that one but rather the characteristic trait of quantum mechanics"* [1]. Este trabalho vai explorar a não-localidade associada ao emaranhamento e encara-la como recurso para comunicação.

Apesar de essencial para toda monografia, o capítulo 1 tem o simples objetivo expor os postulados da mecânica quântica, definir emaranhamento e reconhecer que esta deve ser tratada como uma teoria de informação. Vou usar a notação canônica da área, de tal maneira que o leitor familiarizado com informação quântica possa compreender o resto do trabalho sem se preocupar com esta introdução.

O capítulo 2 vai explorar resultados importantes que envolvem a comunicação de duas partes, focando nas restrições impostas pela mecânica quântica e nas particularidades do emaranhamento. Irei tratar da informação contida em sistemas físicos, discutir copia e discriminação de estados quânticos, exibir protocolos que trocam bits por qubits e estabelecer uma cota máxima para a informação carregada por um sistema quântico. Este capítulo termina com um teorema relacionando emaranhamento com não-sinalização.

A definição de não-localidade aparece no capítulo 3, é nele que que vou explicitar as restrições impostas por uma teoria dita realista local. Começarei explorando as propriedades do estado singleto para fazer uma abordagem intuitiva destas correlações não-locais e, logo depois, apresentar a desigualdade CHSH para demonstrar que todo estado emaranhado apresenta não-localidade. Feito o vínculo emaranhamento/não-localidade, vamos verificar que existe uma cota para a não-localidade quântica, que implora a pergunta, "por quê não mais?". Para dar estrutura a esta pergunta irei apresentar as caixas Popescu-Rohrlich, uma metateoria que nos permite tratar de correlações supra-quânticas que respeitam a condição de não-sinalização. Com a base teórica fundamentada, levarei a discussão de realismo/localidade para o mundo prático, exibindo um protocolo de distribuição de chaves criptográficas que tem sua segurança baseada na impossibilidade de prever as correlações quânticas por um modelo realista-local. Encerro o capítulo com uma breve discussão sobre a verificação experimental da não-localidade quântica.

Entendido que teorias realistas locais nos impõe restrições, usarei uma linguagem de jogos de cooperação no capítulo 4 para ver as possíveis vantagens de jogadores que usam estratégias não-locais. Será apresentado o jogo do quadrado mágico, que possui uma estrutura muito simples, e pode-se facilmente

verificar que estratégias locais implicam que a probabilidade de sucesso dos jogadores é necessariamente menor que 1, enquanto o uso de estratégias não-locais permite que os jogadores ganhem sempre. Aproveitando a linguagem de jogos, irei tratar de um sistema com emaranhamento multipartite e, com o teorema de recurso mínimo para pseudotelepatia quântica demonstrado na ultima seção, concluir que o ele é de alguma maneira mais "poderoso" que o bipartite.

No capítulo 5 usarei a ideia de complexidade de comunicação para quantificar os bits de informação que duas partes precisam trocar para realizar uma tarefa em comum. Os casos em que o emaranhamento quântico prévio reduz a complexidade de comunicação será discutido. Ao final vou demonstrar que, caso as partes tenham acesso a uma não-localidade equivalente a das caixas Popescu-Rohrlich, toda função decisão pode ser avaliada com a troca de 1 bit de informação.

Capítulo 1

Mecânica quântica: teoria de informação

1.1 Teoria da informação

"Everything is information"
John Wheeler

Preocupado em quantificar e transmitir informação, Claude Shannon publica em 1948 o famoso *"A Mathematical Theory of Communication"* [2]. Assim nasce a teoria da informação, que além de aplicações diretas em áreas como criptografia, compressão de dados[1] e inferência estatística, é útil como ferramenta para física teórica.

O coração da teoria da informação está na definição de entropia, uma função que mede a incerteza de uma variável aleatória e captura a nossa intuição de quantidade de informação. Uma maneira natural de introduzir a função entropia é buscar antes uma função $I : (0, 1] \to \mathbb{R}$ que satisfaça as seguintes condições:

- A informação de um evento x deve depender apenas de sua probabilidade p_x.
- A função I deve ser contínua.
- A função I deve ser aditiva, *i.e.*: $I(p_x p_y) = I(p_x) + I(p_y)$. Assim, a informação de eventos independentes ($p_{xy} = p_x p_y$) é a soma da informação dos eventos individuais.

Condições que implicam que a informação de um evento x deve ser, a menos de uma transformação linear, $I(x) = \log p_x$ [3].

Como no exemplo de [3], chover na Floresta Amazônica e nevar na Sibéria são eventos associados a pouca informação. Mas, nevar na Floresta Amazônica é um evento muito mais significante, e contém muita informação[2].

[1] Isto inclui os famosos algoritmos ZIP (compressão sem perda de dados) e MP3 (compressão com perda de dados).

[2] Vale notar que eventos de probabilidade 0 teriam informação infinita, mas no caso de espaço amostral finito eles nunca vão acontecer, portanto não representam problemas.

A função I nos motiva definir a entropia de uma variável aleatória X como:

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x),$$

onde a escolha da base 2 para o logaritmo é justificada pela definição de bit, que é a quantidade máxima de informação que pode ser armazenada em um sistema físico de dois estados distintos[3]

Em teoria de informação, a palavra bit também é usada com outro sentido, chamamos de bit uma variável aleatória que pode assumir os valores do conjunto $\{0, 1\}$. Sempre que não for causar problemas de compreensão, a palavra bit é usada sem especificar exatamente qual seu significado.

O leitor pode buscar uma introdução em teoria da informação em [5], no capítulo 1 de [3] ou no capítulo 11 de [6].

1.2 Álgebra linear em notação de Dirac

Os postulados da mecânica quântica são enunciados com o auxílio da álgebra linear e, para alguns sistemas, a análise funcional. Nesta monografia vamos nos preocupar apenas com sistemas de dimensão finita, exigindo do leitor alguma familiaridade com álgebra linear.

Existem muitos bons livros com uma introdução mais completa do que a que será apresentada. O capítulo 2 do livro *Quantum Information and Quantum Computation* [6] de M. Nilsen e I. Chuang é suficiente para cobrir todos os pré-requisitos de álgebra linear para informação quântica. Uma boa alternativa é buscar a ref. [7], que também é voltado para informação quântica. Além disso, temos o livro de Asher Peres [8] que se preocupa mais com conceitos, o clássico *Quantum Mechanics* [9], que é visto como uma bíblia por muitos estudantes de física e *Noções de Informação Quântica* [10] que possui uma abordagem mais matemática.

No livro *The principles of quantum mechanics* [11], Paul Dirac introduziu uma notação bastante útil para a quântica, ou mesmo para álgebra linear. Segue um pequeno resumo.

Os elementos de um espaço vetorial $\mathcal{V}$ são escritos como $|v\rangle$. No caso desse espaço ser completo e possuir produto interno (ou seja, ser um espaço de Hilbert), os funcionais lineares limitados podem ser entendidos como projeção em algum vetor[4]. Logo, é interessante escrever os elementos do espaço dual $\mathcal{V}^*$ como $\langle v|$, que quando aplicados em $|u\rangle \in \mathcal{V}$ são entendidos como "realizar o produto interno $(|u\rangle, |v\rangle)$".

Com a notação de Dirac fica bem simples entender a ação de um operador escrito da forma $|a\rangle\langle b|$ no vetor $|c\rangle$. Temos o vetor $|a\rangle$ multiplicado pelo produto interno $(|b\rangle, |c\rangle)$, $|a\rangle\langle b||c\rangle$, sendo essa "associatividade" a principal vantagem da notação.

[3] Em 1936 Vannevar Bush usou o termo *"bits of information"* para tratar das marcas dos cartões perfurados [4].

[4] Em análise funcional, esta interpretação é permitida pelo lema de Riesz [12], que enuncia: Para todo $f : \mathcal{H} \to \mathbb{C}$ existe um único $y_f \in \mathcal{H}$ tal que $f(x) = (y_f, x)$ para todo $x \in \mathcal{H}$. Vale lembrar que no nosso caso (dimensão finita) espaços vetoriais com produto interno são sempre completos, e interpretar funcionais lineares como projeções é simples.

Como é comum na literatura, sempre que houver um produto interno $(|a\rangle,|b\rangle)$, vamos simplesmente escrever $\langle a|b\rangle$.

1.3 Regras da mecânica quântica

> *"Over the years, the mathematics of quantum mechanics has become more abstract and, consequently, simpler."*
>
> V. S. Varadarajan

Nesta seção serão apresentados os postulados que formam a mecânica quântica. Vamos assumir uma postura bastante operacional: enuncia-los e trata-los como regras de um jogo.

Postulado 1. *Todo sistema isolado está associado a um espaço vetorial complexo munido de produto interno*[5] $\mathcal{H}$*, chamado de espaço de estados. O sistema é completamente descrito por um vetor normalizado que pertence ao espaço de estados, chamado de estado.*

Postulado 2. *Sempre podemos transformar um estado $|\psi\rangle$ em um novo estado $|\psi'\rangle = U|\psi\rangle$, desde que U seja um operador unitário*[6]*.*

Postulado 3. *As medições são descritas por uma coleção de operadores de medição $\{M_m\}$ que agem no espaço do sistema a ser medido e satisfazem a relação de completeza:* [7]

$$\sum_m M_m^\dagger M_m = I.$$

O índice m se refere ao valor que será lido após a medição.

A probabilidade de obter obter o resultado m dado um certo estado $|\psi\rangle$ é:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle.$$

Após a medição o sistema passa a ser descrito por:

$$|\psi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}.$$

Postulado 4. *O espaço de estados de um sistema composto por duas partes A e B é gerado pelo produto tensorial dos espaços de estados individuais, $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.*

Um caso especial de medição, simples porém importante, é o de medição projetiva, que é o caso em que operadores de medição $\{M_m\}$ são projetores. Assim podemos definir um observável.

[5] Logo, um espaço de Hilbert. E vamos usar a convenção do produto interno ser anti-linear na primeira componente e linear na segunda.

[6] Um operador U é chamado de unitário se $UU^\dagger = U^\dagger U = I$, e segue direto que U preserva produtos internos, *i.e.*, $(U|a\rangle,U|b\rangle) = (|a\rangle,|b\rangle)$.

[7] $M_m^\dagger$ representa o adjunto de M_m.

Definição 1. *Um observável M é um operador auto-adjunto, que pelo teorema da decomposição espectral pode ser escrito na forma $M = \sum_m \lambda_m |\psi_m\rangle\langle\psi_m|$, com $\sum_m |\psi_m\rangle\langle\psi_m| = I$, sendo $|\psi_m\rangle\langle\psi_m|$ o projetor associado ao autovalor λ_m. Usamos então $\{|\psi_m\rangle\langle\psi_m|\}$ como os operadores de medição.*

O valor da medição projetiva se dá devido ao fato de podermos associar um operador auto adjunto a um observável físico, facilitando a interpretação física.

Um resultado conhecido como teorema de Neumark[8] nos garante que todas medições possíveis de um sistema quântico podem ser feitas com um sistema auxiliar, operações unitárias e medição projetiva. Assim, percebemos que não se perde muito ao restringir nosso mundo apenas a observáveis.

1.4 Comentários sobre o produto tensorial

Como o produto tensorial será bastante usado durante todo o trabalho e geralmente não é apresentado em cursos introdutórios de álgebra linear, é válido dedicar uma seção a ele. Vamos apresentar as propriedades do produto tensorial como feito na ref. [10].

Definição 2. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais complexos, $|v\rangle \in \mathcal{V}$ e $|w\rangle \in \mathcal{W}$. Criamos um novo elemento $|v\rangle \otimes |w\rangle$, chamado produto tensorial de $|v\rangle$ com $|w\rangle$. O produto tensorial dos espaços vetoriais $\mathcal{V}$ e $\mathcal{W}$, denotado $\mathcal{V} \otimes \mathcal{W}$, será o espaço vetorial gerado pelos vetores da forma $|v\rangle \otimes |w\rangle$, sujeito às relações*

1. $(\lambda|v\rangle) \otimes |w\rangle = \lambda(|v\rangle \otimes |w\rangle) = |v\rangle \otimes (\lambda|w\rangle)$;
2. $(|u\rangle + |v\rangle) \otimes |w\rangle = |u\rangle \otimes |w\rangle + |v\rangle \otimes |w\rangle$;
3. $|v\rangle \otimes (|w\rangle + |z\rangle) = |v\rangle \otimes |w\rangle + |v\rangle \otimes |z\rangle$,

para todos $|u\rangle$,$|v\rangle \in \mathcal{V}$ e $|w\rangle$,$|z\rangle \in \mathcal{W}$.

Definição 3. *Considere agora que $\mathcal{V}$ e $\mathcal{W}$ possuem produto interno. Para $|u\rangle$,$|v\rangle \in \mathcal{V}$ e $|w\rangle$,$|z\rangle \in \mathcal{W}$, define-se o produto interno $\mathcal{V} \otimes \mathcal{W}$ por*

$$(\langle u| \otimes \langle z|)(|v\rangle \otimes |w\rangle) = \langle u|v\rangle\langle z|w\rangle.$$

Para tratar dos operadores de $\mathcal{V}$ e $\mathcal{W}$ agindo em elementos de $\mathcal{V} \otimes \mathcal{W}$, usamos o produto de Kronecker.

Definição 4. *Seja $A : \mathcal{V} \to \mathcal{V}$ e $B : \mathcal{W} \to \mathcal{W}$, define-se $A \otimes B$ como*

$$(A \otimes B)|v\rangle \otimes |w\rangle \equiv A|v\rangle \otimes B|w\rangle.$$

Dois conceitos ligados ao produto tensorial que vamos utilizar são os de operação local e medição local.

[8] O trabalho original de Neumark [13] não se preocupa com estados quânticos e medições, e prova na verdade um teorema mais forte. Para uma demonstração com os olhos da informação quântica, ver pg. 84 de [14] ou pg. 285 de [8].

Definição 5. *Seja $A : \mathcal{V} \to \mathcal{V}$ e $B : \mathcal{W} \to \mathcal{W}$. Operações da forma $A \otimes B$ são chamadas de operações locais.*[9]

Medições locais são medições feitas a partir dos operadores com a forma $M_i \otimes M_j$.

Na definição acima, usamos um espaço vetorial que é escrito como $\mathcal{V} \otimes \mathcal{W}$. Mas repare que podemos ter $\mathcal{W} = \mathcal{E} \otimes \mathcal{F}$. Estados que são escritos como vetores de $\mathcal{V} \otimes \mathcal{W}$ são chamados estados bipartites. No caso de mais partes (como em $\mathcal{V} \otimes \mathcal{E} \otimes \mathcal{F}$), falamos que é um estado multipartite.

Apesar da notação mais precisa para o produto tensorial de dois vetores ser $|v\rangle \otimes |w\rangle$, ela facilmente se torna pesada. Há duas outras notações bastante utilizadas, que são boas sempre que não oferecem riscos de má compreensão:

$$|v\rangle \otimes |w\rangle \equiv |v\rangle|w\rangle \equiv |vw\rangle.$$

1.5 Informação quântica

"Information is physical"

Rolf Landauer

O ramo que ficou conhecido como Teoria Quântica da Informação consiste em impor as regras da mecânica quântica nos conceitos de teoria da informação. Assim, podemos estudar toda mecânica quântica sem depender de um sistema físico, nos ajudando a conhecer mais sobre seus fundamentos e particularidades.

A idéia principal é perceber que um estado quântico pode ser entendido como um pacote de informação, sendo informação que retiramos do sistema dada pela medição. Para facilitar uma analogia com a teoria clássica, vamos definir os bits quânticos.

Definição 6 (Qubit)**.** *O qubit é um estado quântico que pertence a um espaço de estados de dimensão 2.*

É comum em teoria da informação quântica que todos os qubits sejam escritos na base ortonormal $\{|0\rangle,|1\rangle\}$. Uma medição bastante natural para qubits é feita com os operadores $M_0 = |0\rangle\langle 0|$ e $M_1 = |1\rangle\langle 1|$, processo que, devido a sua ligação com informação clássica, é conhecido como medir na base computacional.

1.6 Exemplos de evolução unitária

Vamos agora ilustrar a notação de Dirac e o postulado da evolução de sistemas quânticos definindo alguns operadores que são encontrados nos trabalhos de informação quântica. Eles também serão utilizados ao decorrer desta monografia.

Seja $\mathcal{H}_2$ o espaço vetorial gerado pela base ortonormal $\{|0\rangle,|1\rangle\}$, os operadores abaixo são da forma $\mathcal{H}_2 \to \mathcal{H}_2$, com exceção do operador $cNOT$ que leva elementos de $\mathcal{H}_2 \otimes \mathcal{H}_2$ nele mesmo.

[9] Podemos entender as operações locais como a aplicação das extensões triviais de A e B, *i.e.*, $A \otimes I$ e $I \otimes B$. Já que $(A \otimes I)(B \otimes I) = (B \otimes I)(A \otimes I)$.

- $X \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$;
- $Y \equiv i|1\rangle\langle 0| - i|0\rangle\langle 1|$;
- $Z \equiv |0\rangle\langle 0| - |1\rangle\langle 1|$;
- $H \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$;
- $phase(\phi) \equiv |0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|$;
- $\mathbf{n} \cdot \sigma \equiv n_x X + n_y Y + n_z Z, \quad \text{com } n_i \in \mathbb{R} \text{ e } n_x^2 + n_y^2 + n_z^2 = 1$;
- $cNOT \equiv |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$.

Alguns comentários interessantes:

- Os letras X,Y e Z surgiram da teoria de spin $1/2$ na física, onde cada letra representa uma direção do espaço.
- A notação $\mathbf{n} \cdot \sigma$ pode ser entendida como um "produto interno" entre um vetor normalizado em $\mathbb{R}^3$ e um vetor com os operadores X, Y, Z. $\mathbf{n} \cdot \sigma$ representa todos os operadores hermitianos unitários de traço zero que levam $\mathcal{H}_2$ em $\mathcal{H}_2$.
- O operador X também é muito conhecido como porta NOT devido ao fato de possuir um análogo clássico que consiste em "negar"o bit. Note que $X|0\rangle = |1\rangle$, e $X|1\rangle = |0\rangle$.
- A operação $cNOT$ devido ao termo em inglês *Controlled Not*. Note que, na base $\{|0\rangle,|1\rangle\}$ o primeiro qubit nunca é modificado. No caso dele ser ser $|0\rangle$, o segundo qubit continua em seu estado. No caso do primeiro ser $|1\rangle$, o segundo é negado.
- O operador H é usado para indicar as diferenças fundamentais do bit para o qubit, já que ele leva os qubits $|0\rangle$ e $|1\rangle$ em combinação linear dos mesmos. É interessante notar que o operador H faz a mudança da base Z ($\{|0\rangle,|1\rangle\}$) para a base X, que é normalmente escrita como $\{|+\rangle,|-\rangle\}$.

1.7 Emaranhamento

"Hilbert space is a big place"

Carlton Caves

Como afirmado no quarto postulado, o espaço de estados que descreve a união de dois sistemas é o produto tensorial dos espaços individuais. Esse novo espaço vetorial "esconde"estados com propriedades interessantes. Poderíamos imaginar que espaços da forma $\mathcal{V} \otimes \mathcal{W}$ contêm apenas vetores da forma $|v\rangle \otimes |w\rangle$. Mas uma análise mais profunda mostra que o conjunto de vetores desta forma é desprezível se comparado ao conjunto de todos os vetores de $\mathcal{V} \otimes \mathcal{W}$.[10]

[10] Ver capítulo 1.3.1 de [10].

Definição 7. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais que descrevem um sistema quântico de forma que o sistema todo é descrito por $\mathcal{V} \otimes \mathcal{W}$. Estados que podem ser escritos como $|\psi\rangle = |v\rangle \otimes |w\rangle$, com $|v\rangle \in \mathcal{V}$ e $|w\rangle \in \mathcal{W}$ são chamados de estados fatoráveis.*

Definição 8. *Estados não-fatoráveis são estados emaranhados.*

Veremos neste trabalho que muitos resultados importantes da mecânica quântica são consequência direta do emaranhamento. Para ilustrar estes estados emaranhados, vamos apresentar os chamados pares de Bell:

$$|\phi^+\rangle \equiv |\beta_{00}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\phi^-\rangle \equiv |\beta_{01}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\psi^+\rangle \equiv |\beta_{10}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\psi^-\rangle \equiv |\beta_{11}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Teorema 1. *Todos os pares de Bell são estados emaranhados.*

Demonstração. Vamos demonstrar o teorema para apenas um dos quatro pares de Bell, já que para os outros três a demonstração é totalmente análoga.

Suponha que o estado $|\beta_{00}\rangle$ possa ser escrito como

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle),$$

com $\alpha, \beta, \gamma, \delta \in \mathbb{C}$. Então temos a igualdade:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle.$$

A ortogonalidade dos vetores $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ nos impõe as condições:

$$\alpha\gamma = \frac{1}{\sqrt{2}}, \qquad \alpha\delta = 0;$$
$$\beta\gamma = 0, \qquad \beta\delta = \frac{1}{\sqrt{2}},$$

que não podem ser satisfeitas simultaneamente. □

Vamos apresentar uma receita para gerar pares de Bell a partir do estado $|00\rangle$ utilizando os operadores X, H e $cNOT$. É simples verificar que

$$|\beta_{ab}\rangle = (cNOT)(H \otimes I)(X^a \otimes X^b)|00\rangle.$$

Repare que $cNOT$ não é uma operação local, e é exatamente por isso que conseguimos levar um estado separável em um emaranhado. Segue da definição que operações locais não podem emaranhar estados.

Essa discussão tem papel fundamental na quantificação de emaranhamento, que consiste em buscar uma função[11] $E : \mathcal{V} \otimes \mathcal{W} \to \mathbb{R}_+$ que não cresça se suas partes têm direito a apenas operações locais e comunicação clássica[12].

[11] Vale ressaltar que este não é o caso geral. Existe emaranhamento multipartite, que ocorre quando escrevemos nosso espaço vetorial como produto tensorial de mais de duas partes.

[12] Condição conhecida como LOCC, do inglês *Local Operations and Classic Communication*.

Na seção 1.9 vamos exibir um quantificador para o caso especial de estados puros e bipartites, e no capítulo 2 veremos uma aplicação dos quantificadores.

Em [15], Vedral *et al.* propõem uma abordagem axiomática para quantificar emaranhamento, explicitando as propriedades que devemos exigir da função E. Para uma introdução, o leitor pode buscar o capítulo XV de [16] ou o capítulo 4 de [17].

1.8 Limitações da descrição por estados puros

Como podemos tratar um estado quântico com uma incerteza clássica? Isto é, se uma fonte gera com probabilidade p_a o estado $|a\rangle$, e com probabilidade p_b o estado $|b\rangle$. Qual é a melhor descrição para um estado gerado por esta fonte?

Se um físico experimental faz uma medição na base computacional no estado $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, mas por algum motivo não tem acesso ao resultado da medição. Como ele pode descrever o sistema pós-medição?

Podemos escrever $\{(p_i, |\psi_i\rangle)\}$ para representar um sistema que está no estado $|\psi_i\rangle$ com probabilidade p_i, e aplicar os postulados que foram apresentados na seção 1.3 em cada estado individual. Esta descrição não possui problema algum, mas existe uma ferramenta bem mais prática para tratar de sistemas desta forma, os *operadores densidade*.

Definimos operador densidade como[13,14]:

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

o caso particular em que $\rho = |\psi\rangle\langle\psi|$ é chamado de estado puro[15], e todos estados não-puros são chamados de estados mistos.

Vamos escrever o espaço vetorial dos operadores densidade que contém os estados puros de $\mathcal{H}$ como $\mathcal{HS}$. Pode-se agora verificar que após o sistema ρ sofrer a ação do operador unitário U vamos ter

$$\rho' = U\rho U^\dagger,$$

as probabilidades dos resultados das medições feitas com o conjunto $\{M_m\}$ são calculadas com o traço

$$p(m) = \mathrm{Tr}\,(M_m \rho M_m^\dagger),$$

e após a medição o sistema passa a ser descrito por

$$\rho_m = \frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m \rho)}.$$

[13] Perceba também, que escrito como operador densidade, perdemos a fase global do estado, *i.e.*, $e^{i\phi}|\psi\rangle$ e $|\psi\rangle$ são representados pelo mesmo operador. Se olharmos para o postulado da medição, vamos concluir que, de fato, as probabilidades de obter um dado resultado independem da fase global.

[14] De maneira alternativa, e menos intuitiva, podemos definir o operador densidade como um operador positivo semidefinido de traço 1.

[15] Perceba que estamos simplesmente fazendo combinação convexa dos estados quânticos, e a definição de estado puro coincide com a definição de ponto puro.

Uma grande vantagem do formalismo de operadores densidade é a facilidade para tratar de uma parte isolada de um sistema composto. Tome um espaço vetorial da forma $\mathcal{HS}_A \otimes \mathcal{HS}_B$ e um sistema deste espaço descrito por ρ_{AB}. Existe uma maneira de atribuir um estado ρ_A para descrever as medições locais ($\{M_m \otimes I\}$) feitas em A, *i.e.*:

$$p(m) = \mathrm{Tr}\left(M_m \rho_A M_m^\dagger\right) = \mathrm{Tr}\left(M_m^\dagger M_m \otimes I \rho_{AB}\right).$$

Basta usarmos o traço parcial[16] em B, mapa definido como o traço no espaço $\mathcal{HS}_B$:

$$\mathrm{Tr}_B : \mathcal{HS}_A \otimes \mathcal{HS}_B \to \mathcal{HS}_A, \mathrm{Tr}_B = I \otimes \mathrm{Tr}\,.$$

Pode-se verificar que para estados fatoráveis vamos ter $\mathrm{Tr}_B\left(\rho_A \otimes \rho_B\right) = \rho_A$. E para estados emaranhados? O formalismo de operador densidade nos permite descrever o estado das partes A e B separadamente?

A resposta é sim, o traço parcial é um mapa válido para todo elemento de $\mathcal{HS}_A \otimes \mathcal{HS}_B$. Vamos calcular o traço parcial de um par de Bell e descrever isoladamente o sistema da parte A.

$$\begin{aligned}
\mathrm{Tr}_B\left(|\beta_{00}\rangle\langle\beta_{00}|\right) &= \frac{1}{2}\mathrm{Tr}_B\left((|00\rangle + |11\rangle)(\langle 00| + \langle 11|)\right) \\
&= \frac{1}{2}\mathrm{Tr}_B\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right) \\
&= \frac{1}{2}(|0\rangle\langle 0|\,\mathrm{Tr}\left(|0\rangle\langle 0|\right) + |0\rangle\langle 1|\,\mathrm{Tr}\left(|0\rangle\langle 1|\right) + \\
&\qquad |1\rangle\langle 0|\,\mathrm{Tr}\left(|1\rangle\langle 0|\right) + |1\rangle\langle 1|\,\mathrm{Tr}\left(|1\rangle\langle 1|\right)) \\
&= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \\
&= \frac{1}{2}I.
\end{aligned}$$

Assim, a melhor descrição local da parte A do sistema é a identidade, e este resultado vale para todos os estados maximamente emaranhados (ver seção 1.9). Que é um resultado totalmente plausível, não poderíamos imaginar que usar um formalismo diferente nos permitisse dizer mais sobre as probabilidades locais de um estado.

Apesar dos operadores densidade serem uma ferramenta poderosa para a mecânica quântica, sua notação as vezes é desnecessária, e pode nos tirar a intuição do que está acontecendo. Vamos sempre que possível usar a notação de estados puros, *i.e.*, escrever os estados quânticos como $|\psi\rangle$.

1.9 Decomposição de Schmidt

A decomposição de Schmidt [18, 19] é uma ferramenta muito útil para descrever sistemas bipartites, e pode ser usada para detectar e quantificar emaranhamento.

[16] Para entender porque o traço parcial, ver Box 2.6 de [6] ou siga o exercício 39 de [10].

Teorema 2 (Decomposição de Schmidt). *Seja* $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, $|\psi\rangle$ *pode ser escrito como* $\sum_i^d \lambda_i |i_A\rangle|i_B\rangle$, *onde* λ_i *são números reais positivos únicos (a menos de uma re-ordenação), os conjuntos* $\{|i_A\rangle\}$, $\{|i_B\rangle\}$ *formam uma base ortonormal para os espaços* $\mathcal{H}_A$ *e* $\mathcal{H}_B$ *e* $d = \min(\dim \mathcal{H}_A, \dim \mathcal{H}_B)$[17] .

Demonstração. Vamos escrever $|\psi\rangle = \sum_{jk} a_{jk}|j\rangle|k\rangle$, com os vetores $\{|j\rangle\}$ e $\{|k\rangle\}$ ortogonais entre si.

Seja A uma matriz que tenha os valores a_{jk}. Pelo teorema da decomposição em valores singulares [20], existem matrizes que representam transformações unitárias $U : \mathcal{H}_A \to \mathcal{H}_A$ e $V : \mathcal{H}_B \to \mathcal{H}_B$ tal que $A = U\Lambda V^\dagger$, onde Λ é uma matriz diagonal j por k com números reais únicos e não-negativos, com d parâmetros complexos.

Basta agora usar os valores λ_i de Λ, e tomar $|i_A\rangle = U|j\rangle$, $|i_B\rangle = V^\dagger|k\rangle$. □

Podemos agora utilizar os λ_i para definir a função entropia de Schmidt:

$$E : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathbb{R}^+, \quad E(|\psi_{AB}\rangle) = -\sum_i \lambda_i^2 \log(\lambda_i^2).$$

A condição de estado quântico exige que $\sum_i \lambda_i^2 = 1$, então fica fácil notar que estados com apenas um coeficiente λ_1 são fatoráveis e possuem $E = 0$. E um estado está emaranhado se e somente se tem mais de um coeficiente λ, e portanto $E > 0$.

Note que E é contínua, invariante a transformações unitárias locais (*i.e.*, operações da forma $U_A \otimes U_B$) e que $E(|\psi_{AB}\rangle \otimes |\phi_{AB}\rangle) = E(|\psi_{AB}\rangle) + E(|\phi_{AB}\rangle)$.

E é uma boa medida para o emaranhamento. Se percebemos que as condições acima são exatamente as condições que exigimos da função entropia, pode-se mostrar que a função E é, a menos de uma transformação afim, única [21, 22].

Vale ressaltar alguns detalhes:

- O valor máximo da função entropia de Schmidt é 1. Assim, para sistemas bipartites, podemos definir estado maximamente emaranhado, e verificar que todos os pares de Bell satisfazem possuem $E = 1$.
- Embora o teorema de Schmidt não possa ser estendido para o caso de sistemas multipartites, existe uma ideia parecida para o caso de 3 qubits [23].
- Os vetores $|i_A\rangle$ e $|i_B\rangle$ não são únicos, para um caso simples e interessante veja o singleto (seção 3.2).
- Repare que o traço parcial em B de um sistema escrito na forma de Schmidt é simplesmente $\rho_A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$. Vendo assim, podemos sempre purificar um estado ρ. Isto é, um estado misto sempre pode ser visto como o traço parcial um estado puro num sistema maior, basta escolher uma base ortonormal $\{|i_B\rangle\}$ e escrever $|\psi_{AB}\rangle = \sum_i \lambda_i |i_a\rangle|i_b\rangle$.

[17] Onde a dimensão aqui é entendida como o número de vetores linearmente independetes de $\mathcal{H}$.

Capítulo 2

Comunicação via qubits

Este capítulo irá tratar de resultados importantes que envolvem informação quântica. Eles serão úteis para compreender os fundamentos da mecânica quântica, a diferença dos bits clássicos para os qubits e o poder do emaranhamento.

2.1 Teorema da não-clonagem

Apesar de bastante simples, o teorema da não-clonagem foi reconhecido pela primeira vez apenas em 1982 [24][1], indicando que entender mecânica quântica como teoria de informação contribui para que resultados fundamentais apareçam naturalmente.

A história de como o teorema veio a ser publicado é curiosa, pois ele foi uma resposta (errada) ao FLASH(*first light amplification superluminal hookup*), um protocolo (errado) para troca de informação com velocidade arbitrária. [26]

Teorema 3. *Não existe um processo que faz cópias de um estado quântico arbitrário.*

Demonstração. Suponha exista um operador unitário C com a seguinte propriedade:

$$C(|\psi\rangle|x\rangle) = |\psi\rangle|\psi\rangle,\ \forall|\psi\rangle \in \mathcal{H}. \tag{2.1}$$

Assim, $|\psi\rangle$ é que desejamos clonar, e $|x\rangle$ é um estado que vai assumir as propriedades de $|\psi\rangle$. Podemos entender $|x\rangle$ como uma folha em branco, que se transforma no estado $|\psi\rangle$.

Como C deve valer para todo estado de $\mathcal{H}$,

$$C(|\phi\rangle|x\rangle) = |\phi\rangle|\phi\rangle,$$

assim temos

$$(\langle\phi|\langle x|)C^\dagger = \langle\phi|\langle\phi|.$$

Podemos aplicar este funcional algum $|\psi\rangle$,

$$(\langle\phi|\langle x|)C^\dagger C(|\psi\rangle|x\rangle) = \langle\phi|\langle\phi||\psi\rangle|\psi\rangle.$$

[1] Na década de 1930 a mecânica quântica já tinha sua base matemática bem fundamentada em livros como o de Paul Dirac [11] e von Neuman [25]

Usando o fato de C ser unitário e $\langle x|x\rangle = 1$,

$$\langle \phi|\psi\rangle = \langle \phi|\psi\rangle^2.$$

Como $\langle \phi|\psi\rangle \in \mathbb{C}$, equação é satisfeita apenas em duas situações:

$$\langle \phi|\psi\rangle = 0 \quad \text{e} \quad \langle \phi|\psi\rangle = 1, \quad \phi \in \mathbb{R}.$$

Ou seja, o operador C só pode copiar $|\phi\rangle$ e estados ortogonais a ele. □

Se tomarmos o caso especial do sistema de dois níveis, os estados são qubits. Vemos que só podemos clonar qubits ortogonais, ou seja, se mapearmos os bits clássicos nos qubits ortogonais $|0\rangle$ e $|1\rangle$ a cópia é permitida, indicando que o bit é realmente um caso particular de qubit.

Algumas consequências do teorema da não-clonagem:

- Os métodos mais comuns de correção de erro utilizados em informação clássica dependem do fato de poder criar várias cópias de um mesmo bit. Logo não podem ser utilizados para a informação quântica[2].
- A não-clonagem impede um espião de ter cópias da informação trocada por duas partes, fato que garante a segurança do BB84 [28], um protocolo de distribuição quântica de chaves criptográficas.
- Wiesner propõem em [29] a noção de um dinheiro quântico, à prova de falsificações. Para isso devemos, além de marcar cada nota com um número de série, colocar vários qubits, nos quais apenas o banco sabe os estados. Vale notar que a noção de dinheiro e assinatura digital existe independente da mecânica quântica. Para uma discussão amigável, veja [30].
- No capítulo 3 veremos o conceito de localidade e não-sinalização. Um resultado muito interessante é que o teorema da não clonagem é válido para toda teoria não-local que respeita a condição de não-sinalização [31].
- Como veremos na seção 2.2, estados quânticos arbitrários não podem ser perfeitamente discriminados. O teorema da não-clonagem está relacionado com a discriminação dos estados quânticos. No caso de estados ortogonais, podemos clonar e discriminar, e pode-se demonstrar que um protocolo de clonagem implicaria num protocolo para discriminar estados, *vice versa*.

2.2 Discriminação de estados quânticos

Na informação clássica, não existem problemas para discriminar estados diferentes, *i.e.*, eles sempre podem ser discriminados via medição. Medir o bit 0 nos retorna o valor 0, medir o bit 1 nos retorna 1. Com mecânica quântica

[2] Apesar de isto não ser o fim do mundo, existe correção de erro quântica. Uma introdução pode ser encontrada em [27] ou no capítulo 10 do livro de Nilsen e Chuang [6].

a situação não é tão simples assim. Vamos introduzir o assunto com um experimento mental.

Alice tem duas caixas: a caixa a, onde ela guarda o qubit $|a\rangle = |0\rangle$, e a caixa b, onde ela guarda $|b\rangle = |1\rangle$. Eve sabe que Alice guarda o qubit $|a\rangle$ na caixa a e $|b\rangle$ na caixa b, mas não sabe qual caixa é qual. Seria possível Eve identificar as caixas?

A resposta é sim. Basta ela medir os qubits na base computacional. Se Eve ler 0, com certeza ela mediu a caixa a. Caso ela leia 1, com certeza ela mediu a caixa b.

Imagine uma situação similar, com a única diferença que Alice guarda os qubits $|a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|b\rangle = |1\rangle$. Note que medir na base computacional pode não ser suficiente para resolver o problema. Se Eve obtém 0, ela mediu o qubit da caixa a, mas se Eve obtém 1 ela pode ter medido a caixa a ou a b.

Os operadores[3] $M_0 = |a_\perp\rangle\langle a_\perp|$ e $M_1 = |b_\perp\rangle\langle b_\perp|$ são capazes de discriminas os estados $|a\rangle$ e $|b\rangle$. Mas repare, $M_0M_0^\dagger + M_1M_1^\dagger \neq I$, implica que eles não formam um conjunto de operadores de medição válido.

Teorema 4. *Estados não-ortogonais não podem ser discriminados com apenas uma medição.*

Demonstração. A demonstração deste teorema pode ser vista como um corolário do limite de Helstrom, que será apresentada no fim da seção. □

Vamos exibir 3 protocolos para discriminar um estado $|a\rangle$ de um $|b\rangle$, sendo cada um dos três ótimo em uma dada situação e, no caso de $\langle a|b\rangle = 0$, são equivalentes.

Eve pode usar os operadores $M_a = |a\rangle\langle a|$ e $M_{a_\perp} = I - |a\rangle\langle a|$, desta forma, sempre que eve medir $a_\perp$, ela sabe que estava com $|b\rangle$, mas medir a não garante que ela tinha o estado $|a\rangle$.

Eve pode usar $M_a = \lambda|b_\perp\rangle\langle b_\perp|$, $M_b = \lambda|a_\perp\rangle\langle a_\perp|$ e $M_c = I - M_a - M_b$.[4] Desta forma, obter a implica em ter com certeza $|a\rangle$, b implica em $|b\rangle$ e se Eve obtém c, a situação é indeterminada.

Caso Eve queira uma medição que não tenha preferência sobre a ou b e retorne apenas duas saídas, podemos estabelecer uma cota para sua probabilidade de sucesso máxima. Esta cota é conhecida como limite de Helstrom [32].

Queremos operadores M_a e M_b que acertem qual estado é qual sem preferência sobre algum dado estado e que também satisfaça a condição de operadores de medição. Com isso calculamos a probabilidade de sucesso média, assumindo que, *a priori*, $|a\rangle$ e $|b\rangle$ são equiprováveis.

$$p_s = \frac{1}{2}(\langle a|M_a|a\rangle + \langle b|M_b|b\rangle).$$

[3] Onde $|\psi_\perp\rangle$ é um estado ortogonal a $|\psi\rangle$.

[4] Na verdade desejamos maximizar o λ para termos mais chances de obter a ou b, fazendo as contas encontramos $\lambda = 1 + \langle a|b\rangle$.

A relação de completude dos operadores de medição nos permite escrever

$$\begin{aligned} p_s &= \frac{1}{2}(\langle a|M_a|a\rangle + \langle b|(I - M_a)|b\rangle) \\ &= \frac{1}{2}(1 + \mathrm{Tr}\,(M_a(|a\rangle\langle a| - |b\rangle\langle b|))). \end{aligned}$$

O truque agora é maximizar o traço de $M_a\Gamma$, com $\Gamma = |a\rangle\langle a| - |b\rangle\langle b|$. Para isso, devemos encontrar os autovetores de Γ, sendo M_a uma projeção no autovetor com o maior autovalor de Γ. Como os autovalores de Γ são $\pm\sqrt{1 - |\langle a|b\rangle|^2}$,[5] a probabilidade máxima de sucesso é:

$$p_s^{max} = \frac{1}{2}(\pm\sqrt{1 - |\langle a|b\rangle|^2}).$$

2.3 Teorema de Holevo

Até agora ainda não fizemos uma conexão direta entre informação clássica e a informação quântica. Como podemos mapear informação clássica em estados quânticos?

Mapear bits em qubits é fácil, basta associar os bits 0 e 1 nos estados $|0\rangle$ e $|1\rangle$. Perceba que a ortogonalidade dos vetores $|0\rangle, |1\rangle$ tem um papel fundamental. Se o mapeamento $0 \to |0\rangle$ e $1 \to |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ for feito, teremos problemas para recuperar a informação, já que $\langle 0|+\rangle = 1/\sqrt{2} \neq 0$, eles não podem ser perfeitamente discriminados (ver seção 2.2).

A pergunta então é: Quantos bits de informação podemos codificar em um qubit? Ou de maneira mais geral, se Alice quer transmitir para Bob a informação de uma variável aleatória X, e pretende fazer isto usando um estado quântico, qual a ligação entre os resultados Y das medições feitas no estado enviado e variável aleatória X? O *teorema de Holevo* impõe uma cota sobre as correlações de X e Y. Para entender este teorema, vamos antes apresentar duas definições.

Definição 9. *A informação mútua entre duas variáveis aleatórias X e Y é dada por:*

$$H(X : Y) = H(X) + H(Y) - H(X,Y).$$

A informação mútua captura a ideia de quão correlacionadas estão as distribuições das variáveis X e Y. Perceba que $H(X : X) = H(X)$, e podemos usar a aditividade da entropia para mostrar que X e Y são independentes se e somente se $H(X : Y) = 0$.

Definição 10. *A entropia de um estado quântico ρ é definida como:*

$$S(\rho) = -\sum_i p_i \log_2 p_i,$$

onde p_i são os autovalores do operador ρ.

[5] Para encontrar os autovalores basta escrever $|a\rangle$ como $\begin{bmatrix}1\\0\end{bmatrix}$ e $|b\rangle$ como $\begin{bmatrix}\alpha\\\beta\end{bmatrix}$ e calcular os autovalores da matriz $\begin{bmatrix}|\alpha|^2 - 1 & \alpha^*\beta\\ \alpha\beta^* & |\beta|^2\end{bmatrix}$.

A entropia de um estado quântico mede "quão desorganizado" o estado ρ está. Verifique que, para estados puros, temos $S(|\psi\rangle\langle\psi|) = 0$, e $S(\rho) \leq \log_2 d$, com d sendo a dimensão do espaço de estados de ρ, e S atinge seu máximo se o estado quântico é proporcional a identidade.

Estamos agora em condições de enunciar o teorema de Holevo [33].

Teorema 5 (Holevo). *Seja $\rho_X = \sum_i p_i \rho_i$ um estado construído com os p_i dados de acordo com a distribuição de probabilidade de uma variável aleatória X. A distribuição de probabilidade das medições feitas em ρ_X são descritas pela variável aleatória Y.*

Independente da escolha dos operadores de medição, a desigualdade

$$H(X:Y) \leq S(\rho_X) - \sum_i p_i S(\rho_i)$$

é sempre satisfeita. Onde a cota $\chi(\rho) \equiv S(\rho_X) - \sum_i p_i S(\rho_i)$ é chamada de quantidade χ de Holevo.

A prova deste teorema pode ser encontrada na seção 12.1.1 de [6], ou de maneria alternativa na seção 6.2 de [3]

Assim, se Alice deseja enviar para Bob um estado quântico contendo um bit de informação, a informação mútua da variável aleatória X de Alice com a variável Y de Bob deve ser igual a 1, então precisamos que $\chi \geq 1$.

Como $S(\rho) \leq \log_2 d$, um corolário da cota de Holevo é um sistema quântico de dois níveis pode conter no máximo a informação de um bit. Perceba também que para maximizar a informação enviada, Alice deve codificar sua informação em estados puros, para que o segundo termo de χ seja nulo.

A próxima seção vai exibir um protocolo que parece violar do teorema de Holevo. Vamos discutir este aparente paradoxo na seção 2.6, onde será apresentada uma extensão do teorema de Holevo.

2.4 Codificação superdensa

Codificação superdensa é um protocolo que mostra como podemos transmitir a informação dois bits clássicos enviando apenas um qubit. Este resultado foi publicado por Charles Bennett e Stephen Wiesner em 1992 [34] e foi um dos primeiros exemplos de que o "emaranhamento pode facilitar a comunicação".

Alice e Bob compartilham o estado $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, onde o primeiro qubit pertence a Alice e o segundo pertence a Bob.

A primeira parte do protocolo consiste em Alice realizar operações unitárias no seu qubit de acordo com a mensagem que deseja enviar.

- Se Alice deseja enviar $x_1 = 0$ e $x_2 = 0$ ela não faz nenhuma operação, e o estado final é: $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Se Alice deseja enviar $x_1 = 0$ e $x_2 = 1$ ela aplica Z no seu qubit, e o estado final é: $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.
- Se Alice deseja enviar $x_1 = 1$ e $x_2 = 0$ ela aplica X no seu qubit, e o estado final é: $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$.

- Se Alice deseja enviar $x_1 = 1$ e $x_2 = 1$ ela aplica XZ no seu qubit, e o estado final é: $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$.

Repare que os estados $|\psi_{x_1x_2}\rangle$ são ortogonais entre si, ou seja, sempre podem ser discriminados. Alice agora envia o seu qubit a Bob, que com o estado $|\psi_{x_1x_2}\rangle$ em mãos pode fazer uma medição com os projetores de Bell $\{|\beta_{00}\rangle\langle\beta_{00}|, |\beta_{01}\rangle\langle\beta_{01}|, |\beta_{10}\rangle\langle\beta_{10}|, |\beta_{11}\rangle\langle\beta_{11}|\}$ e usar o resultado para obter x_1 e x_2.

E caso Alice e Bob não possuam um par de qubits maximamente emaranhado? Via operações locais, sempre podemos assumir que Alice e Bob começam com o estado[6] $|\psi_0\rangle = a|00\rangle + b|11\rangle$.

O trabalho [35] relaciona a capacidade C, informação máxima (em bits) que pode ser enviada usando um qubit do estado $|\psi_0\rangle$, com o emaranhamento prévio:

$$\begin{aligned} C &= 1 + E(|\psi_0\rangle) \\ &= 1 - (a^2 \log_2 a^2 + b^2 \log_2 b^2). \end{aligned}$$

É interessante usar a condição de normalização do estado quântico[7] para plotar $C(a^2)$.

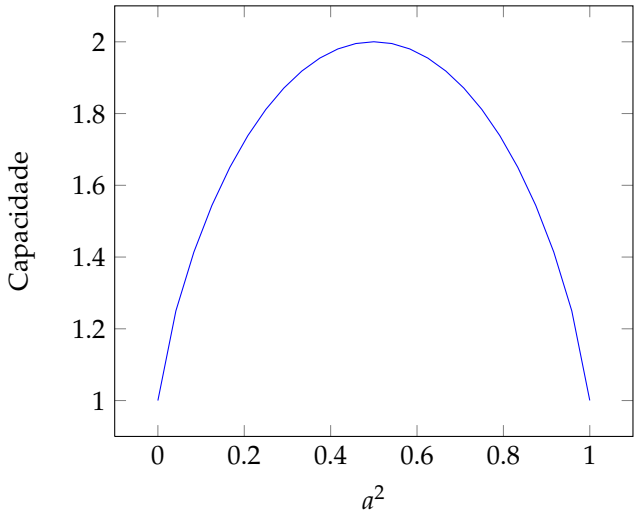

Figura 2.1: Capacidade da codificação superdensa em função de a^2, dada por $C(a^2) = 1 - a^2 \log_2 a^2 - (1 - a^2)(\log_2(1 - a^2))$.

Fica claro então que a "vantagem quântica" depende do emaranhamento prévio compartilhado previamente por Alice e Bob.

[6] É só eles usarem decomposição de Schmidt, seção 1.9
[7] Que implica em $a^2 = 1 - b^2$.

2.5 Teleporte quântico

Figura 2.2: http://xkcd.com/465/

Alice deseja enviar para Bob o qubit $|\psi\rangle = a|0\rangle + b|1\rangle$, porém eles não têm um canal quântico a sua disposição. Seria possível enviar um qubit apenas com operações locais e comunicação clássica?

Caso as partes compartilhem um estado maximamente emaranhado a resposta é sim [36]. Este protocolo ficou conhecido como teleporte, apesar de não envolver de fato o que se imagina de um teleporte, que é transmissão instantânea de matéria ou de informação[8] [37].

Vamos considerar agora o caso em que Alice e Bob compartilham o estado $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Desta forma, o sistema todo é descrito por

$$\begin{aligned}|\Phi\rangle &= |\psi\rangle \otimes |\beta_{00}\rangle \\ &= \frac{1}{\sqrt{2}}(a|0\rangle + b|1\rangle) \otimes (|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle),\end{aligned}$$

onde os dois primeiros qubits pertencem a Alice.

O protocolo consiste em 3 etapas:

1. Alice faz uma medição dos seus qubits com os projetores de Bell $\{|\beta_{00}\rangle\langle\beta_{00}|, |\beta_{01}\rangle\langle\beta_{01}|, |\beta_{10}\rangle\langle\beta_{10}|, |\beta_{11}\rangle\langle\beta_{11}|\}$ e obtém o estado $|\beta_{xy}\rangle$.
2. Alice envia os bits xy a Bob.
3. Bob aplica o operador $X^y Z^x$ no seu qubit.

Para ficar mais claro o que está acontecendo, é conveniente escrever $|\Phi\rangle$ na base Bell.

Note que:

$$\begin{aligned}|00\rangle &= \frac{1}{\sqrt{2}}(|\beta_{00}\rangle + |\beta_{01}\rangle), \ |01\rangle = \frac{1}{\sqrt{2}}(|\beta_{10}\rangle + |\beta_{11}\rangle); \\ |10\rangle &= \frac{1}{\sqrt{2}}(|\beta_{10}\rangle - |\beta_{11}\rangle), \ |11\rangle = \frac{1}{\sqrt{2}}(|\beta_{00}\rangle - |\beta_{01}\rangle).\end{aligned}$$

[8] Na verdade, a quântica sozinha não impõe restrições na velocidade de transmissão da informação. O que "freia" o processo do teleporte é o fato de Bob necessitar receber bits de Alice, e a física nos dá bons motivos para acreditar que os bits clássicos não podem ser transmitidos com velocidade infinita.

Assim, podemos escrever

$$\begin{aligned}|\Phi\rangle &= \frac{1}{2}(|\beta_{00}\rangle(a|0\rangle + b|1\rangle) + (|\beta_{01}\rangle(a|0\rangle - b|1\rangle) \\ &+ (|\beta_{00}\rangle(b|0\rangle + a|1\rangle) + (|\beta_{11}\rangle(-b|0\rangle + a|1\rangle) \\ &= \frac{1}{2}(|\beta_{00}\rangle|\psi\rangle + |\beta_{01}\rangle Z|\psi\rangle + |\beta_{10}\rangle X|\psi\rangle + |\beta_{11}\rangle ZX|\psi\rangle).\end{aligned}$$

Como $XX = ZZ = I$, deve ficar claro que no final do protocolo, Bob terá exatamente $|\psi\rangle$.

2.6 Codificação superdensa, teleporte e o teorema de Holevo

> *"In this significant sense, quantum theory subscribes to the view that the whole is greater than the sum of its parts."*
>
> Hermann Weyl

A codificação superdensa troca 1 bit quântico por 2 bits clássicos, o teleporte troca 2 bits clássicos por 1 quântico. Em [38] Nilsen estendeu o teorema de Holevo para demonstrar que tanto a codificação superdensa quanto o teleporte são ótimos, no sentido de que um qubit pode ser trocado por no máximo dois bits, e dois bits podem fornecer no máximo um qubit.

Mas isto não seria uma violação do teorema de Holevo? Como Alice pode enviar 2 bits clássicos a troco de um qubit?

O detalhe que as vezes passa despercebido na codificação superdensa é que o sistema que descreve o estado de Alice e Bob tem dimensão 4. Apesar de Alice enviar um qubit no final do protocolo, existem na verdade dois qubits que, pelo fato de estarem emaranhados, não podem ser vistos como sistemas independentes individuais.

Vamos então enunciar o teorema demonstrado por Nilsen.

Teorema 6. *Alice quer enviar n bits de informação para Bob usando qubits, e sabe-se que eles não possuem nenhum emaranhamento prévio. Seja n_{AB} o número de qubits enviados de Alice para Bob e n_{BA} o número de qubits enviados de Bob para Alice. Para que Bob receba os n bits de informação, as desigualdades abaixo devem ser satisfeitas*[9]*:*

$$\begin{aligned}n_{AB} &\leq \lceil n/2 \rceil, \\ n_{AB} + n_{BA} &\leq n.\end{aligned}$$

Para tratar casos onde existe emaranhamento prévio, basta permitir que Bob possa enviar qubits para Alice sem custo. Assim, Bob emaranha localmente alguns qubits e envia parte para Alice, daí precisamos apenas nos preocupar com a cota $n_{AB} \leq \lceil n/2 \rceil$.

Esta interpretação sugere também uma aplicação interessante para a codificação superdensa. Alice pode criar um estoque de qubits emaranhados com

[9] $\lceil n/2 \rceil$ é o número inteiro pertencente ao intervalo $[n/2,(n+1)/2]$.

Bob durante a noite, quando o canal está ocioso. E de dia, quando precisam se comunicar, usam os qubits emaranhados como recurso para a codificação superdensa.

2.7 Emaranhamento e não-sinalização

Protocolos como o de codificação superdensa, teleporte e vários outros que serão apresentados nos próximos capítulos, revelam que o emaranhamento, de alguma maneira, facilita a comunicação. Mas, poderiam Alice e Bob trocar informação apenas utilizando operações e medições locais feitas em estados emaranhados?

A resposta é não.

Teorema 7. *Mesmo com estados emaranhados, operações e medições locais não podem ser utilizadas para troca de informação entre duas partes.*

Demonstração. Seja $|\psi\rangle \in (\mathcal{H}_A \otimes \mathcal{H}_B)$. Operações locais feitas por Bob, por definição, não alteram o estado de Alice. Logo, não podem ser usadas para trocar informação.

Agora poderíamos imaginar que Alice, de alguma maneira descubra algo sobre as medições feitas por Bob, o que implica em ganho de informação. Do postulado da medição, temos:

$$p(n = a, m = b|\{A_n\}, \{B_m\}) = \langle\psi|(A_a^\dagger A_a \otimes B_b^\dagger B_b)|\psi\rangle.$$

Se temos acesso apenas a parte das medições dadas por $\{A_n\}$, o melhor que podemos obter é a probabilidade marginal, dada por:

$$\begin{aligned} p(n = a|\{A_n\},\{B_m\}) &= \sum_b p(n = a,m = b|\{A_n\},\{B_m\}) \\ &= \sum_b \langle\psi|(A_a^\dagger A_a \otimes B_b^\dagger B_b)|\psi\rangle \\ &= \langle\psi|(A_a^\dagger A_a \otimes I)|\psi\rangle. \end{aligned}$$

Vemos que as probabilidades de Alice obter algum resultado a independe da escolha dos operadores de medição $\{B_m\}$ feita por Bob. Logo, Alice não pode obter informações sobre as operações feitas por Bob medindo seu estado.[10] □

Vale lembrar que toda informação obtida de um sistema quântico vem das medições e se Alice não pode descobrir as operações feitas por Bob com medição, ela não pode descobrir as operações feitas por Bob de maneira alguma! Este é um teorema fundamental para o trabalho e vale a pena discutir um caso especial, visto que o postulado da medição é facilmente mal interpretado[11]:

[10] Usando o formalismo de operador densidade com a definição de traço parcial, ou interpretando o teorema 6, chegamos de maneira mais simples ao mesmo resultado. Porém, abrir as contas para estados puros pode ser mais esclarecedor.

[11] Quase toda discussão de paradoxo EPR [39] que veremos no capítulo 3 acontece devido a uma interpretação errônea do postulado da medição.

Vamos assumir que Alice e Bob não têm acesso a comunicação, mas compartilham o estado $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Suponha que Bob mede seu qubit na base computacional e obtém 0. A partir deste momento o estado compartilhado é $|00\rangle$, e o qubit de Alice passou de algo indeterminado para $|0\rangle$. Einstein se referiu a este efeito como *"Spooky action at a distance"*, e viu aí algo estranho. Uma medição feita por Bob modificou instantaneamente o estado de Alice!

Repare porém que Alice ainda não sabe o resultado de Bob, ou pior, Alice ainda nem sabe se Bob fez de fato a medição.

Alguém poderia pensar em um protocolo da forma: caso Bob deseja enviar o bit 0, ele deve obter o resultado 0; caso ele queira enviar 1, ele deve obter o resultado 1. Mas Bob não pode "obrigar" sua medição a retornar o valor desejado.

Apesar do postulado da medição afirmar que o estado de Alice se modifica imediatamente após a medição de Bob, não é possível medir essa troca de informação. Logo, para um olhar positivista, não existe ação à distância.

Capítulo 3

Não-localidade: quântica e supra-quântica[1]

Como vimos no capitulo anterior, o emaranhamento está por trás de fenômenos atraentes da mecânica quântica. Historicamente ele ganhou atenção especial em 1935, quando Einstein, Podolsky e Rosen publicaram o famoso *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* [39], que apontavam um possível furo na mecânica quântica. Historicamente, foi esta a motivação para Schrödinger cunhar o termo *quantenverschränkung*, primeira palavra utilizada para se tratar de sistemas emaranhados[2].

O artigo de Einstein ficou conhecido como paradoxo EPR e gerou uma enorme discussão na comunidade científica [42]. Discussões que, assim como as feitas por Einstein, não davam uma explicação satisfatória para o problema. A situação muda em 1964, quando John S. Bell publica *On the Einstein-Poldolsky-Rosen paradox* [43] e esclarece o problema. Bell define realismo e localidade e mostra que as regras da mecânica quântica são incompatíveis com assumir ambos.

Vamos tentar trabalhar como Bell, evitar discussões confusas e ir para resultados concretos.

3.1 Definições

Esta é uma parte delicada do trabalho, pois as definições que serão feitas são fundamentais para o resto da monografia e facilmente se confundem. Esta seção e vários trechos deste capítulo foram inspirados por [44].

Para facilitar a compreensão vamos tratar apenas de sistemas com duas partes. A parte A tem à sua disposição uma coleção de propriedades X que podem ser mensuradas. Medir uma certa propriedade $x \in X$ retorna um resultado $a \in x$. A parte B tem uma coleção de propriedades Y, e medir $y \in Y$ retorna um resultado $b \in y$.

[1] Para uma introdução a não-localidade com uma abordagem similar a apresentada neste capítulo, veja [40]

[2] Na verdade, o próprio Schrödinger batizou os termos quantenverschränkung [41] e entanglement [1], dando margem para a discussão de qual termo veio primeiro.

Vamos denotar por $p_{a,b|x,y}$ a probabilidade dos resultados a e b serem obtidos, dado que as medições x e y foram realizadas.

A descrição individual de cada sistema é feita pelas probabilidades marginais,

$$p_{a|x,y} = \sum_b p_{a,b|x,y}.$$

Repare que estamos permitindo que a medição de Alice dependa da propriedade y que Bob deseja medir. Podemos imaginar uma situação em que realizar a medição y comunica algo para o receptor de x. É justamente para garantir que não teremos essa comunicação que vamos definir não-sinalização.

Não-sinalização

Definição 11 (Não-sinalização)**.** *As diferentes partes do sistema não trocam informação entre si. Isto é,* $p_{a|x,y} = p_{a|x}$ *e* $p_{b|x,y} = p_{b|y}$.

Para ilustrar o conceito por trás da não-sinalização, imagine que uma moeda seja cortada ao meio, de modo a ter uma parte só com cara e outra só coroa e que cada metade seja colocada em um envelope. Um destes envelopes é enviado a Alice, o outro a Bob. Ao abrir seu envelope e obter cara, Alice sabe, com certeza, que Bob vai obter coroa.

Pode parecer que ouve troca de informação, já que Alice descobriu algo sobre o envelope de Bob. Mas perceba eles não podem usar este envelope para trocar informação, Alice não tem poder para escolher o que Bob vai abrir[3].

Vale lembrar da seção 2.7, que as probabilidades previstas para sistemas quânticos bipartites respeitam a condição de não sinalização.

Perceba que a condição de não-sinalização não é suficiente para garantir que uma medição esteja descorrelacionada da outra. Vamos dizer que duas medições estão correlacionadas quando $p_{a,b|x,y} \neq p_{a|x}p_{b|y}$.

Além do caso de estados emaranhados, o leitor pode construir um simples exemplo dessas correlações com a caixa Popescu-Rohrlich [45], que será discutida em 3.7.

Realismo

> *"I recall that during one walk Einstein suddenly stopped, turned to me and asked whether I really believed that the moon exists only when I look at it. The rest of this walk was devoted to a discussion of what a physicist should mean by the term "to exist"."*
>
> Abraham Pais

Os *elementos de realidade* de Einstein [39] se baseiam na ideia de que existe uma teoria na qual todos os resultados de medições podem (pelo menos em princípio) ser previstos com probabilidade 1.

[3]Para se convencer que não há troca de informação, tente usar estes envelopes para desenvolver um protocolo em que Bob conte para Alice o resultado do lançamento de um dado.

O realismo está associado a noção de que o resultado de nossas observações já está pré-determinado. A ideia informal se baseia no fato de que quando observamos uma bola verde, apenas *descobrimos* que ela é verde. Deve haver uma variável que *sabe* a cor de todas as bolas, mas nós apenas não temos acesso a ela.

Definição 12 (Realismo)**.** *Determinado o sistema conjunto AB, existe uma variável* λ *tal que* $p_{a,b|x,y,\lambda}$ *é* 1 *ou* 0, $\forall a \in x, b \in y, x \in X, y \in Y$.

Localidade

Mesmo assumindo a existência da variável λ, ainda podemos ter $p_{a,b|x,y,\lambda} \neq p_{a|x,\lambda} p_{b|y,\lambda}$.

Uma hipótese natural é que tendo o conhecimento de λ, vamos saber a origem de todas correlações, logo todos os eventos passam a se tornar independentes.

Definição 13 (Localidade)**.** *Dado* λ*, sempre vamos ter* $p_{a,b|x,y,\lambda} = p_{a|x,\lambda} p_{b|y,\lambda}$.

Assim, experimentos realistas locais podem ser descritos por[4]

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

onde q_λ é uma distribuição de probabilidade da variável λ no conjunto Λ.

Teorema 8. *Todas as correlações de teoria realista local satisfazem a condição de não sinalização*

Demonstração.

$$\begin{aligned} p_{a|x,y} &= \sum_b \int_\Lambda q_\lambda p_{a|x,\lambda} p_{b|y,\lambda} d\lambda \\ &= \int_\Lambda q_\lambda p_{a|x,\lambda} (\sum_b p_{b|y,\lambda}) d\lambda \\ &= p_{a|x}. \end{aligned}$$

□

3.2 O singleto

Para relacionar as definições dadas com a mecânica quântica, é interessante usar o exemplo de um sistema com dois qubits emaranhados.

Vamos então explorar as propriedades do singleto[5]: $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, estado que também ficou famoso por ser coração do paradoxo EPR.

[4]Poderíamos também escrever $p_{a,b|x,y} = \int_\Lambda p_{a|x,\lambda} p_{b|y,\lambda} d\mu(\lambda)$, com μ sendo uma dada medida arbitrária. Mas para nossa discussão, essa generalização não acrescenta muita coisa.

[5]A origem deste nome vem da teoria de spin, onde o singleto descreve o estado quântico de duas partículas de spin $\frac{1}{2}$ que tem spin total nulo.

Teorema 9. *Seja $U : \mathcal{H}_2 \to \mathcal{H}_2$ um operador unitário, temos necessariamente $U \otimes U|\beta_{11}\rangle = |\beta_{11}\rangle$. Ou seja, o singleto é invariante a unitárias locais.*

Demonstração. Segue da definição que um operador unitário preserva a ortogonalidade de dois vetores. Então, podemos parametrizar a ação de U como:

$$\begin{aligned} U|0\rangle &= \alpha|0\rangle + \beta|1\rangle; \\ U|1\rangle &= \beta^*|0\rangle - \alpha^*|1\rangle. \end{aligned}$$

Vamos aplicar diretamente $U \otimes U$ em $|\beta_{11}\rangle$:

$$\begin{aligned} U \otimes U|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(U \otimes U|01\rangle - U \otimes U|10\rangle) \\ &= \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) \otimes (\beta^*|0\rangle - \alpha^*|1\rangle) \\ &- \frac{1}{\sqrt{2}}(\beta^*|0\rangle - \alpha^*|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= \frac{1}{\sqrt{2}}(\alpha\beta^*|00\rangle - |\alpha|^2|01\rangle + |\beta|^2|10\rangle - \alpha^*\beta|11\rangle \\ &- \alpha\beta^*|00\rangle - |\beta|^2|01\rangle + |\alpha|^2|10\rangle + \alpha^*\beta|11\rangle) \\ &= (|\alpha|^2 + |\beta|^2)\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\ &= |\beta_{11}\rangle. \end{aligned}$$

□

Seja $M : \mathcal{H}_2 \to \mathcal{H}_2$ um operador auto-adjunto e unitário. Desta maneira M é um observável com os operadores medição dados por $\{M_{-1} = |m_+\rangle\langle m_+|, M_{+1} = |m_-\rangle\langle m_-|\}$.

O teorema 9 nos permite escrever $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|m_+\rangle|m_-\rangle - |m_-\rangle|m_+\rangle)$.[6] Assim, se Alice (que possui primeiro qubit) e Bob (dono do segundo qubit) fizerem uma medição com o observável $M \otimes M$ sempre vão obter resultados anti-correlacionados. Isto é, sempre que Alice obtiver $+1$, Bob vai obter -1, *vice versa*.

Um olhar superficial pode indicar que esta anti-correlação não apresenta nenhuma característica surpreendente. Em [46], Bell conta a história de Bertelmann, um homem que sempre usa suas meias com cores diferentes. Se você vê que ele está com um pé de meia rosa, já sabe com certeza que o outro não é rosa.

Mas perceba que as meias de Bertelmann não tem a mesma correlação que um sistema descrito pelo singleto. Repare que a anti-correlação do singleto não vale apenas para um específico observável M, mas para todos aqueles que tem autovalores $+1$ e -1.

[6] Lembrando que $|m_+\rangle$ é o autovetor de M associado ao auto-valor de $+1$, e $|m_-\rangle$ o auto-vetor associado a -1.

3.3 Desigualdade de Wigner

Vamos agora usar as propriedades do singleto para mostrar que não podemos criar uma teoria realista local que prevê as mesmas probabilidades da mecânica quântica[7].

Alice e Bob compartilham várias cópias do estado $|\beta_{11}\rangle$. Eles combinam 3 observáveis $\mathbf{a}\cdot\sigma$, $\mathbf{b}\cdot\sigma$, $\mathbf{c}\cdot\sigma$ [8] e fazem medições isoladamente.

Como vimos na seção anterior, ambos só podem obter os resultados $+1$ ou -1 e, no caso de escolherem os mesmos observáveis, vão ter necessariamente resultados anti-correlacionados.

Vamos agora assumir realismo e localidade e analisar as condições impostas por estas. Seja $(\mathbf{a}_+, \mathbf{b}_+, \mathbf{c}_-)$ o estado da partícula que retorna $+1$ para o observável $\mathbf{a}\cdot\sigma$, $+1$ para $\mathbf{b}\cdot\sigma$ e -1 para $\mathbf{c}\cdot\sigma$. Podemos escrever todos os estados possíveis de maneira análoga e construir uma tabela que atribui probabilidades aos estados de Alice e Bob.

Probabilidade	Estado de Alice	Estado de Bob
P_1	$(\mathbf{a}_+, \mathbf{b}_+, \mathbf{c}_+)$	$(\mathbf{a}_-, \mathbf{b}_-, \mathbf{c}_-)$
P_2	$(\mathbf{a}_+, \mathbf{b}_+, \mathbf{c}_-)$	$(\mathbf{a}_-, \mathbf{b}_-, \mathbf{c}_+)$
P_3	$(\mathbf{a}_+, \mathbf{b}_-, \mathbf{c}_+)$	$(\mathbf{a}_-, \mathbf{b}_+, \mathbf{c}_-)$
P_4	$(\mathbf{a}_+, \mathbf{b}_-, \mathbf{c}_-)$	$(\mathbf{a}_-, \mathbf{b}_+, \mathbf{c}_+)$
P_5	$(\mathbf{a}_-, \mathbf{b}_+, \mathbf{c}_+)$	$(\mathbf{a}_+, \mathbf{b}_-, \mathbf{c}_-)$
P_6	$(\mathbf{a}_-, \mathbf{b}_+, \mathbf{c}_-)$	$(\mathbf{a}_+, \mathbf{b}_-, \mathbf{c}_+)$
P_7	$(\mathbf{a}_-, \mathbf{b}_-, \mathbf{c}_+)$	$(\mathbf{a}_+, \mathbf{b}_+, \mathbf{c}_-)$
P_8	$(\mathbf{a}_-, \mathbf{b}_-, \mathbf{c}_-)$	$(\mathbf{a}_+, \mathbf{b}_+, \mathbf{c}_+)$

Tabela 3.1: Todos os possíveis estados permitidos por uma teoria realista local.

Pode parecer que utilizamos apenas o realismo para montar a tabela acima, mas repare por exemplo no grupo P_1. Se Alice medir $\mathbf{a}\cdot\sigma$ ela vai obter $+1$, e este fato independe da escolha da medição feita por Bob.

Da tabela 3.1 podemos obter as probabilidades dos resultados de Alice e Bob dado um observável. Por exemplo

$$p(\mathbf{a}_+,\mathbf{b}_+) = P_3 + P_4,$$

que é a probabilidade de Alice obter $+1$ ao medir o observável $\mathbf{a}\cdot\sigma$, e de Bob obter $+1$ ao medir o observável $\mathbf{b}\cdot\sigma$. De maneira análoga:

$$p(\mathbf{a}_+,\mathbf{c}_+) = P_2 + P_4, \qquad p(\mathbf{c}_+,\mathbf{b}_+) = P_3 + P_7.$$

Assim temos a desigualdade[9]

$$p(\mathbf{a}_+,\mathbf{b}_+) \leq p(\mathbf{a}_+,\mathbf{c}_+) + p(\mathbf{c}_+,\mathbf{b}_+). \tag{3.1}$$

[7] A abordagem que vamos usar nesta seção foi feita por Bell em [46] e é baseada do trabalho de Wigner [47].

[8] Lembrando que $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$ são vetores normalizados em $\mathbb{R}^3$ e usamos a notação $\mathbf{a}\cdot\sigma \equiv a_x X + a_y Y + a_z Z$

[9] No trabalho original, Wigner interpreta essa desigualdade como "O número de mulheres novas é menor ou igual ao número de mulheres fumantes mais o número de pessoas novas não fumantes".

Vamos analisar as probabilidades previstas pela mecânica quântica. Considere $p(\mathbf{a}_+,\mathbf{b}_+)$, neste as regras da mecânica quântica nos afirmam que a probabilidade é

$$\langle\beta_{11}|(|a_+\rangle\langle a_+|\otimes|b_+\rangle\langle b_+|)|\beta_{11}\rangle.$$

Logo, basta encontrar os autovetores do obversável $\mathbf{n}\cdot\boldsymbol{\sigma}$, e fazer as contas. Mas podemos evitar algumas contas se pensamors que Alice mede $\mathbf{a}_+$ com probabilidade $1/2$, e o fato de Alice obter $\mathbf{a}_+$ implica que o estado de Bob será descrito por $|a_-\rangle$. Dado este estado, a probabilidade[10] de Bob obter $\mathbf{b}_+$ é

$$|\langle a_-|b_+\rangle|^2 = \text{sen}^2\,(\theta_{ab}/2),$$

onde $\theta_{ab} = \mathbf{a}\cdot\mathbf{b}$ é o angulo entre os eixos $\mathbf{a}$ e $\mathbf{b}$.

Assim,

$$p(\mathbf{a}_+,\mathbf{b}_+) = \frac{1}{2}\,\text{sen}^2\left(\frac{\theta_{ab}}{2}\right).$$

E usando (3.1) podemos escrever

$$\text{sen}^2\left(\frac{\theta_{ab}}{2}\right) \leq \text{sen}^2\left(\frac{\theta_{ac}}{2}\right) + \text{sen}^2\left(\frac{\theta_{cb}}{2}\right).$$

Tomando $\theta_{ab} = \theta$, $\theta_{ac} = 2\theta$ e $\theta_{cb} = 2\theta$ com $0 < \theta < \frac{\pi}{2}$, a desigualdade não é respeitada.

Este exemplo mostra que as correlações do estado singleto não podem ser obtidas de uma teoria realista local. Desigualdades que são capazes de "separar" teorias realistas locais da mecânica quântica são chamadas de *Desigualdades de Bell*. Na próxima seção veremos que esta não-localidade da mecânica quântica está diretamente relacionada com o emaranhamento.

3.4 CHSH

A desigualdade $CHSH$, proposta por Clauser, Horne, Shimony e Holt em 1969 [48], é provavelmente a desigualdade de Bell mais conhecida. Grande parte de sua fama se deve ao fato dela ter sido utilizada em trabalhos pioneiros para verificação experimental de desigualdades de Bell [49] e, por além de impor uma cota superior a teorias realistas e locais, impõe também uma cota superior para a mecânica quântica [50].

Tome o cenário em que duas partes (A e B) podem medir duas propriedades de um sistema com duas possíveis saídas para cada propriedade. Assim como na seção 3.1, as probabilidades conjuntas serão descritas por $p_{a,b|x,y}$, com[11] $a,b,x,y \in \{0,1\}$. Defina:

$$\begin{aligned}\beta_{CHSH} \equiv\ & p_{a=b|0,0} - p_{a\neq b|0,0} + p_{a=b|0,1} - p_{a\neq b|0,1} \\ & + p_{a=b|1,0} - p_{a\neq b|1,0} - p_{a=b|1,1} + p_{a\neq b|1,1},\end{aligned} \tag{3.2}$$

[10] Para simplificar mais as contas, note que podemos escolher $\mathbf{b}$ como sendo um vetor unitário na direção de $\mathbf{z}$, assim $|b_+\rangle = |0\rangle$, e precisamos apenas do autovetor de $\mathbf{a}\cdot\boldsymbol{\sigma}$ associado ao autovalor -1.

[11] Lembrando que a é o valor obtido por Alice ao medir o observável x e b o valor obtido por Bob ao medir y.

onde

$$p_{a=b|x,y} = p_{0,0|x,y} + p_{1,1|x,y},$$
$$p_{a\neq b|x,y} = p_{0,1|x,y} + p_{1,0|x,y}.$$

Como p representa probabilidades, temos $p \in [0,1]$, e é trivial verificar que $|\beta_{CHSH}| \leq 4$.

CHSH em teorias realistas locais

Vamos assumir agora realismo e localidade, logo existem λ e q_λ tal que:

$$p_{a=b|x,y} = \int_\Lambda q_\lambda \Big(p_{0|x,\lambda} p_{0|y,\lambda} + p_{1|x,\lambda} p_{1|y,\lambda} \Big) d\lambda,$$
$$p_{a\neq b|x,y} = \int_\Lambda q_\lambda \Big(p_{0|x,\lambda} p_{1|y,\lambda} + p_{1|x,\lambda} p_{0|y,\lambda} \Big) d\lambda.$$

Perceba que não comentamos sobre a estrutura de uma teoria que use a variável λ, apenas assumimos sua existência.

Teorema 10. *Em teorias realistas locais, temos obrigatoriamente* $|\beta_{CHSH}| \leq 2$.

Demonstração. Com a hipótese da existência de λ e a condição $\sum_a \sum_b p_{a,b|x,y} = 1$, podemos escrever β_{CHSH} como:

$$\beta_{CHSH} = 2 \int_\Lambda q_\lambda [(2p_{a=0|x=0,\lambda} - 1)(p_{b=0|y=0,\lambda} + p_{b=0|y=1,\lambda} - 1) + (2p_{a=0|x=1,\lambda} - 1)(p_{a=0|x=1,\lambda} - p_{b=0|y=1,\lambda})] d\lambda.$$

Lembre que dado λ, as probabilidades só podem ser 0 ou 1. Com isso fica fácil ver que o resultado do termo entre colchetes é -1 ou 1.

Como estamos integrando sobre uma distribuição de probabilidade, o valor da integral não pode ter módulo maior que 1. Logo,

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

□

Está montada então uma desigualdade de Bell. Vamos agora escrever β_{CHSH} usando as previsões da mecânica quântica.

CHSH na mecânica quântica

Sejam A_0 e A_1 observáveis unitários[12] que vão representar as propriedades que Alice vai medir. Sejam B_0 e B_1 as propriedades que Bob vai medir.

É conveniente fazer uma mudança de notação; vamos usar $a,b \in \{-1,1\}$. Mas repare que o β_{CHSH} definido na equação (3.2) independe dos valores que a e b podem assumir.

[12] Logo, um operadores auto-adjuntos e unitários, que sempre têm autovalores $+1$ e -1.

Vamos calcular o valor esperado do observável $A_x \otimes B_y$ para um certo estado $|\psi\rangle$:

$$\begin{aligned}\langle A_x \otimes B_y \rangle_{|\psi\rangle} &= \sum_{a=\pm 1} \sum_{b=\pm 1} ab\, p_{a,b|x,y} \\ &= p_{-1,-1|x,y} - p_{1,-1|x,y} - p_{-1,1|x,y} + p_{1,1|x,y} \\ &= p_{a=b|x,y} - p_{a\neq b|x,y}.\end{aligned}$$

Agora podemos escrever:

$$\beta_{CHSH} = \langle A_0 \otimes B_0 \rangle_{|\psi\rangle} + \langle A_0 \otimes B_1 \rangle_{|\psi\rangle} + \langle A_1 \otimes B_0 \rangle_{|\psi\rangle} - \langle A_1 \otimes B_1 \rangle_{|\psi\rangle},$$

que nos motiva a definir um observável Bell associado a desigualdade $CHSH$,

$$\mathcal{B}_{CHSH} \equiv A_0 \otimes B_0 + A_0 \otimes B_0 + A_1 \otimes B_0 - A_1 \otimes B_1.$$

Com o operador $\mathcal{B}_{CHSH}$ em mãos, podemos calcular o valor esperado para algum estado qualquer, e verificar se a mecânica quântica respeita $|\beta_{CHSH}| \leq 2$.

As correlações de estados da forma $|\psi\rangle = |a\rangle \otimes |b\rangle$ sempre podem ser descritas por teorias realistas locais, pois neste caso temos

$$\langle A_0 \otimes B_0 \rangle_{|\psi\rangle} = \langle a|A_0|a\rangle \langle b|B_0|b\rangle.$$

Assim, podemos tomar os observáveis A_0, A_1, B_0 e B_1 como números reais que pertencem ao intervalo $[0, 1]$, que nos permite fazer

$$\begin{aligned}\beta_{CHSH} &= A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 \\ &= A_0(B_0 - B_1) + A_1(B_0 + B_1) \\ &\leq 2.\end{aligned}$$

O leitor que se interessar na construção de uma teoria realista e local que simula os resultados da mecânica quântica para estados fatoráveis pode buscar a tese de Benjamin Francis Toner [51].

No caso dos operadores A_0, A_1, B_0 e B_1 comutarem entre si, também podemos criar um modelo realista local, pois operadores que comutam podem ser diagonalizados simultaneamente. Assim eles podem também ser tratados como números reais. [52] [13]

Vamos agora exibir um exemplo mais interessante. Tome o estado $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ e os operadores

$$\begin{aligned} A_0 = X, \quad A_1 = Z; \\ B_0 = \frac{X+Z}{\sqrt{2}}, \quad B_1 = \frac{X-Z}{\sqrt{2}}. \end{aligned}$$

[13] Vale notar que o fato da mecânica quântica permitir observáveis não compatíveis, *i.e.*, descritos por operadores que não comutam, é apontado como sua principal diferença sobre a mecânica clássica, onde todos observáveis são compatíveis. Muitos físicos gostam de introduzir mecânica quântica assumindo que os observáveis posição e momento não são compatíveis.

Assim temos,

$$\begin{aligned}\langle \mathcal{B}_{CHSH}\rangle_{|\beta_{00}\rangle} &= \langle\beta_{00}|\left(X\otimes\frac{X+Z}{\sqrt{2}}\right)|\beta_{00}\rangle + \langle\beta_{00}|\left(X\otimes\frac{X-Z}{\sqrt{2}}\right)|\beta_{00}\rangle \\ &+ \langle\beta_{00}|\left(Z\otimes\frac{X+Z}{\sqrt{2}}\right)|\beta_{00}\rangle - \langle\beta_{00}|\left(Z\otimes\frac{X-Z}{\sqrt{2}}\right)|\beta_{00}\rangle \\ &= \left(\frac{1}{\sqrt{2}}\right)+\left(\frac{1}{\sqrt{2}}\right)+\left(\frac{1}{\sqrt{2}}\right)-\left(-\frac{1}{\sqrt{2}}\right) \\ &= 2\sqrt{2},\end{aligned}$$

que é uma violação da desigualdade $CHSH$.

3.5 Ligação entre emaranhamento e não-localidade

> *"and correlations cry out for explanations..."*
>
> John S. Bell

Na seção anterior vimos que não-localidade é característica de estados emaranhados. Mas será que todos estados emaranhados exibem não-localidade?

Está pergunta foi respondida (para o caso de sistemas bipartites) em 1991 por Gisin [53].

Teorema 11. *Todo sistema bipartite emaranhado (puro) viola alguma desigualdade CHSH.*

Demonstração. Seja $|\psi\rangle$ um estado emaranhado. Usando a decomposição de Schmidt ele pode ser escrito como

$$|\psi\rangle = \sum_i c_i|\Xi_i\rangle\otimes|\phi_i\rangle.$$

A condição de emaranhamento impõe que pelo menos c_1 e c_2 são maiores que zero. Vamos então definir:

$$\begin{aligned}|\psi_1\rangle &= c_1|\Xi_1\rangle|\phi_1\rangle + c_2|\Xi_2\rangle|\phi_2\rangle; \\ |\psi_2\rangle &= \sum_{i>2} c_i|\Xi_i\rangle|\phi_i\rangle;\end{aligned}$$

assim, $|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle$.

O vetor[14] $|\psi_1\rangle$ pode ser tratado como um sistema de dois qubits e, para simplificar a notação vamos escrever $|\psi_1\rangle = c_1|01\rangle + c_2|10\rangle$.

Tome os observáveis unitários como:

$$\begin{aligned}A_0 &= Z; \\ A_1 &= -X; \\ B_y &= \operatorname{sen}\alpha_y X + Z\cos\alpha_y.\end{aligned}$$

[14]Perceba que $|\psi_1\rangle$ e $|\psi_2\rangle$ no caso geral não são estados. Pois não são necessariamente vetores normalizados, apenas $|\psi\rangle$ tem obrigatoriamente norma 1.

Assim vamos ter

$$\beta_{CHSH} = \cos\alpha_0 - \cos\alpha_1 + 2c_1c_2(\operatorname{sen}\alpha_0 + \operatorname{sen}\alpha_1),$$

e o máximo se encontra em $\cos\alpha_0 = -\cos\alpha_1 = (1+4(c_1c_2)^2)^{-1/2}$, então temos

$$\beta_{CHSH} = 2\sqrt{1+4(c_1c_2)^2},$$

que é estritamente maior que 2. □

Em 2010 o teorema de Gisin foi estendido; demonstrou-se que todo estado emaranhado multipartite (puro) viola alguma desigualdade de Bell. [54].

Assim, temos uma ligação direta entre emaranhamento e não-localidade.

3.6 Uma cota para a não-localidade quântica

Como foi antecipado no início da seção 3.4, assim como teorias realistas e locais, a mecânica quântica impõe restrição no valor máximo de $|\beta_{CHSH}|$. Este resultado foi apresentado pela primeira vez por Tsirelson em 1980 [50] e ficou conhecido como *"Tsirelson's Bound"*, ou apenas cota de Tsirelson.

Teorema 12. *Assumindo os postulados de mecânica quântica, temos necessariamente* $|\beta_{CHSH}| \leq 2\sqrt{2}$.

Demonstração. Vamos calcular

$$\mathcal{B}^2_{CHSH} = (A_0 \otimes B_0 + A_0 \otimes B_0 + A_1 \otimes B_0 - A_1 \otimes B_1)^2.$$

Segue direto das contas que:

$$\mathcal{B}^2_{CHSH} = 4I - [A_0,A_1] \otimes [B_0,B_1].$$

Defina $||A_0||$ como o módulo do maior autovalor do operador A_0. Assim, temos

$$||[V,W]|| \leq 2||V||\,||W|| \quad , \quad ||V \otimes W|| = ||V||\,||W|| \quad \text{e} \quad ||V^2|| = ||V||^2,$$

que nos permite escrever

$$||\mathcal{B}_{CHSH}||^2 \leq 4 + 4||A_0||\,||A_1||\,||B_0||\,||B_1||.$$

Como os autovalores dos operadores pertencem a $\{-1,1\}$, temos

$$||\mathcal{B}^2_{CHSH}|| \leq 8, \quad \text{ou simplesmente} \quad ||\mathcal{B}_{CHSH}|| \leq 2\sqrt{2}.$$

Logo, basta tomar como estado o autovetor associado ao maior autovalor de $\mathcal{B}_{CHSH}$ para concluir que:

$$|\beta^{max}_{CHSH}| \leq 2\sqrt{2}.$$

□

3.7 Caixas Popescu-Rohrlich

Ao analisar a não localidade permitida pela mecânica quântica, Sandu Popescu e Daniel Rohrlich tiveram a ideia de assumir não-localidade como um axioma e derivar os postulados da mecânica quântica [45].

Nesta busca, eles construíram um artefato teórico que respeita a condição de não sinalização e que tem exatamente $\beta_{CHSH} = 4$. Este artefato ficou conhecido como caixa de Popescu-Rohrlich, ou caixa PR. No capítulo 4 vamos encarar a caixa PR de uma maneira um pouco diferente; para este capítulo podemos simplesmente imaginar que os resultados a e b de Alice e Bob sempre ficam correlacionados com as propriedades x e y satisfazendo a seguinte relação:

$$a + b = x.y,$$

onde quando estivermos tratando de variáveis binárias[15], vamos entender o sinal "$+$" como soma em $\mathbb{Z}_2$, ou seja, soma módulo 2.

Os resultados da caixa são descritos por:

$$p_{a,b|x,y} = 1/2, \quad \text{se } a + b = x.y;$$
$$p_{a,b|x,y} = 0, \quad \text{se } a + b \neq x.y.$$

Pode-se verificar que a caixa PR satisfaz a condição de não-sinalização:

$p_{0,0\|0,0} = 1/2$	$p_{0,0\|0,1} = 1/2$
$p_{0,1\|0,0} = 0$	$p_{0,1\|0,1} = 0$
$p_{1,0\|0,0} = 0$	$p_{1,0\|0,1} = 0$
$p_{1,1\|0,0} = 1/2$	$p_{1,1\|0,1} = 1/2$
$p_{0,0\|1,0} = 1/2$	$p_{0,0\|1,1} = 0$
$p_{0,1\|1,0} = 0$	$p_{0,1\|1,1} = 1/2$
$p_{1,0\|1,0} = 0$	$p_{1,0\|1,1} = 1/2$
$p_{1,1\|1,0} = 1/2$	$p_{1,1\|1,1} = 0$

Tabela 3.2: Probabilidades $p_{a,b|x,y}$ da caixa PR

$p_{a|x,y} = p_{a,0|x,y} + p_{a,1|x,y} = p_{a|x}$. Mesmo Alice sabendo x e a, ela não tem informações sobre y nem b.

Perceba também que

$$p_{a=b|00} = p_{a=b|01} = p_{a=b|10} = p_{a\neq b|11} = 1;$$
$$p_{a\neq b|00} = p_{a\neq b|01} = p_{a\neq b|10} = p_{a=b|11} = 0,$$

então temos $\beta_{CHSH} = 4$.

A caixa PR serviu para mostrar que podemos obter valores maiores que $2\sqrt{2}$ para β_{CHSH} que respeitam a condição de não-sinalização. E no capítulo 5 vamos mostrar algumas consequências desta "super não-localidade".

[15] Nesta seção estamos usando $a, b, x, y \in 0, 1$.

3.8 Distribuição não-local de chaves criptográficas

"I couldn't help but overhear, probably because I was eavesdropping."

Eve

Em 1991, Artur Ekert trouxe as discussões filosóficas de realismo e localidade para o mundo prático. O protocolo E91 [55] explora a não-localidade quântica para garantir que duas partes se comuniquem com o conforto de saber que não existe uma terceira pessoa interceptando a conversa.

O ramo conhecido como *Criptografia Quântica* possui grande interesse prático[16]; vale notar artigo de revisão sobre criptografia quântica de Gisin *et al.* [57] é um dos mais citados de toda informação quântica.

O motivo de tanto interesse é que protocolos quânticos relacionados a criptografia têm sua segurança garantida por princípios físicos, e não simplesmente por limites tecnológicos, como os protocolos clássicos. Vamos agora exibir o E91:

Alice e Bob compartilham várias cópias do singleto[17](ver seção 3.2) $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, onde o primeiro qubit pertence a Alice e o segundo a Bob.

De forma aleatória, Alice vai realizar medições com os observáveis A_α e Bob com os observáveis B_β:

$$\begin{aligned} A_0 &= Z, & B_0 &= \frac{1}{\sqrt{2}}(X - Z); \\ A_1 &= \frac{1}{\sqrt{2}}(X + Z), & B_1 &= \frac{1}{\sqrt{2}}(X + Z); \\ A_2 &= X, & B_2 &= X. \end{aligned}$$

O processo é repetido um número grande de vezes, e ao final Alice terá uma coleção de inteiros $\{\alpha_i\}$, indicando sua escolha de observáveis, e uma coleção $\{a_i\}$ com o resultado das medições. Bob de maneira análoga obtém as coleções $\{\beta_i\}$ e $\{b_i\}$.

Os valores $\{\alpha_i\}$ e $\{\beta_i\}$ são divulgados sem se preocupar com um possível espião. Agora, Alice e Bob comparam os números α_i e β_i que pertencem ao conjunto $\{1, 2\}$. Devido as correlações do singleto, sempre que a igualdade $\alpha_i = \beta_i$ for satisfeita, temos $a_i \equiv b_i + 1 \mod 2$). Assim Alice e Bob têm uma coleção de bits perfeitamente (anti)correlacionados está criada a chave criptográfica[18].

De onde vem a segurança do E91? Alice e Bob podem estimar o valor de $\langle A_0 \otimes B_0\rangle$, $\langle A_0 \otimes B_1\rangle$, $\langle A_2 \otimes B_0\rangle$ e $\langle A_2 \otimes B_1\rangle$ e, com estes valores, construir uma desigualdade CHSH. O fato deles obterem $|\beta_{CHSH}| = 2\sqrt{2}$ garante que

[16] Com o curioso fato de existir um grupo de pesquisa séria conhecido como *Quantum Hacking* [56], que investiga possíveis falhas em implementações de protocolos de criptografia quântica.

[17] Poderíamos usar também qualquer outro estado maximamente emaranhado, mas para facilitar a argumentação, vamos explorar as propriedades do singleto.

[18] Para saber como usar esta chave para duas partes trocarem informação de forma completamente segura, o leitor pode procurar por *One Time Pad* [58].

não existe teoria realista local capaz de prever a chave. Ou seja, a chave é criada apenas quando Alice e Bob precisam se comunicar.

Poderíamos agora imaginar que um espião consiga obter alguma informação sobre a chave criptográfica, acoplando secretamente um terceiro qubit ao singleto. Mas, devido a monogamia da desigualdade de bell[19], o fato Alice e Bob obter $|\beta_{CHSH}| = 2\sqrt{2}$ garante que esse terceiro qubit não está correlacionado com o singleto.

3.9 A resposta da natureza

"No creo en brujas, pero que las hay, las hay..."

Ditado espanhol

A mecânica quântica tem uma validade experimental muito forte, seus postulados são bem consolidados e, como vimos neste capítulo, ela não é uma teoria realista local.

Podemos nos perguntar por experimentos que descrevem a desigualdade $CHSH$ sem mencionar mecânica quântica. De maneira ficamos aparte dos postulados e podemos perguntar à natureza se ela é realista local. Assim, resposta será dada pelo valor de β_{CHSH}, e não pelos postulados da quântica.

Experimentos que envolvem desigualdades de Bell são feitos desde 1982 [49] e indicam que sim, nosso mundo não é realista local. Porém, garantir que a montagem experimental seja equivalente aos experimentos teóricos propostos é complicado. Fato que dá margem para os chamados *loopholes*, que são os pontos onde o experimento real não simula exatamente o teórico.

Os *loopholes* podem ter diferentes naturezas e as mais comum são problemas de detecção e a garantia que as duas partes não vão se comunicar umas com as outras. Devido ao possíveis falhas[20], a busca por uma desigualdade de Bell que possa ser verificada experimentalmente ainda continua.

Recentemente Alain Aspect, que liderou vários experimentos de desigualdade de Bell, escreveu sobre a natureza ser ou não local [60]. O leitor interessado pela história e problemas dos experimentos de desigualdade de Bell pode buscar por [61].

[19] A monogamia da desigualdade de Bell afirma que se três partes A, B, C compartilham um estado quântico e as partes A e B violam maximamente uma desigualdade CHSH, C está necessariamente descorrelacionado do resto do sistema [59].

[20] Que para grande parte dos físicos é vista como simplesmente um problema de tecnologia.

Capítulo 4

Telepatia quântica

> All of you out there who believe in telepathy, raise your hand. All right. Now, everyone who believes in telekinesis... raise MY hand.
>
> Dennis Owens

Este capítulo vai se preocupar com jogos que exibem pseudotelepatia quântica[1]. Em 1999 Brassard e colaboradores mostraram que o emaranhamento pode ajudar duas partes realizarem tarefas impossíveis em teorias realistas locais [65]. O termo pseudotelepatia quântica surge de maneira explícita em 2003, em um trabalho que se preocupa em fazer com que muitas partes resolvam uma dada tarefa sem que haja comunicação entre elas [66].

Suponha que Alice e Bob participem de um jogo que pode ser facilmente vencido caso eles possam trocar informação. Carol, que acredita que o mundo é descrito por uma teoria realista local, analisa o jogo e percebe que, caso não haja comunicação entre as partes, eles não podem ganhar sempre.

Alice e Bob jogam um número muito grande de vezes e, para surpresa de Carol, vencem todas. Intrigada, esta conclui que telepatia é a única explicação plausível para tal acontecido.

Vamos mostrar que a não-localidade permite que duas (ou mais) partes realizem tarefas que não podem ser explicadas em um mundo realista local. Assim podemos desenvolver uma intuição maior das correlações quânticas, buscar por um experimento de desigualdade de Bell livre de *loopholes* e investigar os limites e consequências da não-localidade.

[1] A definição precisa de jogo será dada na próxima seção, mas podemos antecipar que não vamos usar a abordagem de teoria econômica, introduzida por Von Neumann e Morgenstern [62]. Vale notar que a extensão quântica desta teoria existe e permite, em algum sentido, resolver o dilema do prisioneiro [63], bem como criar um *contrato quântico* que previne os jogadores de aumentar seus *payoffs* com *traição* [64].

4.1 Definições

Definição 14. *Um jogo*[2] $G = (X, Y, W)$ *é um conjunto de inputs* $X = X^A \times X^B \times \ldots X^n$*, um conjunto de outputs* $Y = Y^A \times Y^B \times \ldots Y^n$ *e uma relação* $W \subseteq X \times Y$*. O número de jogadores é dado pela variável* $n \in \mathbb{Z}$*.*

Para poder falar em probabilidade de sucesso de uma estratégia, vamos assumir que os jogadores recebem seus inputs $x^i \in X^i$ *de acordo com uma distribuição de probabilidade uniforme*[3]*.*

Um caso particular importante é o de jogo bipartite, que são os jogos de $n = 2$, vamos usa-los para interpretar a ideia de um jogo. Alice recebe *input* $x^A \in X^A$, Bob recebe $x^B \in X^B$, e devem gerar respectivamente $y^A \in Y^A$ e $y^B \in Y^B$. Caso os *inputs* e *output*s satisfaçam a relação, *i.e.*: $(x^A, x^B, y^A, y^B) \in W$, eles vencem o jogo.

Uma estratégia é um protocolo para gerar *outputs*, uma estratégia vencedora é uma estratégia que vence o jogo para todo *input* X. Os jogos ficam interessantes se Alice e Bob tem acesso as regras (conjunto W) e podem fazer qualquer arranjo prévio, mas não podem se comunicar (trocar informação) depois que recebem seus *inputs*. Caso contrário eles poderiam simplesmente analisar toda a entrada, e gerar uma saída para satisfazer as condições de W.

Definição 15. *Uma estratégia determinística é aquela em que o input de todos jogadores são descritos pela função*

$$y^i : X^i \to Y^i.$$

Repare que as estratégias determinísticas capturam a ideia de realismo e localidade e, como consequência, não permitem que Alice saiba o *input* de Bob, *vice versa*.

Agora, podemos escrever a probabilidade máxima de sucesso de um jogo G dado por estratégias determinísticas:

$$\omega_D(G) = \max_{y^A,\ldots,y^n} \frac{\#\{(x^A,\ldots,x^n) \in X | (x^A,\ldots,x^n, y^A(x^A),\ldots,y^n(x^n)) \in W\}}{\#X}.$$

Outra ideia natural, é permitir que os jogadores tem acesso a um gerador de números aleatórios, assim eles podem sortear uma estratégia de acordo com o *input*.

Definição 16. *Uma estratégia probabilística é aquela em que dado seus inputs cada jogador pode utilizar uma distribuição de probabilidade* π^i *para escolher sua estratégia determinística.*

Então, a probabilidade máxima de sucesso usando uma estratégia probabilística é:

$$\omega_P(G) = \max_{\pi^1,\ldots,\pi^n} \sum_i \sum_{p_k \in \pi^i} p_k \omega_D$$

[2] Alguns autores gostam de obrigar que os jogadores só recebam bits como *inputs*, e definem jogo como $G = (X, Y, P, W)$, sendo P um conjunto de premissas que as relações dos *inputs* devem obedecer, *e.g.*, a soma dos *inputs* de todos jogadores é um número par. Porém, definir P não acrescenta em nada, já que todas as premissas podem ser incluídas em X.

[3] Poderíamos também permitir uma outra distribuição de probabilidade sobre os inputs, mas esta generalização não é muito interessante.

Teorema 13. $\omega_P = \omega_D$.

Demonstração. Basta notar que como π^i é uma distribuição de probabilidade, $\omega_P(G)$ é simplesmente uma combinação convexa arbitrária de ω_D. □

As estratégia determinísticas e probabilísticas são conhecidas como estratégias clássicas, veremos agora uma classe de estratégia que permite os participantes usarem não-localidade.

Definição 17. *Uma estratégia quântica é aquela que permite que os jogadores compartilhem um estado $|\psi\rangle \in \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \ldots \otimes \mathcal{H}^n$, com direito de usar operações e medições locais para gerar seus outputs.*

$$y^i : X^i \times O_i \to Y^i,,$$

onde O_i é o conjunto das medições locais feitas em $|\psi\rangle$, ou seja, medições feitas com os operadores $\{M_i : \mathcal{H}_k \to \mathcal{H}_k\}$.

Deve ficar claro que permitir que as partes usem medições em estados emaranhados não permite que as partes troquem informação, como vimos no teorema 7.

Entendendo D como o conjunto das estratégias determinísticas, P como o das probabilísticas e Q como o das quânticas, podemos verificar que para o caso de jogos com apenas um jogador temos $D \subseteq P = Q$, mas veremos que no caso de jogos bipartites $D \subseteq P \neq Q$. E a relação $P \neq Q$ é uma consequência do emaranhamento. E apesar de $D \subseteq P$, as estratégias probabilísticas não são mais vantajosas que as determinísticas (teorema 13).

Para os jogos bipartites, vamos definir também um outro tipo de estratégia, as estratégias PR, que consiste em permitir que Alice e Bob possuem uma maquina na qual eles entram com os bits a^A, a^B e recebem os bits z^A, z^B, satisfazendo as condições da caixa PR.

Definição 18. *Uma estratégia PR é aquela que permite Alice manipular o bit a^A, Bob manipular o bit a^B e usar uma caixa PR.*

$$y^A : X^A \times P_A \to Y^A, \quad y^B : X^B \times P_B \to Y^B,$$

com P_k sendo o conjunto dos resultados z_k da caixa PR, que garantem a relação $z^A + z^B = a^A.a^B$.

Permitir acesso a uma caixa PR ainda não permite que os participantes troquem informação, pois basta construir a caixa como foi feito na seção 3.7.

Vamos então a definição de pseudotelepatia quântica.

Definição 19. *Um jogo exibe pseudotelepatia quântica quando jogadores sempre podem vencer o jogo com uma estratégia quântica, mas não existe estratégia probabilística vencedora.*

4.2 O jogo do quadrado mágico

Baseado no quadrado de Mermim-Peres [67], o *Magic Square Game* foi introduzido em 2002 por Aravind [68] com o objetivo de provar o teorema de Bell sem necessitar de desigualdades[4]. Usaremos uma abordagem mais intuitiva [71, 72], na qual o jogo pode ser compreendido por meio de conceitos muito simples, sendo facilmente demonstrável que não existe uma estratégia clássica vencedora.

Vamos mostrar porém, que se permitimos que os participantes utilizem uma caixa não local ou compartilhem estados emaranhados, existe um protocolo que vence o jogo com certeza.

As regras do jogo são: Carol[5] sorteia (uniformemente) dois *inputs* x^A, x^B que pertencem ao conjunto $\{1,2,3\}$ e envia para Alice e Bob. Os jogadores devem, respectivamente, enviar para Carol os *outputs* $y^A = (y_1^A, y_2^A, y_3^A)$, $y^B = (y_1^B, y_2^B, y_3^B)$ com $y_k^i \in \{0,1\}$, ou seja, cada um envia 3 bits. Eles vencem o jogo se a soma dos bits de *output* da Alice for um número par, a soma dos do Bob for um número ímpar e a igualdade $y^A_{x^B} = y^B_{x^A}$ for satisfeita.

Perceba agora Alice e Bob podem usar uma matriz 3×3 para ganhar sempre, basta construir uma matriz na qual a soma dos elementos nas linhas é um número par, dos elementos nas colunas é impar, devemos entender o *input* de Alice como o número de uma linha e de Bob como o número de uma coluna. Com esta construção, fica claro também que condição do elemento de interseção linha/coluna ($y^A_{x^B} = y^B_{x^A}$) é sempre satisfeita, logo basta os jogadores combinarem esta matriz antes de receber seus *inputs* para ganhar sempre.

Esta matriz ganhou o nome de quadrado mágico por uma simples razão, ela não pode existir! Note que somando todos os 9 elementos utilizando o resultado das linhas, tem-se um número par; somando os 9 elementos utilizando o resultado das colunas, tem-se um número ímpar. Assim, a soma de todos seus elementos é um número par e ímpar.

Vamos formalizar a estrutura do jogo:

Definição 20 (Quadrado mágico)**.** *Alice e Bob recebem inputs uniformemente sorteados do conjunto $X^A = X^B = \{1,2,3\}$, e devem gerar outputs do conjunto $Y^A = Y^B = \{0,1\} \times \{0,1\} \times \{0,1\}$. As condições de vitória são dadas por W, que é definido são todos elementos que satisfazem as seguintes propriedades*[6]

$$\begin{aligned} y_1^A + y_2^A + y_3^A &= 0; \\ y_1^B + y_2^B + y_3^B &= 1; \\ y^A_{x^B} &= y^B_{x^A}. \end{aligned}$$

Teorema 14. *Restrito ao conjunto das estratégias probabilísticas, a probabilidade máxima de sucesso é* $8/9$.

[4] Apesar de parecer diferente em uma primeira análise, o jogo proposto em 2001 por Adán Cabello [69] é totalmente equivalente ao jogo do quadrado mágico(ver seção 4.5 de [70]).

[5] Esta terceira personagem está sendo usada apenas distribuir as entradas e avaliar se as condições de vitória foram satisfeitas, sendo seu papel dispensável em um discussão mais formal.

[6] Lembra que quando estivermos tratando de bits, vamos entender o sinal "+" como soma em $\mathbb{Z}_2$, ou seja, soma módulo 2.

Demonstração. Todas estratégias determinísticas vencedoras podem ser entendidas como uma matriz 3×3 combinada previamente. Como foi comentado antes, satisfazer a condição de paridade para toda linha e coluna da matriz é impossível. Logo, o melhor que eles podem fazer é combinar um protocolo que falha em uma das 9 possíveis combinações de entrada. Usando o teorema 13, vemos que a probabilidade máxima usando estratégias probabilísticas é $8/9$. □

0	0	0
0	0	0
1	1	?

Tabela 4.1: Ilustração do problema de criar uma matriz que sempre ganhe o jogo do quadrado mágico.

Teorema 15. *O jogo do quadrado mágico pode ser vencido com probabilidade 1 se os participantes tiverem direito de enviar 1 bit de informação.*

Demonstração. Alice e Bob combinam duas estratégias. A estratégia $S0$ consiste em montar um quadrado em que eles ganham para todo *input*, com exceção do caso $x^A = x^B = 3$. Já a estratégia $S1$ consiste em montar um quadrado no qual eles ganham quando $x^A = x^B = 3$ e perdem apenas para algum outro *input*.

Se Alice recebe $x^A \neq 3$, ela joga a estratégia $S0$ e envia o bit 0 para Bob, que deve jogar $S0$. Agora, se Alice recebe $x^A = 3$, ela joga a estratégia $S1$ e envia o bit 1 para Bob, que deve jogar $S1$. □

0	1	1
1	1	0
0	1	1

(a) Alice-$S0$

0	1	1
1	1	0
0	1	0

(b) Bob-$S0$

x	x	x
x	x	x
0	1	1

(c) Alice-$S1$

x	x	1
x	x	1
x	x	1

(d) Bob-$S1$

Figura 4.1: Exemplos de estratégias $S0$ e $S0$, Alice e Bob podem usar.

Teorema 16. *Existe uma estratégia que ganha o jogo com certeza quando os participantes compartilham 2 pares de qubits maximamente emaranhados.*

Demonstração. A prova será por construção. Alice e Bob compartilham o estado

$$|\psi\rangle = \frac{1}{2}(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle),$$

sendo os dois primeiros qubits da Alice e os outros do Bob[7]. Após receberem os *inputs* x^A e x^B, Alice e Bob aplicarão, respectivamente, A_{x^A} e B_{x^B} no seus qubits.

Para fazer contas e apresentar vetores/operadores de sistemas grandes, é interessante representá-los como matrizes. Basta definir

$$|00\rangle \equiv \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \quad |01\rangle \equiv \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \quad |10\rangle \equiv \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \quad |11\rangle \equiv \begin{bmatrix}0\\0\\0\\1\end{bmatrix},$$

entender aplicação de operador como produto de matrizes e o produto tensorial como produto de Kronecker[8].

Desta maneira, os operadores unitários são:

$$A_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} i & 0 & 0 & 1 \\ 0 & -i & 1 & 0 \\ 0 & i & 1 & 0 \\ 1 & 0 & 0 & i \end{bmatrix}, \; A_2 = \frac{1}{2}\begin{bmatrix} i & 1 & 1 & i \\ -i & 1 & -1 & i \\ i & 1 & -1 & -i \\ -i & 1 & 1 & -i \end{bmatrix}, \; A_3 = \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix};$$

$$B_1 = \frac{1}{2}\begin{bmatrix} i & -i & 1 & 1 \\ -i & -i & 1 & -1 \\ 1 & 1 & -i & i \\ -i & i & 1 & 1 \end{bmatrix}, \; B_2 = \frac{1}{2}\begin{bmatrix} -1 & i & 1 & i \\ 1 & i & 1 & -i \\ 1 & -i & 1 & i \\ -1 & -i & 1 & -i \end{bmatrix}, \; B_3 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix}.$$

Após aplicarem as operações unitárias, Alice e Bob devem medir seus qubits na base computacional, o que retorna 2 bits de informação para cada um. Agora, basta usarem os dois qubits para construir y^A e y^B, sendo o terceiro bit ajustado para satisfazer a regra da paridade.

Apesar de tedioso, verificar que este protocolo funciona para todo *input* x^A e x^B é trivial. Para exemplificar, vamos mostrar o resultado $x^A = 2$ e $x^B = 3$. Neste caso, Alice e Bob aplicarão, respectivamente, A_2 e B_3 para obter:

$$\begin{aligned} A_2 \otimes B_3|\psi\rangle = \frac{1}{2\sqrt{2}}(&|0000\rangle - |0010\rangle - |0101\rangle + |0111\rangle \\ &+|1001\rangle + |1011\rangle - |1100\rangle - |1110\rangle). \end{aligned}$$

Agora basta verificar que independente do resultado da medição, Alice e Bob vão ganhar o jogo.

□

Teorema 17. *Os participantes podem vencer o jogo com apenas um uso da caixa PR.*

Demonstração. Alice constrói o conjunto de estratégias $\{A0,A1\}$ e Bob constrói $\{B0,B1\}$, de tal maneira que as estratégias representem as seguintes condições:

[7] É interessante explicitar que este estado não é nada mais do que Alice e Bob compartilhando dois qubits maximamente emaranhados $|\beta_{11}\rangle$. Podemos escrever $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_C - |1\rangle_A|0\rangle_C) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_D - |1\rangle_B|0\rangle_D)$, com os índices A, B, C e D usados para enumerar os qubits na ordem em que $|\psi\rangle$ foi apresentado.

[8] O produto de Kronecker uma matriz A $(n \times m)$, e uma B $(p \times q)$, é feito multiplicado cada elemento da matriz A pela matriz B, $A \otimes B \equiv \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$.

- $A0$ e $A1$ satisfazem $y_3^A = y_1^A + y_2^A$;
- $B0$ e $B1$ satisfazem $y_3^B = y_1^B + y_2^B + 1$;
- Os pares ($A0$,$B0$) e ($A1$,$B1$) tem $y_{x^B}^A = y_{x^A}^B$ exceto quando $x^A = x^B = 3$;
- Os pares ($A0$,$B1$) e ($A1$,$B0$) tem $y_3^A = y_3^B$.

Agora, Alice e Bob vão usar a caixa PR para decidir qual estratégia devem adotar. Caso eles recebam *input* 3, colocarão 1 na caixa, caso contrário, entram com 0. Sejam z^A e z^B os *outputs* que Alice e Bob recebem da caixa. Basta agora usarem a estratégia Az^A e Bz^B.

Perceba que no caso $x^A = x^B = 3$, eles receberão bits que respeitam $z^A = z^B + 1$. Caso contrario vão receber bits que respeitam $z^A = z^B$.

□

0	1	1
1	1	0
0	1	1

(a) Alice-$A0$

0	1	1
1	1	0
0	1	0

(b) Bob-$B0$

1	1	0
0	0	0
0	0	0

(c) Alice-$A1$

1	1	0
0	0	0
0	0	1

(d) Bob-$B1$

Figura 4.2: Exemplo de estratégias $\{A0,A1\}$ e $\{B0,B1\}$ Alice e Bob podem usar.

4.3 Extensões do jogo do quadrado mágico

Ao invés de imaginar um quadrado 3×3, podemos propor um quadrado $n \times n$. É simples mostrar que, para todo n par, temos uma estratégia clássica vencedora, já que é trivial construir uma matriz que satisfaça a condição de paridade[9].

Mas o que pode ser dito sobre as dimensões ímpares? Este problema é explorado em [73] e os resultados são que, assim como no caso $n = 3$, Alice e Bob tem uma estratégia vencedora compartilhando dois pares de qubits emaranhados, ou usando uma caixa PR.

Porém, é fácil verificar que uma estratégia clássica vence o jogo com $p = 1 - 1/n^2$. Basta construir uma matriz análoga à tabela 4.1. Logo, aumentar o quadrado não é interessante, pois isto "aproxima" o caso quântico do clássico.

A robustez do quadrado mágico é explorada em [74], onde os autores discutem a probabilidade de sucesso em função de um possível ruído[10]. A conclusão é que verificar experimentalmente a vantagem da estratégia quântica é bem difícil, pois um pouco de ruído já faz com que probabilidade de sucesso seja menor que 8/9.

[9] Tome uma que matriz tenha 1 em todos elementos da última linha e 0 nas outras entradas.

[10] Foram levados em consideração os efeitos de reservatórios sujeitos a depolarização, *amplitude damping*, *phase flip*, *bit flip* e *bit phase flip*.

4.4 Jogo GHZ: emaranhamento multipartite

Nesta seção vamos explorar o emaranhamento multipartite no jogo GHZ [75], inspirado na simplificação feita por Mermim [76] do trabalho original de Greenberger, Horne e Zeilinger [77].

O jogo GHZ com n partes é definido como:

Definição 21 (GHZ). *Cada jogador i recebe de input um bit $x^i \in X^i = \{0,1\}$ e deve gerar de output um bit $y^i \in Y^i = \{0,1\}$. Eles ganham se a soma dosinputs for um ímpar, ou se a quantidade de* 1*s nos outputs for congruente a metade dos* 1*s nos inputs módulo* 2*,*

$$W = \left\{ x^i \in X^i, y^i \in Y^i \middle| \left(\sum_i^n x^i = 1 \right) \text{ ou } \left(\sum_i^n y^i \equiv \frac{\#\{x^i \in X^i | x^i = 1\}}{2} \right) \mod 2 \right\}.$$

O jogo GHZ é interessante com $n \geq 3$, pois nesta situação não temos uma estratégia clássica vencedora.

Teorema 18. *Não existe estratégia clássica vencedora para o jogo GHZ quando $n \geq 3$.*

Demonstração. A demonstração de uma versão mais forte deste teorema pode ser encontrada em [75][11]. Vamos exibir uma demonstração elegante para o caso $n = 3$.

Uma estratégia clássica vencedora deve satisfazer:

$$\begin{aligned} y^A(0) + y^B(0) + y^C(0) &= 0; \\ y^A(0) + y^B(1) + y^C(1) &= 1; \\ y^A(1) + y^B(0) + y^C(1) &= 1; \\ y^A(1) + y^B(1) + y^C(0) &= 1. \end{aligned}$$

Somando as 4 equações temos $0 = 1$, que é um absurdo. Logo, não existe estratégia clássica vencedora. □

Teorema 19. *Sempre existe uma estratégia quântica vencedora para participantes que começam com o estado $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$.*

Demonstração. Para que os jogadores vençam, basta usarem a estratégia descrita:

1. Se o jogador tem $x_i = 1$, ele deve aplicar $S = |0\rangle\langle 0| + i|1\rangle\langle 1|$ no seu qubit.
2. Todos jogadores aplicam H no seus qubits.
3. Os jogadores medem seu qubit na base computacional e atribuem o valor do resultado no seu *output* y^i.

[11] Da maneira que foi apresentado o jogo GHZ aqui, a melhor estratégia clássica vence o jogo com $p = 1/4 + 2^{-\lceil n/2 \rceil - 1}$, onde $\lceil n/2 \rceil$ o número inteiro pertencente ao intervalo $[n/2, (n+1)/2]$.

Nos resta agora verificar que o protocolo resulta em uma estratégia vencedora.

Se $\sum_i^n x^i = 1$, não há o que verificar. Se a metade da soma nos inteiros dos inputs é par, é fácil verificar que o estado final após a etapa 1 será o próprio $|GHZ\rangle$. Então, após aplicar H, temos:

$$H^{\otimes n}|GHZ\rangle = \frac{1}{\sqrt{2}}(H^{\otimes n}|0\rangle^{\otimes n} + H^{\otimes n}|1\rangle^{\otimes n}.)$$

Para facilitar a demonstração, faremos um certo abuso de notação ao escrever os estados quânticos como números inteiros e entende-los como a expansão binária. Por exemplo em um sistema de 4 qubits, $|3\rangle = |0010\rangle$. Vamos usar também a função distância de Hamming $\Delta(a)$ que conta a quantidade de 1s contida no número a quando escrito na base 2.

$$\begin{aligned} H^{\otimes n}|GHZ\rangle &= \frac{1}{\sqrt{2}}\left(\frac{\sum_{a=0}^{2^n-1}|a\rangle}{\sqrt{2^n}} + \frac{\sum_{a=0}^{2^n-1}(-1)^{\Delta(a)}|a\rangle}{\sqrt{2^n}}\right) \\ &= \frac{1}{\sqrt{2^{n+1}}}\left(\sum_{a=0}^{2^n-1}(1+(-1)^{\Delta(a)})\right)|a\rangle \\ &= \frac{1}{\sqrt{2^{n-1}}}\sum_{\Delta(a)\ \text{par}}|a\rangle. \end{aligned}$$

Assim verificamos que, independente do resultado que cada parte individual obtiver, sempre teremos um número $a = \sum_i^n y^i = 0$.

Se a metade da soma nos inteiros dos inputs é ímpar, o estado após a etapa 1 será

$$|GHZ_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} - |1\rangle^{\otimes n}).$$

Após cada parte aplicar H em seu qubit, o sistema passa a ser descrito por:

$$H^{\otimes n}|GHZ\rangle = \frac{1}{\sqrt{2^{n-1}}}\sum_{\Delta(a)\ \text{ímpar}}|a\rangle,$$

e as medições vão sempre satisfazer $a = \sum_i^n y^n = 1$. □

Existe também um resultado interessante que relaciona o jogo GHZ com a verificação experimental da não-localidade quântica. Em uma versão estendida, onde os participantes recebem l bits cada um, pode-se mostrar [78] que, mesmo com detectores de eficiência arbitrariamente próxima de zero, é possível obter pseudotelepatia quântica. Basta ajustar os parâmetros n e l.

4.5 Recurso mínimo para a pseudotelepatia quântica

Em [79], Brassard *et al.* perguntaram qual o recurso mínimo para a existência de pseudotelepatia quântica. No mesmo trabalho, demonstraram se dois jogadores compartilham um estado $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ e $\dim(\mathcal{H}_a) = 2$,[12] ela

[12] Lembrando que $\dim(\mathcal{H})$ é o número de vetores linearmente em $\mathcal{H}$.

não pode existir. Em especial se Alice e Bob compartilham apenas um par de qubits, eles não é possível construir um jogo que exiba pseudotelepatia quântica.

Teorema 20. *Não existe jogos bipartites que exibem pseudotelepatia quântica com caso os participantes possuam apenas um par de qubits.*

Demonstração. Vamos utilizar as ideias do teorema apresentada em [79]. Porém vamos assumir que os jogadores começam com o estado singleto, e vão medir apenas observáveis unitários, assim construímos toda a ideia do teorema de maneira mais limpa, sem precisar fazer contas grandes e carregar muitas variáveis.

Suponha o jogo $G = (X^A, X^B, Y^A, Y^B, W)$ que admite pseudotelepatia quântica com duas partes que compartilham o estado $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, e tem a sua disposição observáveis da forma $\mathbf{n} \cdot \sigma$.

Nós vamos exibir uma estratégia clássica que também ganha este jogo para criar um absurdo[13]. Esta estratégia clássica não precisa simular as correlações quânticas[14], só precisamos de uma maneira esperta de usar o resultado de uma medição quântica, sem de fato efetuar a medição.

Como Alice e Bob devem usar observáveis unitários, eles vão usar seus *inputs* para escolher vetores $\mathbf{a}$ e $\mathbf{b}$, o depois utilizar o resultado da medição com o observável $(\mathbf{a} \cdot \sigma) \otimes (\mathbf{b} \cdot \sigma)$ para criar seus outputs.

Os possíveis resultados das medições têm as probabilidades dadas por[15]:

$$p(\mathbf{a}_+, \mathbf{b}_+) = \frac{1}{2}\operatorname{sen}^2\left(\frac{\theta_{ab}}{2}\right), \quad p(\mathbf{a}_+, \mathbf{b}_-) = \frac{1}{2}\cos^2\left(\frac{\theta_{ab}}{2}\right);$$
$$p(\mathbf{a}_-, \mathbf{b}_+) = \frac{1}{2}\cos^2\left(\frac{\theta_{ab}}{2}\right), \quad p(\mathbf{a}_-, \mathbf{b}_-) = \frac{1}{2}\operatorname{sen}^2\left(\frac{\theta_{ab}}{2}\right).$$

Sempre que $p(i,j) \neq 0$, o resultado da medição quântica pode ser usado para construir uma estratégia clássica vencedora. E vamos ter $p(i,j) = 0$ somente quando $\theta_{ab} = 0$, ou $\theta_{ab} = \pi$, que são os casos em que os resultados estão perfeitamente correlacionados, ou perfeitamente anti-correlacionados. Então, basta Alice e Bob combinarem: quando os *inputs* forem utilizados para construir vetores com angulo $\theta_{ab} = 0$, eles usam resultados perfeitamente correlacionados para gerar seus outputs, quando os *inputs* forem utilizados para construir vetores com angulo $\theta_{ab} = \pi$ eles usam resultados perfeitamente anti-correlacionados. Dessa maneira eles constroem uma estratégia clássica, sem precisar efetuar a medição.

□

Teorema 21. *Todo jogo que com pseudotelepatia quântica em espaço de estados de dimensão $d_A \times d_B$, também exibe em um espaço de estados de dimensão $d \times d$, onde $d = \min(d_A, d_B)$.*

[13] Por definição, jogos de pseudotelepatia quântica não admitem uma estratégia vencedora clássica.

[14] O que seria impossível, devido a não-localidade quântica.

[15] Estas são as mesmas probabilidades para a desigualdade de Wigner, seção 3.3

Demonstração. Segue decomposição de Schmidt (seção 1.9) que, qualquer estado do sistema de dimensão $d_A \times d_B$ pode ser escrito como $\sum_i^d \lambda_i |A_i\rangle|B_i\rangle$, com $d = \min(d_A, d_B)$. Logo, Alice e Bob, não precisam de usar as partes do seu sistema que possui dimensões maiores que d. □

Como corolário, não existe pseudotelepatia quântica caso dois jogadores compartilhem um estado $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ e $\dim(\mathcal{H}_a) = 2$. Assim vemos que a pseudotelepatia quântica exige mais recurso do que uma simples demonstração de não-localidade, no capítulo 3 vimos maneiras de detectar a não-localidade quântica que usam apenas um par de qubits emaranhados.

Uma conclusão é que a menor dimensão do espaço de estados para jogos bipartites que exibe pseudotelepatia quântica é 3×3, e existe um jogo que cada parte tem um sistema de três níveis, e o jogo de Kochen-Specker satisfaz esta propriedade [71, 80]. Vemos também que o jogo GHZ com 3 jogadores usa um espaço de estados de dimensão total $2 \times 2 \times 2 = 8$, e é a dimensão mínima em que podemos ter pseudotelepatia.

Capítulo 5

Complexidade de comunicação

Mergulhado num contexto de informação clássica Yao, em 1979 [81], encontrou alguma maneira de quantificar a informação que duas (ou mais) partes precisam trocar para concluir uma tarefa em comum. Ramo que ficou conhecido como complexidade de comunicação.

Os capítulos anteriores nos sugerem que permitir não-localidade vai reduzir a complexidade de comunicação para algumas situações.

5.1 Definições

O problema pode ser encarado da seguinte forma: quantos bits Alice e Bob precisam trocar para computar a função $f : A \times B \to Z$, onde Alice tem acesso apenas aos elementos de A e Bob apenas os elementos de B.

Vamos nos restringir as funções de decisão, que são as funções onde $A = B = \{0,1\}^n$ e $Z = \{0,1\}$, com $n \in \mathbb{N}$.

Definição 22. *Seja $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, onde os primeiros n bits, $\vec{a} = (a_1, \ldots, a_n)$ pertencem a parte A, e os outros n bits, $\vec{b} = (b_1, \ldots, b_n)$ parte B.*

A complexidade de comunicação (CC) da função f é o número mínimo de bits(clássicos) que as partes precisam trocar para que A possa ter certeza do valor de $f(\vec{a}, \vec{b})$ para qualquer entrada $(\vec{a}, \vec{b}) \in \{0,1\}^n \times \{0,1\}^n$.

Perceba que a complexidade de comunicação é dada pelo *pior caso*. Pois ela é calculada sem assumir *a priori* que as partes têm um $(\vec{a}, \vec{b})$ específico.

Fica implícito na definição acima que as partes não podem usar o resultado de medições quânticas nem de caixas PR no processo de computar f. A notação usual é sempre avisar quando permitir o uso de não-localidade.

5.2 Complexidade de comunicação com emaranhamento

Em 1997, Buhrman, Cleve e van Dam publicaram um trabalho que relaciona o emaranhamento com a complexidade de comunicação [82]. Eles mostraram que se Alice e Bob ficarem satisfeitos em acertar a função com uma certa probabilidade p, então pode-se exibir uma função que possui menor complexidade de comunicação quando as partes compartilham previamente qubits

emaranhados. Vale notar que, no mesmo artigo de 1997, foi mostrado que se 3 partes querem computar uma função, temos situações que o uso de emaranhamento de fato reduz a CC, nos indicando novamente que o emaranhamento multipartite é de alguma maneira "mais poderoso" que o bipartite. Em sua tese[83], van Dam explorou a função produto interno[1],

$$IP(\vec{a},\vec{b}) = \sum_{i}^{n} a_i.b_i,$$

e mostrou as "vantagens quânticas" quando não exigimos $p = 1$.

Porém, se Alice e Bob querem o valor de $f(\vec{a},\vec{b})$ com $p = 1$, não sabemos de um caso em que o uso de emaranhamento resulte em um protocolo mais eficiente. Vamos ver na próxima seção que se permitimos "mais não-localidade", a situação é diferente.

5.3 Consequência de uma não-localidade supra-quântica

Nesta seção, vamos provar um teorema que ficou conhecido como "O uso de caixas PR trivializa a comunicação". Para este resultado fazer sentido, vamos enunciar um teorema no qual a demonstração pode ser encontrada em [84] ou [85].

Teorema 22. *A função* $IP : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, $IP(\vec{a},\vec{b}) = \sum_i^n a_i.b_i$ *tem* $CC = n$.

E o resultado do teorema continua valendo quando permitimos que as partes usem o emaranhamento quântico[83], a função produto interno ainda possui[2] $CC = n$.

Agora vamos provar um lema que vai relacionar toda função decisão com a função produto interno.

Lema 1. *Toda função* $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *pode ser escrita como*

$$\sum_{i=1}^{2^n} P_i(\vec{a})Q_i(\vec{b}),$$

onde p *são polinômios em* $\vec{a} \in \{0,1\}^n$ *e* Q *são monômios em* $\vec{b} \in \{0,1\}^n$

Demonstração. Primeiro note que qualquer função decisão pode ser escrita como polinômios em várias variáveis usando produto e soma módulo 2. Agora vamos colocar em evidência todos os monômios Q_i que dependem de $\vec{b}$, definindo implicitamente os polinômios p_i, que dependem apenas de $\vec{a}$:

$$f(\vec{a},\vec{b}) = \sum_{i} P_i(\vec{a})Q_i(\vec{b}).$$

[1] Lembrando que, como estamos trabalhando apenas com bits, toda soma será entendida como soma em elementos de $\mathbb{Z}_2$, ou seja, soma módulo 2.

[2] Vale ressaltar que para funções do tipo decisão, sempre temos $CC \leq n$. Basta Bob enviar todos os seus n bits.

Então precisamos apenas contar quantos monômios Q_i podem existir. Sabemos que estes monômios podem ter a forma $Q_i = b_1^{k_1} b_2^{k_2} \dots b_n^{k_n}$, onde cada k_j pode assumir dois valores, 0 ou 1. Assim, podemos ter 2^n monômios diferentes. Logo

$$f(\vec{a},\vec{b}) = \sum_{i=1}^{2^n} P_i(\vec{a}) Q_i(\vec{b}).$$

□

Podemos agora provar o resultado principal, que foi apresentado por van Dam em [83, 86].

Teorema 23. *Se Alice e Bob possuem uma caixa de Popescu Rohrlich, qualquer função decisão f possui CC igual a 1.*

Demonstração. Vamos escrever f como:

$$f(\vec{a},\vec{b}) = \sum_{i}^{2^n} P_i(\vec{a}) Q_i(\vec{b}).$$

Alice e Bob entram com os bits $p_i(\vec{a})$ e $Q_i(\vec{b})$ na caixa PR para obter α_i e β_i que satisfazem $P_i(\vec{a}).Q_i(\vec{b}) = \alpha_i + \beta_i$. Assim temos:

$$\sum_{i}^{2^n}(\alpha_i + \beta_i) = (\sum_{i}^{2^n}\alpha_i) + (\sum_{i}^{2^n}\beta_i).$$

Repare agora que Bob pode somar os bits β_i sem precisar comunicar com Alice. Basta agora ele enviar o bit $\sum_i^{2^n} \beta_i$, para que Alice possa calcular $f(\vec{a},\vec{b})$. □

Concluímos então que se Alice e Bob compartilham uma caixa PR, toda função decisão pode ser avaliada com apenas um bit de comunicação! Brassard *et al.*[87] demonstraram que qualquer teoria que permite simulações de uma caixa PR com probabilidade maior que $\frac{3+\sqrt{6}}{6} \approx 0{,}908$, é suficiente para que a comunicação seja trivial[3].

Uma pergunta natural é: "Exatamente quanta de não-localidade precisamos para que a comunicação seja trivial?". Apesar de alguns resultados relacionados, este ainda é um problema em aberto.

[3]Para efeito de comparação, a mecânica quântica simula as caixas PR com probabilidade $\frac{2+\sqrt{2}}{4} \approx 0{,}854$. Já teorias realistas locais simulam com probabilidade igual 0,75.

Bibliografia

[1] E. Schrödinger. "Discussion of Probability Relations between Separated Systems". *Mathematical Proceedings of the Cambridge Philosophical Society* **31**, 04 (1935), pp. 555–563.

[2] C. E. Shannon. "A mathematical theory of communication". *Bell system technical journal* **27** (1948).

[3] Vlatko Vedral. *Introduction to Quantum Information Science*. Oxford University Press, 2007.

[4] George B. Dyson. *Darwin Among The Machines: The Evolution Of Global Intelligence*. Basic Books, 1997.

[5] Thomas M. Cover e Joy A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 2006.

[6] Michael A. Nielsen e Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[7] Benenti *et al. Principles of quantum computation and information*. World Scientific Publishing Co Pte Ltd, 2004.

[8] Asher Peres. *Quantum Theory: Concepts and Methods*. Springer, 1995.

[9] Claude Cohen-Tannoudji, Bernard Diu e Franck Laloe. *Quantum Mechanics*. Wiley, 1977.

[10] Marcelo O. Terra Cunha. *Noções de Informação Quântica*. IMPA, 2007.

[11] Paul M. Dirac. *Principles of Quantum Mechanics*. Oxford University Press, 1930.

[12] Michael Reed e Barry Simon. *Methods of modern mathematical physics: Functional Analysis*. Academic Press, 1970.

[13] М. А. Наймарк. "Спектральные функции симметрического оператора". *Изв. АН СССР. Сер. матем.* **4:3** (1940), 277–318. URL: http://83.149.209.141/php/archive.phtml?wshow=paper&jrnid=im&paperid=3893&option_lang=rus.

[14] John Preskill. *Lecture Notes - Quantum Information and Computation*. URL: http://www.theory.caltech.edu/people/preskill/ph229/notes/chap3.pdf.

[15] V. Vedral *et al.* "Quantifying Entanglement". *Physical Review Letters* **78** (1997), pp. 2275–2279. arXiv:quant-ph/9702027.

[16] R. Horodecki *et al.* "Quantum entanglement". (2007). arXiv:quant-ph/0702225.

[17] Bárbara Lopes Amaral. "Emaranhamento em sistemas de dois qubits". Diss. de mestrado. UFMG, 2010.

[18] Erhard Schmidt. "Zur Theorie der linearen und nichtlinearen Integralgleichungen. 1. Entwicklung willküriger Funktionen nach Systemevorgeschriebener". *Mathematische Annalen* **63** (4 1907), pp. 433–476.

[19] Artur Ekert e Peter L. Knight. "Entangled quantum systems and the Schmidt decomposition". *Am. J. Phys.* **63**, 5 (1995), pp. 415–423.

[20] URL: http://en.wikipedia.org/wiki/Singular_value_decomposition.

[21] S. Popescu e D. Rohrlich. "Thermodynamics and the measure of entanglement". *Physical Review A* **56** (1997), pp. 3319–+. arXiv:quant-ph/9610044.

[22] V. Vedral e E. Kashefi. "Uniqueness of Entanglement Measure and Thermodynamics". *ArXiv Quantum Physics e-prints* (2001). eprint: arXiv:quant-ph/0112137.

[23] A. Acín *et al.* "Generalized Schmidt Decomposition and Classification of Three-Quantum-Bit States". *Physical Review Letters* **85** (2000), pp. 1560–1563. arXiv:quant-ph/0003050.

[24] W.K. Wootters e W.H. Zurek. "A Single Quantum Cannot be Cloned". *Nature*, 299 (1982), 802–803.

[25] John von Neumann. *Mathematical Foundations of Quantum Mechanics*. Beyer, R. T., 1932.

[26] A. Peres. "How the no-cloning theorem got its name". *Fortschritte der Physik* **51** (2003), pp. 458–461. arXiv:quant-ph/0205076.

[27] E. Knill *et al.* "Introduction to Quantum Error Correction". (2002). arXiv:quant-ph/0207170.

[28] *Quantum Cryptography: Public key distribution and coin tossing*. Proceedings of the IEEE International Conference on Computers, Systems, e Signal Processing, Bangalore, 1984.

[29] Stephen Wiesner. "Conjugate coding". *SIGACT News* **15**, 1 (1983), pp. 78–88. ISSN: 0163-5700.

[30] Douglas Stebila e Michele Mosca. *Uncloneable Quantum Money*. URL: www.iqis.org/events/cqisc06/papers/Mon-1130-Stebila.pdf.

[31] Ll. Masanes, A. Acin e N. Gisin. "General properties of nonsignaling theories". *Phys. Rev. A* **73**, 1 (2006), p. 012112.

[32] Carl W. Helstrom. "Quantum detection and estimation theory". *Journal of Statistical Physics* **1** (2 1969), pp. 231–252. ISSN: 0022-4715.

[33] А. С. Холево. "Некоторые оценки для количества информации, передаваемого квантовым каналом связи ". *Изв. АН СССР. Сер. матем.* **9:3** (1973), 3–11. URL: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi&paperid=903&option_lang=rus.

[34] Charles H. Bennett e Stephen J. Wiesner. "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". *Phys. Rev. Lett.* **69**, 20 (1992), pp. 2881–2884.

[35] V. Vedral. "The role of relative entropy in quantum information theory". *Reviews of Modern Physics* **74** (2002), pp. 197–234. arXiv:quant-ph/0102094.

[36] Charles H. Bennett *et al.* "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". *Phys. Rev. Lett.* **70**, 13 (1993), pp. 1895–1899.

[37] URL: http://www.xkcd.com/465.

[38] R. Cleve *et al.* "Quantum Entanglement and the Communication Complexity of the Inner Product Function". (1997). arXiv:quant-ph/9708019.

[39] A. Einstein, B. Podolsky e N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Phys. Rev.* **47**, 10 (1935), pp. 777–780.

[40] Marco Túlio Coelho Quintino e Mateus Santos Araújo. *Desigualdades de Bell: Uma introdução à não-localidade quântica*. 2010. URL: http://www.mat.ufmg.br/~tcunha/Bell-Mateus-MTulio.pdf.

[41] E. Schrödinger. "Die gegenwärtige Situation in der Quantenmechanik". *Naturwissenschaften* **23** (48 1935), pp. 807–812. ISSN: 0028-1042.

[42] N. Bohr. "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?" *Phys. Rev.* **48**, 8 (1935), pp. 696–702.

[43] J. S. Bell. "On the Einstein-Poldolsky-Rosen paradox". *Physics* (1964).

[44] Rafael Luiz da Silva Rabelo. "Não-localidade quântica: matemática e fundamentos". Diss. de mestrado. UFMG, 2010.

[45] D. Rohrlich e S. Popescu. "Nonlocality as an axiom for quantum theory". (1995). arXiv:quant-ph/9508009.

[46] J. S. Bell. "Bertlmann's socks and the nature of reality". *Journal de Physique Colloques* (1981).

[47] Eugene P. Wigner. "On Hidden Variables and Quantum Mechanical Probabilities". *Am. J. Phys.* (1970). URL: http://dx.doi.org/10.1119/1.1976526.

[48] John F. Clauser *et al.* "Proposed Experiment to Test Local Hidden-Variable Theories". *Phys. Rev. Lett.* **23**, 15 (1969), pp. 880–884.

[49] Alain Aspect, Philippe Grangier e Gérard Roger. "Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities". *Phys. Rev. Lett.* **49**, 2 (1982), pp. 91–94.

[50] B. S. Cirel'son. "Quantum generalizations of Bell's inequality". *Lett. Math. Phys.* **4**, 2 (1980), pp. 93–100. ISSN: 0377-9017.

[51] Benjamin Francis Toner. "Quantifying Quantum Nonlocality". Tese de doutorado. 2007.

[52] B. S. Cirel'son. Comunicação particular. 2010.

[53] N. Gisin. "Bell's inequality holds for all non-product states". *Physics Letters A* **154**, 5-6 (1991), pp. 201 –202. ISSN: 0375-9601.

[54] M. Li e S.-M. Fei. "Gisin's Theorem for Arbitrary Dimensional Multipartite States". *Physical Review Letters* **104**, 24 (2010), pp. 240502–+. arXiv:1006.3557 [quant-ph].

[55] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". *Phys. Rev. Lett.* **67**, 6 (1991), pp. 661–663.

[56] URL: http://www.iet.ntnu.no/groups/optics/qcr/.

[57] N. Gisin *et al.* "Quantum cryptography". *Reviews of Modern Physics* **74** (2002), pp. 145–195. arXiv:quant-ph/0101098.

[58] URL: http://en.wikipedia.org/wiki/One-time_pad.

[59] B. Toner e F. Verstraete. "Monogamy of Bell correlations and Tsirelson's bound". (2006). arXiv:quant-ph/0611001.

[60] Alain Aspect. "Quantum mechanics: To be or not to be local". *Nature* **446** (2007), 866–867.

[61] URL: http://en.wikipedia.org/wiki/Bell_test_experiments.

[62] John von Neumann e Oskar Morgenstern. *Theory of Games and Economic Behavior*. Princeton University Press, 1994.

[63] J. Eisert e M. Wilkens. "Quantum games". *Journal of Modern Optics* **47** (2000), pp. 2543–2556. arXiv:quant-ph/0004076.

[64] Simon C. Benjamin e Patrick M. Hayden. "Multiplayer quantum games". *Phys. Rev. A* **64**, 3 (2001), p. 030301.

[65] G. Brassard, R. Cleve e A. Tapp. "Cost of Exactly Simulating Quantum Entanglement with Classical Communication". *Physical Review Letters* **83** (1999), pp. 1874–1877. eprint: arXiv:quant-ph/9901035.

[66] G. Brassard, A. Broadbent e A. Tapp. "Multi-Party Pseudo-Telepathy". (2003). arXiv:quant-ph/0306042.

[67] N. David Mermin. "Hidden variables and the two theorems of John Bell". *Rev. Mod. Phys.* **65**, 3 (1993), pp. 803–815.

[68] P. K. Aravind. "Bell's theorem without inequalities and only two distant observers". (2001). arXiv:quant-ph/0104133.

[69] Adán Cabello. ""All versus Nothing" Inseparability for Two Observers". *Phys. Rev. Lett.* **87**, 1 (2001), p. 010403.

[70] Anne Lise Broadbent. "Quantum Pseudo-Telepathy Games". Diss. de mestrado. Université de Montréal, 2010.

[71] G. Brassard, A. Broadbent e A. Tapp. "Quantum Pseudo-Telepathy". *Foundations of Physics* **35** (2005), pp. 1877–1907. arXiv:quant-ph/0407221.

[72] A. Broadbent e A. A. Methot. "On the power of non-local boxes". (2005). arXiv:quant-ph/0504136.

[73] S. Kunkri *et al.* "Winning strategies for pseudo-telepathy games using single non-local box". (2006). arXiv:quant-ph/0602064.

[74] P. Gawron, J. A. Miszczak e J. Sladkowski. "Noise Effects in Quantum Magic Squares Game". (2008). arXiv:0801.4848 [quant-ph].

[75] G. Brassard, A. Broadbent e A. Tapp. "Recasting Mermin's multi-player game into the framework of pseudo-telepathy". (2004). arXiv:quant-ph/0408052.

[76] N. David Mermin. "What's Wrong with these Elements of Reality?" *Physics Today* **43**, 6 (1990), pp. 9–11.

[77] Daniel M. Greenberger *et al.* "Bell's theorem without inequalities". *American Journal of Physics* **58**, 12 (1990), pp. 1131–1143.

[78] H. Buhrman *et al.* "Combinatorics and Quantum Nonlocality". *Physical Review Letters* **91**, 4 (2003). arXiv:quant-ph/0209052.

[79] G. Brassard, A. A. Methot e A. Tapp. "Minimum entangled state dimension required for pseudo-telepathy". (2004). arXiv:quant-ph/0412136.

[80] R. Cleve *et al.* "Consequences and Limits of Nonlocal Strategies". *ArXiv Quantum Physics e-prints* (2004). eprint: arXiv:quant-ph/0404076.

[81] Andrew Chi-Chih Yao. "Some complexity questions related to distributive computing(Preliminary Report)". *STOC '79: Proceedings of the eleventh annual ACM symposium on Theory of computing*. New York, NY, USA: ACM, 1979, pp. 209–213.

[82] H. Buhrman, R. Cleve e W. van Dam. "Quantum Entanglement and Communication Complexity". (1997). arXiv:quant-ph/9705033.

[83] W. van Dam. "Nonlocality and Communication Complexity". Tese de doutorado. 1999.

[84] Eyal Kushilevitz e Noam Nisan. *Communication complexity*. Cambridge University Press, 1997.

[85] Eyal Kushilevitz. "Communication Complexity". Ed. por Marvin V. Zelkowitz. Vol. 44. Advances in Computers. Elsevier, 1997, pp. 331 – 360. URL: http://www.sciencedirect.com/science/article/B7RNF-4S81S3X-C/2/127b01522317f54a78333a7e4e72c39d.

[86] W. van Dam. "Implausible Consequences of Superstrong Nonlocality". (2005). arXiv:quant-ph/0501159.

[87] G. Brassard *et al.* "Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial". *Physical Review Letters* **96**, 25 (2006). arXiv:quant-ph/0508042.