Yuri Jaloto Santos Machado

Computação quântica e o cassino quântico

Niterói-RJ

Ficha catalográfica automática - SDC/BIF
Gerada com informações fornecidas pelo autor

M149c Machado, Yuri Jaloto Santos
Computação quântica e o cassino quântico / Yuri Jaloto Santos Machado. - 2022.
44 f.

Orientador: Daniel Jost Brod.
Trabalho de Conclusão de Curso (graduação)-Universidade Federal Fluminense, Instituto de Física, Niterói, 2022.

1. Contextualidade. 2. Não localidade. 3. Algoritmos de computação quântica. 4. Produção intelectual. I. Brod, Daniel Jost, orientador. II. Universidade Federal Fluminense. Instituto de Física. III. Título.

CDD - XXX

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

Yuri Jaloto Santos Machado

Computação quântica e o cassino quântico

Monografia apresentada no programa de graduação em Física da UFF como requisito para obtenção do grau de Graduado em bacharel em Física.

Universidade Federal Fluminense – UFF

Orientador: Daniel Jost Brod

Niterói-RJ

Yuri Jaloto Santos Machado

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Física da Universidade Federal Fluminense como requisito parcial para obtenção do título de Bacharel em Física.

Aprovado em 21 de dezembro de 2022.

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
DANIEL JOST BROD
Data: 22/12/2022 21:45:10-0300
Verifique em https://verificador.iti.br

Daniel Jost Brod (UFF) - Orientador

Lucas Mauricio Sigaud (UFF)

Reinaldo Faria de Melo e Souza (UFF)

Agradecimentos

Minha família pela oportunidade e minha filha pelo sentido.

Resumo

Nesse trabalho vamos abordar aspectos peculiares da mecânica quântica e aplicações na área da computação quântica. Para tal, apresentaremos uma análise dos conceitos fundamentais da mecânica quântica através de exemplos e ilustrações.

Em seguida discutiremos não-localidade, que é o fato de duas partículas estarem correlacionadas de forma que a medição em uma delas interfere na outra, mesmo que estejam distantes entre si, e contextualidade, que é característica em que o resultado de medições depende do contexto em que as medições foram feitas. Exemplos e experimentos de pensamento serão apresentados, além de aplicações, como alguns algoritmos de computação quântica.

Por fim, uniremos todos esses conceitos para definir um cassino que pode funcionar como proposta pedagógica, pois mostra que aplicando as regras da mecânica quântica em vez das regras da mecânica clássica em jogos comuns, como jogos de cartas, algumas vantagens financeiras apareceriam apareceriam, de forma que, nesse contexto, o cassino teria mais lucro do que o esperado classicamente.

Palavras-chaves: computação quântica, criptografia, fótons, q-bits, contextualidade, qiskit.

Abstract

In this work we will address peculiar aspects of quantum mechanics and applications in the field of quantum computing. To this end, we will present an analysis of the fundamental concepts of quantum mechanics through examples and illustrations.

We also discuss non-locality, which is the fact that two particles are correlated in such a way that the measurement in one of them interferes the other, even if they are distant from each other, and contextuality, which is the characteristic in which measurements outcomes depends on the context in which the measurements were taken. Examples and thought experiments will be presented, as well as applications such as some quantum computing algorithms.

Finally, we will unite all these concepts to define a casino that can work as a pedagogical proposal, as it shows that applying the rules of quantum mechanics instead of the rules of classical mechanics in common games, such a card game inside a casino, some financial advantages would appear, so that, in this context, the casino would make more profit than classically expected.

Key-words: Quantum computing, cryptography, photons, q-bits, contextuality, qiskit.

Sumário

Capítulo 1

Introdução

Desde meados da década de 1990, a investigação dos fundamentos da mecânica quântica tem se diversificado e se sofisticado, graças ao grande desenvolvimento da área de pesquisa conhecida como computação e informação quânticas [1,2]. Esse interesse renovado se deveu a descobertas como os algoritmos quânticos de busca em base de dados [3], de fatoração de inteiros [4] e ao desenvolvimento de outras aplicações, como por exemplo, a distribuição quântica de chaves criptográficas e o teletransporte quântico [5].

O estudo desses protocolos de informação quântica ajuda a identificar as características quânticas responsáveis pela vantagem do comportamento computacional quântico. Duas das propriedades-chave identificadas são a não-localidade quântica [6] (que aparece em medidas quânticas em estados emaranhados) e a contextualidade quântica [7–10], identificada mais recentemente como um recurso a ser explorado em certos modelos de computação quântica. A área tem crescido bastante nos últimos anos, sendo tema do prêmio Nobel de Física de 2022 por experimentos da chamada desigualdade de Bell.

Para mostrar as consequências desses fatos, será explorada a parábola do vidente superprotetor [7], onde, mais tarde, o foco será em mostrar as vantagens estatísticas da contextualidade quântica frente à teoria clássica. Para isso, apresentaremos certas tarefas associadas a jogos de carta. Uma delas é fazer um jogo de cartas onde a sorte do jogador pode mudar de acordo com o comportamento do jogo. No caso em que as regras do jogo são clássicas, o jogador sairá no lucro, em média. No entanto, se as regras quânticas são aplicadas ao jogo, o jogador entra no jogo achando que vai ganhar, mas o fato é que em média terá sempre prejuízo.

Capítulo 2

Conceitos de mecânica quântica

2.1 A mecânica quântica

Na mecânica clássica, quando queremos discutir sobre o comportamento de um corpo ou partícula, temos o que é conhecido como equação de movimento onde, sabendo as forças que atuam sobre uma determinada partícula e um conjunto de condições iniciais, conseguimos uma equação que nos dá uma previsão sobre o comportamento da partícula em um instante de tempo posterior. Isso é de grande utilidade da descrição de fenômenos que nos rodeiam. No entanto, a coisa é um pouco diferente na mecânica quântica.

Para tal, vamos definir uma função de onda, através da qual podemos prever quais as probabilidades de uma partícula se comportar de determinada forma. A equação que nos informa o comportamento da função onda é a chamada equação de Schrodinger.

$$i\hbar\frac{d}{dt}\left|\psi(t)\right\rangle = H\left|\psi(t)\right\rangle. \tag{2.1}$$

Os operadores de energias cinética e potencial, que aparecem através do operador H, atuam sobre a função de onda para gerar sua evolução no tempo e as energias possíveis do sistema.

Esse comportamento probabilístico pode parecer, a princípio, um problema para aplicações. No entanto, é um dos ingredientes que traz algumas peculiaridades que podem ajudar em tarefas computacionais [1, 2]. É possível pensar em um experimento simples que consegue ilustrar alguns dos comportamentos não intuitivos de sistemas quânticos, que pode ser realizado com um laser e três polarizadores. O formalismo que descreve esse experimento levam diretamente a uma descrição do bit quântico, a unidade fundamental de informação quântica. O experimento não apenas dá uma realização concreta de um bit quântico, mas também ilustra propriedades da medição quântica. Ele consiste no seguinte.

Um feixe de luz é jogado em uma tela de projeção. Um dos polarizadores, que será

chamado de polarizador A, é colocado entre a fonte de luz e a tela, e a intensidade da luz que atinge a tela é reduzida. Suponhamos que sua polarização é horizontal. Em seguida, é colocado um polarizador C entre o polarizador A e a tela de projeção. Se o polarizador C for girado de forma que sua polarização seja vertical, ou seja, ortogonal à polarização de A, nenhuma luz atinge a tela, como pode ser visto na figura (1), à esquerda.

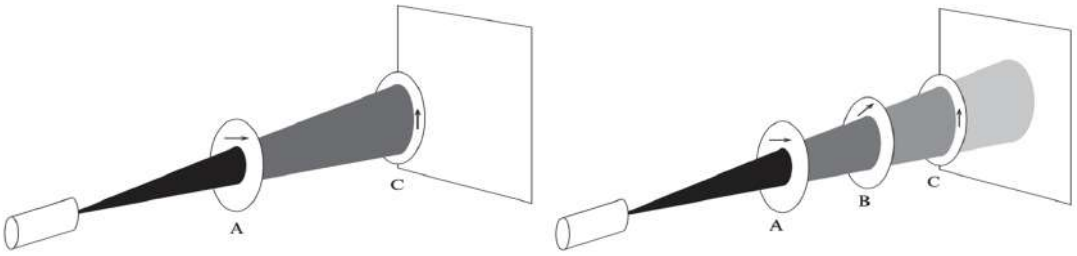

Figura 1 – Imagem à esquerda mostrando os polarizadores A e C. Quando o feixe de luz passa por A, os fótons que por ali passam assumem aquela polarização. Caso eles tentem passar por C, por conta da polarização ortogonal, esses fótons não chegarão na parede. Já na imagem à direita, com inclusão do polarizador B, alguns fótons, ao passar por ali, assumem polarização diagonal, de forma que alguns deles passarão por C.

Fonte: Imagem extraída de [1].

Finalmente, um novo polarizador, B, é colocado agora entre A e C. Como com a configuração anterior, nenhuma luz chega até a tela, é esperado que ao inserir B entre eles, nenhuma diferença no resultado final seja percebida, já que, se nenhuma luz passou por dois deles, não passará também por três. No entanto, contrariando esse pensamento, na maioria dos ângulos de polarização de B a luz chega à tela. A intensidade dessa luz será máxima se a polarização de B for de 45 graus em relação a A e C, como mostrado na figura (1) à direita. Os polarizadores não podem estar agindo como simples peneiras ou filtros, caso contrário a inserção de B não aumentaria o número de fótons que chegam à tela. Tem que haver outra explicação.

Apesar de ter explicação clássica, uma boa forma de entender esse experimento vem da mecânica quântica, e consiste em duas partes: um modelo de um estado de polarização do fóton e um modelo da interação entre um polarizador e o fóton. A mecânica quântica modela o estado de polarização de um fóton por um vetor unitário apontando na direção apropriada. Podemos adotar, para a descrição do experimento, $|\uparrow\rangle$ e $|\rightarrow\rangle$ para os vetores unitários que representam polarização vertical e horizontal, respectivamente. Agora, definimos $|v\rangle$ como um vetor representando um estado quântico genérico. Uma polarização arbitrária pode ser expressa como uma combinação linear $|v\rangle = a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ dos dois vetores de base. Os coeficientes a e b nessa expressão são chamados de amplitudes de $|v\rangle$ nas direções $\uparrow$ e $\rightarrow$, respectivamente. Quando um fóton com polarização $|v\rangle$ encontra um polarizador com eixo preferencial $\uparrow$, ele passará com probabilidade $|a|^2$ e será absorvido com probabilidade $|b|^2$. Além disso, qualquer fóton que passe pelo polarizador será agora

polarizado na direção do eixo que acabou de passar. Um fóton polarizado horizontalmente não tem nenhuma amplitude na direção vertical, então não tem chance de passar por C, que recebeu orientação vertical. Por esse motivo, nenhuma luz atinge a tela. Para entender o que acontece quando o polarizador B, com eixo preferencial diagonal, é inserida, é útil escrever o estado do fóton horizontalmente polarizado como $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\nwarrow\rangle)$.

Como qualquer fóton que passa pelo polarizador A torna-se polarizado horizontalmente, seu estado pode ser representado como na linha anterior e a amplitude do estado de qualquer fóton na direção $\nearrow$ é $\frac{1}{\sqrt{2}}$. O que acontecerá é que um fóton polarizado horizontalmente passará pelo polarizador B com probabilidade $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$. Dessa forma, qualquer fóton que passar por B, agora têm polarização $\nearrow$. Quando esses fótons atingem C, eles têm amplitude não nula na direção vertical, então alguns deles (metade) passarão pelo polarizador C e atingirão a tela, que é o que vemos na figura (1), à direita. Portanto, a mecânica quântica explica como mais luz pode atingir a tela quando o terceiro polarizador é adicionado.

2.2 O qubit

Um bit quântico, ou qubit, é o análogo de um bit, mas agora em vez de clássico, é definido como uma unidade de informação quântica. Esta informação pode ser descrita por um vetor, de forma que qualquer sistema quântico que pode ser modelado por um espaço vetorial bidimensional complexo pode ser visto como um qubit. Vamos representar a base do espaço de estados por $\{|0\rangle,|1\rangle\}$.

Um qubit, ao contrario do caso clássico, tem um contínuo de valores possíveis, ou seja, qualquer estado representado por $|v\rangle = a\,|0\rangle + b\,|1\rangle$ é um valor de qubit legítimo.

Esses sistemas, incluem a polarização de fótons, o spin do elétron e o estado fundamental junto com um estado excitado de um átomo. O rótulo de dois estados para esses sistemas não significa que o espaço de estados tem apenas dois deles, mas sim que todos os estados possíveis podem ser representados como uma combinação linear, ou superposição, de apenas dois estados.

Todas essas possibilidades são representados geometricamente em 3 dimensões como um ponto em uma esfera, conhecida como esfera de Bloch. Na figura (2), é possível ver o estado de um qubit genérico representado nessa esfera. Para tal, coordenadas esféricas são usadas.

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\,. \tag{2.2}$$

É possível notar que, em alguns pontos que passam em cima dos eixos, temos os resultados das medidas dos polarizadores A e C do exemplo.

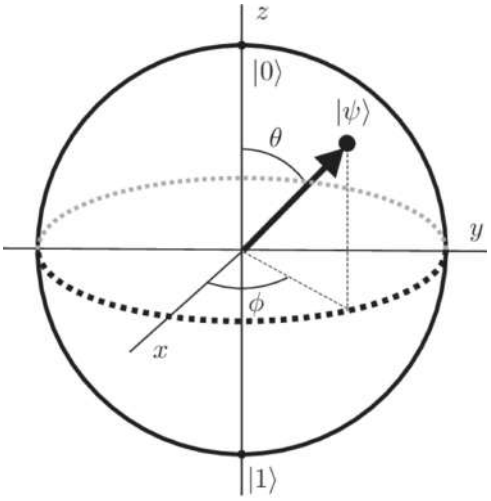

Figura 2 – Um qubit genérico representado como um ponto na esfera de Bloch.

Fonte: Imagem extraída de [2]

2.3 Portas quânticas

Depois da definição e notação para os qubits, é importante definir a representação de sistemas quânticos como circuitos. Eles devem ser lidos da esquerda para a direita. Cada linha no circuito representa a passagem do tempo ou talvez uma partícula física, como um fóton se movendo de um local para outro através do espaço. Geralmente, aparecem as chamadas portas quânticas, que estão associadas à dinâmica dos qubit. Essas portas são transformações unitárias aplicadas ao sistema. Um exemplo pode ser visto na figura (3), onde o estado inicial $|\psi_i\rangle$ foi transformado, através de U, no estado $|\psi_f\rangle$.

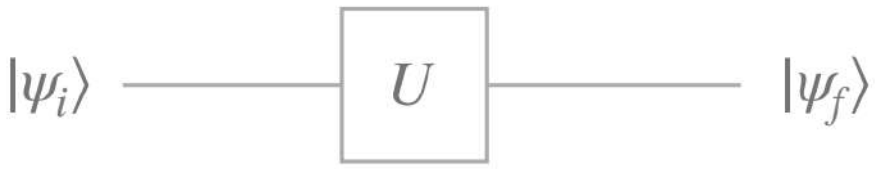

Figura 3 – Uma porta U aplicada a um estado $|\psi_i\rangle$ de entrada, o transformando em $|\psi_f\rangle$.

Fonte: Slide da disciplina de computação e informação quântica ministrada pelo professor Daniel Brod.

As portas que vão aparecer com mais frequência neste trabalho estão relacionadas a observáveis, como as matrizes de Pauli, que estão definidas na equação (2.3) e duas outras, chamadas de Hadamard e CNOT, definidas através da equação (2.4).

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.3}$$

$$C_{not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.4}$$

2.4 Emaranhamento

Imagine uma caso simples, onde temos um estado envolvendo mais de uma partícula, $|01\rangle$. Nesse caso, podemos escrever ele como o produto tensorial de dois estados de uma partícula, $|0\rangle \otimes |1\rangle$. Agora, considere um estado mais complexo, $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$. Ele também pode ser escrito como produto tensorial da seguinte forma, $|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. No entanto há estados para os quais isso não vale. Considere estado (chamado de estado de Bell), definido como:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.5}$$

Suponha que $|\Psi\rangle$ pode ser escrito como produto tensorial de estados de uma partícula,

$$|\Psi\rangle = |A\rangle \otimes |B\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}. \tag{2.6}$$

Podemos escrever (2.5) explicitamente como:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right] = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}. \tag{2.7}$$

Como (2.6) e (2.7) são iguais por hipótese,

$$a_1 b_1 = 0, \quad a_1 b_2 = \frac{1}{\sqrt{2}}, \quad a_2 b_1 = -\frac{1}{\sqrt{2}}, \quad a_2 b_2 = 0. \tag{2.8}$$

De (2.8), tiramos que $a_1 = 0$ ou $b_1 = 0$, pois $a_1 b_1 = 0$. No entanto, como $a_1 b_2$ e $a_2 b_1$ são diferentes de zero, nada poderia se anular, o que é uma contradição. Portanto, $|\Psi\rangle$ não pode ser escrito como produto tensorial de estados de uma partícula. Para esses casos, damos o nome de um estado emaranhado. Mas o que isso implica?

Imagine que duas cartas, uma de cada cor, serão entregues para dois jogadores, uma carta para cada um. Vamos supor que um está no Rio de Janeiro e o outro em Minas Gerais. Estamos preocupados em sortear, através de um jogo de cartas, o mando de campo de um jogo de futebol que participarão. O jogador que tirar a carta com naipe de cor preta tem o direito de decidir o mando de campo. Cada um receberá uma carta, que a princípio não sabe qual é. Quando um deles vira a sua carta, percebe que tem naipe de cor vermelha. Sabendo que as cartas sempre têm cores diferentes, é possível inferir qual a cor da carta do outro jogador, que nesse caso é preta e portanto ganhará o direito de decidir o mando de campo. Isso é perfeitamente explicável classicamente, pois a informação sobre a carta do outro jogador é inferida a partir da medição da primeira pela condição inicial do jogo.

Agora imagine que essas cartas são pares de partículas quanticamente correlacionadas (emaranhadas). Um paralelo pode ser feito com o estado de Bell descrito na equação (2.5), onde os estados $|0\rangle$ e $|1\rangle$ representam, agora, as cartas distribuídas. Será que a correlação entre elas continua sendo parecida com o caso anterior, onde, quando a carta (uma das partículas emaranhadas) é distribuída, já existe uma definição do resultado do jogo, que será descoberta ao virar a carta (medir o estado)? Ou tem algo mais, onde informação sobre a carta do outro jogador é colapsada instantaneamente pela medição do primeiro? Ou seja, inicialmente existe um estado de duas partículas, com uma partícula na mão de cada jogador, porém, não existe definição prévia do universo (ou de quem distribuiu as cartas), sobre quem está com qual naipe? E ainda, a informação sobre a carta do segundo jogador só existirá individualmente no momento em que a do primeiro passa a ser medida e vice-versa? Como veremos com mais detalhes na próxima seção, a segunda hipótese é a mais compatível com a mecânica quântica, e essa conexão de longa distância, chamada de emaranhamento quântico, é muito real e é peça fundamental para a nossa discussão. Não é um mero capricho quântico de interesse apenas para físicos, suas possibilidades chamaram a atenção de muitas áreas do conhecimento, principalmente quando se fala de computação.

Capítulo 3

Não-localidade

"Acreditamos que há uma segunda revolução quântica acontecendo agora", diz o físico Chris Monroe, do Joint Quantum Institute da Universidade de Maryland em College Park [12].

A primeira revolução atingiu o pico quando o físico austríaco Erwin Schrödinger introduziu o termo emaranhamento em um artigo de 1935, inspirado por um experimento de pensamento proposto no mesmo ano por Albert Einstein e colaboradores Boris Podolsky e Nathan Rosen. Esse experimento de pensamento argumentou que, quando dois objetos interagem de uma maneira particular, a física quântica exige que eles se conectem ou se emaranhem, de modo que medir uma propriedade de um revela instantaneamente o valor dessa propriedade para o outro, não importa o quão longe estejam.

Esse famoso paradoxo (em que Einstein fincou o termo "ação fantasmagórica a distância"), ficou conhecido como paradoxo EPR. A crença de Einstein era de que devia haver mais coisas além do que a teoria quântica descreve. Isso levou a algumas hipóteses, como a de que propriedades medidas na verdade já existiam e estavam sendo somente reveladas, trazendo o que se chamou de teoria de variáveis ocultas. Mas, em vez de minar a física quântica, o artigo EPR [11] tornou-se pontapé para outros cientistas que mostraram que essa conexão era de fato real.

Agora, laboratórios em todo o mundo criam e estudam rotineiramente o emaranhamento, forçando os limites dos tipos e tamanhos de objetos que podem ser emaranhados. Alguns estudos estão tentando esclarecer a fronteira que separa a peculiaridade quântica do mundo macroscópico. Outros se concentram no emaranhamento em si, particularmente em como ele muda ao longo do tempo. Grande parte do novo trabalho está construindo uma base para tecnologias poderosas que operam no mundo real, desde a manipulação de informações em computadores quânticos que já são realidade até o envio de mensagens secretas com segurança inquebrável, através de protocolos de criptografia. Depois de anos de pesquisa, o prêmio Nobel de Física de 2022 foi justamente para experimentos sobre a desigualdade

de Bell, uma das peculiaridades que vamos discutir.

3.1 Variáveis ocultas?

Como foi visto, muitas características da teoria quântica vão contra a intuição física que desenvolvemos vivendo em um mundo macroscópico. A descrição da natureza da teoria quântica concorda mais precisamente com os experimentos do que qualquer teoria física anterior, mas ao mesmo tempo suas previsões são intrinsecamente probabilísticas. Muita pesquisa foi feita para tentar descobrir se significa que falta algo na teoria, ou se esse não-determinismo é um traço fundamental da própria natureza.

As teorias de variáveis ocultas foram construídas como tentativas de encontrar alternativas que, ao mesmo tempo, fossem compatíveis com a mecânica quântica, mas com fundamentos conceituais diferentes indicando o determinismo e a localidade da física clássica. Para os físicos, o assunto surge como uma oportunidade de ver um problema através de mais de uma estrutura conceitual alternativa, fornecida por diferentes teorias de variáveis ocultas, de forma a ajudar a desenvolver uma intuição sobre fenômenos quânticos. Particularmente, sua utilidade aparece por conta da aparente inadequação da intuição clássica para explicar muitas características.

Em uma teoria de variáveis ocultas, se supõe que existe uma variável, geralmente chamada de λ, que não é acessível experimentalmente. É através de λ que a distribuição de probabilidades seria feita previamente. Voltando no exemplo das cartas, seria λ a variável que guardaria a informação sobre quem pega a carta vermelha ou preta previamente com determinada probabilidade. Mas seria possível a existência dessa variável de forma que as características da física clássica também estivessem presentes no campo da física quântica? Isto é, variáveis ocultas são compatíveis com outras características clássicas como a localidade? Foi esse tipo de questionamento que os cientistas Alain Aspect, John F. Clauser e Anton Zeilinger fizeram para ganhar o prêmio Nobel de Física no ano de 2022. Eles conseguiram, em laboratório, fazer medições em um estado emaranhado e mostraram que, de fato, a questão levantada pelo paradoxo EPR, de que tinha que existir essa variável oculta, λ, tem uma resposta experimental, a de que a explicação da mecânica quântica para estados emaranhados não está incompleta, λ não é compatível com localidade. A prova disso é feita através da violação da desigualdade CHSH.

3.2 Desigualdade CHSH

Considere agora que as medições sobre o naipe das cartas citadas anteriormente serão feitas de forma que o primeiro jogador pode fazer duas medidas, A_0 e A_1. Da mesma forma, o outro jogador também poderá fazer duas medidas, B_0 e B_1. Todas as quatro

medidas podem retornar os valores +1 ou -1, de forma que cada observável de cada carta (índices 0 e 1 de A ou B) está associada à cor do naipe encontrado ao medir (preto ou vermelho) e ao naipe (caso seja preto, distingue entre espadas e paus. Caso seja vermelho, distingue entre copas e ouro).

Agora, vamos considerar a combinação $A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 = A_0(B_0 + B_1) + A_1(B_0 - B_1)$. Como só temos dois valores possíveis (+1 ou -1), então $B_0 + B_1 = 0$ ou $B_0 - B_1 = 0$, de forma que só sobrará um termo, o que está junto com A_0 ou o que está multiplicando A_1. Ou seja, teremos dois resultados possíveis:

$$A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 = \pm 2. \tag{3.1}$$

A fim de obter um valor médio, ou valor esperado para essas quantidades, imagine que o experimento será realizado diversas vezes, obtendo o que é chamado de desigualdade CHSH:

$$|\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle| \leq 2, \tag{3.2}$$

onde A_i e B_j denotam os resultados da medição i no sistema A e j no sistema B, e os $\langle\rangle$ indicam uma média ao longo de muitas execuções do experimento. Uma maneira simples de verificar que a desigualdade é verdadeira, consiste em substituir todas as dezesseis combinações possíveis de valores para A_0, A_1, B_0, B_1 no lado esquerdo da equação (3.2).

A desigualdade não faz referência à mecânica quântica em si, apenas limita uma combinação particular de médias sobre as variáveis derivando uma desigualdade que deve ser satisfeita por médias de execuções experimentais. Portanto, essa desigualdade possibilita uma comparação de qualquer teoria local com a mecânica quântica, que apenas prevê, a princípio, probabilidades e médias (valores esperados de observáveis). Veremos em breve que as previsões da mecânica quântica conflitam com a desigualdade de localidade CHSH.

3.3 Violação na mecânica quântica e desigualdade de Bell

É importante ressaltar que, nessa demonstração, duas hipóteses foram tomadas:

- **Realismo**: Todas as quatro medidas tem valores bem definidos em cada rodada do experimento, ou seja, toda vez que medimos, temos um resultado pré existente (+1 ou -1).
- **Localidade**: O resultado da medida do primeiro jogador não depende do resultado da medida do segundo (e vice-versa). É isso que nos permite chegar à equação (3.1),

já que somente a partir dessa hipótese, podemos inferir que o resultado da medida A_0 é o mesmo para as medidas de B_0 e B_1.

Agora vamos ver como a mecânica quântica viola a desigualdade e mostra que essas duas hipóteses não podem ser verdadeiras juntas. Para isso, começaremos com um estado maximamente emaranhado de dois qubits visto na seção anterior (equação (2.5)), um em cada região espacial A e B.

As seguintes medidas serão feitas:

$$A_0 = X, A_1 = Z, B_0 = -\frac{1}{\sqrt{2}}(X+Z), B_1 = \frac{1}{\sqrt{2}}(Z-X). \tag{3.3}$$

Dessa forma, para os quatro valores esperados dentro da equação (3.2), teremos que:

$$\langle A_0 B_0 \rangle = \langle \Psi | \, X \otimes \frac{1}{\sqrt{2}}(-X-Z) \, | \Psi \rangle = \frac{1}{\sqrt{2}}. \tag{3.4}$$

$$\langle A_0 B_1 \rangle = \langle \Psi | \, X \otimes \frac{1}{\sqrt{2}}(Z-X) \, | \Psi \rangle = \frac{1}{\sqrt{2}}. \tag{3.5}$$

$$\langle A_1 B_0 \rangle = \langle \Psi | \, Z \otimes \frac{1}{\sqrt{2}}(-X-Z) \, | \Psi \rangle = \frac{1}{\sqrt{2}}. \tag{3.6}$$

$$\langle A_1 B_1 \rangle = \langle \Psi | \, Z \otimes \frac{1}{\sqrt{2}}(Z-X) \, | \Psi \rangle = -\frac{1}{\sqrt{2}}. \tag{3.7}$$

De forma que o resultado final é

$$\left| \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - (-\frac{1}{\sqrt{2}}) \right| = 2\sqrt{2} > 2, \tag{3.8}$$

o que é uma contradição com a equação (3.2). Portanto, temos que: ou o realismo é uma hipótese falsa ou a localidade é. Juntas, essas hipóteses não podem ser verdadeiras. De fato, o que está sendo mostrado é que o que é chamado de realismo local não pode fazer parte da mecânica quântica. Para que existam resultados pré-definidos, que é o que será usado mais para frente, precisamos levar em conta a não-localidade.

Capítulo 4

Contextualidade

4.1 A parábola do vidente super-protetor

Uma outra propriedade fundamental da mecânica quântica é a contextualidade, estudada inicialmente por Kochen e Specker, e que tem se provado importante para a computação quântica. Para iniciar o estudo dessa propriedade, analisamos um cenário conhecido como a parábola do vidente super-protetor, que foi extraído por tradução livre de [7].

Na época do Rei Asarhaddon, existia um homem que tinha uma filha, com a qual muitos jovens queriam se casar. Ele não queria que sua filha se casasse, mas ela queria. Para resolver isso, ele preparou um pequeno jogo para os pretendentes. Quem cumprisse a tarefa tinha a permissão para se casar com ela.

O jogo era o seguinte: cada pretendente ficava sentado numa mesa sobre a qual havia 3 caixas em fila, sendo que cada uma poderia ou não conter um diamante. Pedia-se que ele fizesse uma previsão sobre duas que estariam ou cheias, ou duas vazias. O rei então permitia que o pretendente abrisse as duas caixas para as quais tinha feito a previsão; se ele tivesse acertado, seria sua a mão da princesa.

Não importava quantas vezes isso fosse realizado, parecia ser impossível cumprir a tarefa, já que a cada rodada o pai mandava o pretendente escolher duas caixas para checar (as duas vazias ou as duas cheias), e toda vez que isso acontecia, acabava que sempre uma estava vazia e a outra com a pedra. E mais, o diamante às vezes estava na primeira caixa apontada e às vezes na segunda. Mas como seria possível que, dadas três caixas, ninguém nunca conseguia escolher duas vazias ou duas cheias? (Qualquer estado bem-definido de três caixas deve ter duas caixas vazias ou duas cheias.)

A filha não teria casado até a morte de seu pai se não fosse pelo fato de que, depois do filho de um adivinho (por quem ela se interessou) ter feito sua previsão, ela rapidamente escolheu duas caixas, uma que estaria cheia e a outra vazia, e as abriu, confirmando assim

a previsão de seu pretendente.

A peça principal do texto é o fato de que quando duas das caixas eram reveladas, sempre uma estava cheia e a outra vazia, independente da ordem (no geral, esse era o comportamento, mas individualmente seria impossível prever qual estaria cheia ou vazia). O que chama a atenção nesse exemplo é essa estranha propriedade da qual um subconjunto de caixas tem coisas pré definidas, mas individualmente não. Somando esse fato à contradição estatística causada no conjunto, temos o que é chamado de contextualidade.

- **Contextualidade**: Característica de distribuições de probabilidade pela qual o resultado de medições feitas pode depender de outras medições que são feitas juntas. Ou seja, o resultado de medições depende do contexto em que as medições foram feitas.

Na parábola, se uma das caixas sempre muda de valor dependendo de qual caixa é medida com ela, isso é um exemplo explícito de contextualidade. Mas qual a ligação disso com a mecânica quântica?

Basta pensar num paralelo no qual revelar as caixas seria fazer medições. Imagine uma partícula que tem determinado comportamento global. Agora imagine que vamos medir as 3 componentes individualmente. Os resultados sempre dão uma coisa repetida, da mesma forma que os diamantes na caixa. Mas juntando todas as informações individuais, parece sempre impossível obter uma informação que seja compatível com o comportamento global da partícula. A estatística associada não será a de 100% de erro, como na parábola, mas o que vamos ver mais a frente é que a probabilidade de acerto no caso quântico é menor do que o esperado classicamente. Além disso, no caso do cassino, que será mostrado em breve, um exemplo com 3 caixas (que será feito com 3 cartas de baralho) não pode ser atingido pela mecânica quântica, se tratando apenas de um exemplo ilustrativo de um comportamento real.

4.2 A mecânica quântica é contextual?

Aqui, estaremos interessados no caso onde se tenta medir observáveis que não comutam. Dessa forma, encontramos a partir dessa medida, resultados que parecem indicar que não há um valor para os resultados de observáveis que não comutam antes que de fato seja efetuada a medição. No entanto, esse fato de não existir propriedades pré-definidas, pode indicar interpretação de Copenhague da teoria quântica, que já conhecemos. Aqui, estaremos interessados em provar que esses valores não podem ser pré-definidos, ao menos não de forma não-contextual. Ou seja, o que vamos mostrar é que não conseguimos ter realismo e não-contextualidade simultaneamente. Nesta seção, veremos isso através da demonstração feita por Peres [9], com inspiração de [10].

Para começar, vamos considerar uma partícula que está em um dos estados de Bell vistos anteriormente:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{4.1}$$

Como no nosso estado emaranhado temos duas partículas, faremos medições através de observáveis não-locais, que podem ser definidas por produtos tensoriais dos observáveis descritos em (2.3). Assim, teremos medições da seguinte forma:

$$X_1 \otimes X_2, Y_1 \otimes Y_2, Z_1 \otimes Z_2. \tag{4.2}$$

No entanto nosso estado de Bell inicial é autoestado com autovalor -1 desses observáveis. Sendo assim, se assumirmos que cada resultado associado a cada medida individual é pré-definido e não depende de quais operadores nós decidimos medir junto dele, estamos falando sobre não-contextualidade. Por exemplo, se obtivermos na primeira partícula um resultado $x_1 = +1$ ou $x_1 = -1$, ele não poderia depender de qual medida estamos fazendo junto a dele na outra partícula, ou seja, não poderia depender se medimos X_2, Y_2, Z_2, junto, já que esses três operadores comutam com X_1.

Agora, usando o fato do autovalor dessa medida para nosso estado ser igual a -1, e aliando com a ideia de realismo, ou seja, supondo que há resultados pré-existentes e vamos revelá-los, teremos então que:

$$x_1 x_2 = y_1 y_2 = z_1 z_2 = -1. \tag{4.3}$$

Agora, a ideia é nos atentar a outras medidas nesse mesmo estado. Para isso, vamos considerar dois observáveis:

$$A = X_1 \otimes Y_2, B = Y_1 \otimes X_2. \tag{4.4}$$

A e B comutam, o que significa que podemos medir os dois simultaneamente. Para isso, podemos medir AB diretamente, de forma a obter (note que medir AB diretamente vai nos dar -1, de acordo com (4.2) e (4.3)):

$$AB = (X_1 \otimes Y_2)(Y_1 \otimes X_2) = Z_1 \otimes Z_2. \tag{4.5}$$

Agora, vamos medir separadamente A e B e multiplicar os resultados, de forma que, em teoria, temos que obter o mesmo resultado de medir AB diretamente (-1). No entanto, se supormos não-contextualidade e realismo, obteríamos que o resultado de $A = X_1 \otimes Y_2$ teria que ser $x_1 y_2$, e de $B = Y_1 \otimes X_2$ seria $y_1 x_2$, lembrando que pela nossa hipótese, esses resultados teriam o mesmo valor dos mostrados em (4.3). Isso, significa que:

$$x_1 y_1 y_2 x_2 = (x_1 x_2)(y_1 y_2) = (-1)(-1) = +1. \tag{4.6}$$

Mas obtivemos o valor oposto do esperado medindo separadamente A e B. Dessa forma, só nos resta duas opções válidas. Ou a hipótese de realismo é verdadeira e a de não-contextualidade é falsa ou então a de realismo é falsa e a não-contextualidade é verdadeira. As duas não podem ser verdadeiras juntas. Não faz sentido abrir mão do realismo dentro da nossa discussão sobre o jogo do vidente ou qualquer outro jogo em que estamos querendo revelar alguma propriedade. Já que esse é o ponto de discussão, percebemos então que nesse cenário, a mecânica quântica tem que ser contextual!

Capítulo 5

Aplicações e Computação quântica

"Tornou-se cada vez mais claro que um novo tipo de tecnologia está surgindo. Podemos ver que o trabalho dos laureados com estados emaranhados é de grande importância, mesmo para além das questões fundamentais sobre a interpretação da mecânica quântica". Essa foi a frase dita pelo comitê do prêmio Nobel de Física de 2022. Está cada vez mais claro que a mecânica quântica pode contribuir com o mundo tecnológico, principalmente falando de computação.

5.1 Criptografia

Imagine que uma pessoa, Alice, quer enviar uma mensagem secreta para outra, Bob. Para isso, basta eles compartilharem o chamado one time pad, que seria uma chave secreta que somente elas têm. No entanto, a única forma clássica de compartilhar um one time pad de forma segura é se encontrando pois, a principio, qualquer informação pode ser interceptada. Sendo assim, Alice e Bob precisam se encontrar para definir essa chave. Ela funciona de forma que, quando Alice vai enviar uma mensagem para Bob, ela a codifica usando uma string de bits (a chave), tal que quando Bob a receber, poderá decodificar usando a mesma string. Mas e, se eles não puderem se encontrar antes para fazer essa definição? Teria algum método que mantivesse a segurança da informação? A resposta é sim, e uma das formas é o chamado protocolo BB84 [13].

Para gerar uma chave secreta usando a mecânica quântica, Alice vai sortear duas sequências aleatórias de bits do mesmo tamanho, vamos dizer a e b. Em seguida ela vai preparar um estado (quântico) de forma que, para cada índice de a e b, ela prepara um estado em um autovalor de Z (se $b_i = 0$) ou X (se $b_i = 1$) e escolhe um autovalor $+1$ (se $a_1 = 0$) ou -1 (se $a_i = 1$). Vamos supor que $a = 01101$ e $b = 11001$. Sendo assim, Alice vai enviar 5 qubits, nos estados $|+\rangle, |-\rangle, |1\rangle, |0\rangle, |-\rangle$.

Bob, ao receber, vai escolher uma sequência aleatória c, e cada qubit i será medido na base Z (se $c_i = 0$) ou X (se $c_i = 1$). Imagine que a string de Bob é $c = 11100$, ou seja, ele

vai medir os qubits que receber nas seguintes bases: XXXZZ. Dessa forma, todas as vezes em que Bob medir na mesma base em que os qubits de Alice foram preparados, ele vai obter o mesmo bit que ela. A única forma deles saberem que as bases de Alice e Bob são iguais é publicando a lista de bases medidas em um canal público.

Após isso, será possível eles terem informação sobre em quais qubits as bases coincidiram. Nos casos em que isso aconteceu, em tese, Bob vai obter o mesmo resultado (0 ou 1) relacionado à primeira string de Alice. Esse processo pode ser visto na tabela (1) abaixo, em que o one time pad para esse caso seria a string 101.

string a	1	0	0	1	1
string b	1	0	1	1	0
Base que Alice usou	X	Z	X	X	Z
Qubits codificados	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
string c	1	1	1	0	0
Base que Bob usou	X	X	X	Z	Z
string a'	1	0/1	0	0/1	1

Tabela 1 – Duas strings de Alice (a e b) e as bases em que Bob mediu. Nos casos onde as bases coincidem, Bob tem o mesmo resultado comparado com aquele bit da primeira string de Alice, a substring 101.

Agora, podemos pensar no caso onde ocorre um tipo de ataque. Uma terceira pessoa, Eve, vai interceptar a mensagem de Alice. No canal clássico, Alice e Bob discutem apenas a escolha de bases e não os próprios valores de bits, então Eve não pode obter nenhuma informação sobre a chave ouvindo apenas o canal clássico. Para obter informações, Eve deve interceptar os fótons transmitidos por Alice e ainda deve enviar esses mesmos fótons para Bob antes de saber a escolha de bases feita por Alice e Bob, pois eles comparam as bases somente após Bob confirmar o recebimento dos fótons. Se ela enviar fótons diferentes para Bob, Alice e Bob detectarão que algo está errado quando eles compararem valores de bits medidos na mesma base. No entanto, se ela envia os fótons originais para Bob sem fazer qualquer coisa, ela não ganha nenhuma informação, já que a informação valiosa é a chave final (um subconjunto da string original).

Como Alice ainda não contou a Bob sua sequência de bases, Eve não sabe em qual base medir cada qubit. Se ela medir aleatoriamente os bits, a base errada será usada aproximadamente metade das vezes. Quando ela usa a base errada para medir, a medida altera o estado da partícula antes dela ser reenviada para Bob. Essa mudança significa que, mesmo que Bob meça o fóton na mesma base que Alice usou para codificar o bit, ele obterá o valor de bit correto apenas metade das vezes.

No fim, Bob publica uma substring da substring obtida para que possa comparar se, de fato, o resultado é o mesmo da primeira string de Alice. Se Eve tentou obter alguma informação, mesmo que Bob tenha medido na mesma base, somente metade das vezes

ele vai obter o mesmo resultado que Alice. Essa substring final publicada é sacrificada e somente o restante é aproveitado. Dessa forma, quanto maior a sequência de bits preparada inicialmente e maior a substring publicada posteriormente, maior a acurácia e segurança do processo. Isso nos mostra que essa distribuição de chaves usando propriedades da mecânica quântica tem bastante utilidade e é um protocolo em que a segurança está baseada em princípios da própria natureza física.

5.2 Teletransporte

Vamos imaginar agora que Alice e Bob estão em laboratórios distantes e Alice quer enviar sua informação (quântica) para Bob, mas ela só pode se comunicar com Bob através de um canal clássico. Vamos dizer que a informação que ela quer enviar seja do tipo $|\phi\rangle = a\,|0\rangle + b\,|1\rangle$. E ainda, para que isso seja possível, Alice e Bob precisam compartilhar um estado emaranhado de 2 qubits, $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Sendo assim, temos um estado inicial que pode ser escrito da seguinte forma:

$$\begin{aligned} |\phi\rangle \otimes |\Phi_0\rangle &= \frac{1}{\sqrt{2}}(a\,|0\rangle \otimes (|00\rangle + |11\rangle) + b\,|1\rangle \otimes (|00\rangle + |11\rangle)) \\ &= \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle) + b\,|111\rangle)), \end{aligned} \tag{5.1}$$

tal que Alice controla os dois primeiros qubits e Bob o terceiro. O passo seguinte é definido pelas portas C_{not} e Hadamard, definidas na equação (2.4), de forma que Alice vai usar C_{not} nos dois qubits que tem, seguido de H no primeiro qubit, obtendo um estado da seguinte forma:

$$\begin{aligned} (H \otimes I \otimes I)(C_{not} \otimes I)(|\phi\rangle \otimes |\Phi_0\rangle) =& \frac{1}{2}(|00\rangle\,(a\,|0\rangle + b\,|1\rangle) + |01\rangle\,(a\,|1\rangle + b\,|0\rangle) \\ &+ |10\rangle\,(a\,|0\rangle - b\,|1\rangle) + |11\rangle\,(a\,|1\rangle - b\,|0\rangle)). \end{aligned} \tag{5.2}$$

De acordo com a equação (5.2), se Alice medir os dois primeiros qubits, obtém um dos quatro estados de base padrão $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$ com igual probabilidade. E ainda, dependendo do resultado de sua medição, o estado controlado por Bob será colapsado em um dos seguintes estados: $a\,|0\rangle + b\,|1\rangle$, $a\,|1\rangle + b\,|0\rangle$, $a\,|0\rangle - b\,|1\rangle$ ou $a\,|1\rangle - b\,|0\rangle$. É possível notar que o estado controlado por Bob já é parecido com o estado que Alice queria enviar, a menos de alguma transformação.

Após isso, Alice envia o resultado de sua medição como dois bits clássicos para Bob. Após essas transformações, informações cruciais sobre o estado original estão contidas no qubit controlado por Bob. Quando Bob recebe os dois bits clássicos de Alice, ele sabe, de

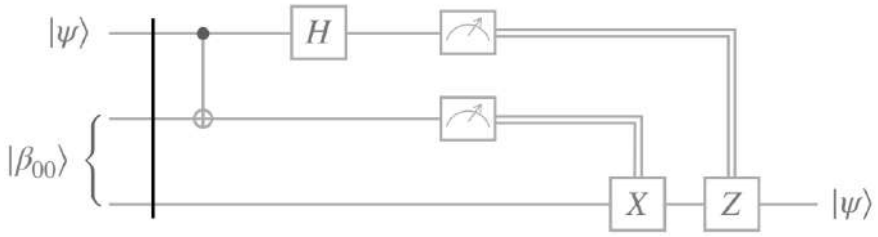

Figura 4 – Circuito que representa o algoritmo para teletransportar um qubit. As duas linhas de cima estão relacionadas aos qubits de Alice e a de baixo, o qubit de Bob.

Fonte: Slide da disciplina de computação e informação quântica ministrada pelo professor Daniel Brod.

acordo com a equação (5.2) como o estado controlado por ele está. Sendo assim, Bob pode reconstruir o estado original do qubit de Alice, aplicando a transformação de decodificação apropriada ao seu qubit.

Se Alice enviou os bits 00, Bob então decodificará usando o operador identidade I. Caso os bits sejam 01, ele usará o operador X. Caso seja 10, usará Z, e se for 11, será usado Y. Essa transformação corrigirá o estado nas mãos de Bob para que o estado pretendido seja obtido. Ou seja, no fim das contas, em qualquer um dos casos, o estado final que Bob terá em mãos é equivalente ao estado original de Alice, $|\phi\rangle = a\,|0\rangle + b\,|1\rangle$.

O princípio da não clonagem [2] implica não ser possível clonar um estado quântico. No momento em que Bob faz a correção final em seu estado, o estado original, antes nas mãos de Alice, não poderá mais existir ali. Apenas Alice ou Bob pode reconstruir o estado quântico original. Quando Bob obtém em seu laboratório o estado pretendido, esse estado já não existe para Alice por conta das medições feitas por ela. O teorema da não clonagem não é violado nesse processo. O circuito que representa todo esse protocolo pode ser representado de acordo com a figura (4).

5.3 Algoritmos

5.3.1 Algoritmo de Deutsch–Jozsa

Agora, vamos explorar o que é chamado de problema de Deutsch, que pode ser descrito como o seguinte jogo. Imagine que Alice está no Rio de Janeiro e seleciona um número aleatório de 0 a $2^n - 1$, que pode ser representado por n bits. Esse número é enviado por correio em uma carta para Bob, que está em outro país. Bob calcula alguma função Booleana $f(x)$ e responde com o resultado, que é 0 ou 1. Bob usa uma função f que é de dois tipos, ou $f(x)$ é constante para todos os valores de x, ou então $f(x)$ é balanceada, ou seja, igual a 1 para exatamente metade de todos os x possíveis, e 0 para a outra. Alice tem

como objetivo determinar com certeza se Bob escolheu uma $f(x)$ constante ou balanceada, de forma que a comunicação entre eles seja a mínima possível. Quão rápido ela pode ter sucesso?

No caso clássico, Alice só pode enviar a Bob um valor de x em cada carta. Na pior das hipóteses, ela precisará consultar Bob pelo menos $\frac{2^n}{2}+1$ vezes, pois ela pode receber metade de todos zeros, mas o primeiro da outra metade ser diferente. Sendo assim, o melhor algoritmo clássico determinístico que ela pode usar requer $\frac{2^n}{2}+1$ consultas. No entanto, imagine que Bob e Alice pudessem trocar qubits, em vez de apenas bits clássicos. Se Bob concordou em calcular $f(x)$ usando uma transformação unitária (oráculo) definida por U: $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$, então Alice teria o que precisa em apenas uma correspondência com Bob, usando o algoritmo [2] representado pelo circuito da figura (5).

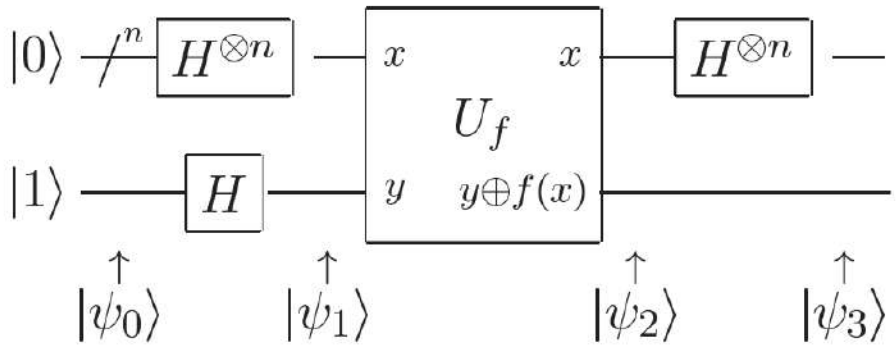

Figura 5 – Circuito que representa o algoritmo de Deutsch-Jozsa.

Fonte: [2].

Alice tem um registro de n qubits para armazenar sua consulta e um único registrador de qubit que ela dará a Bob. O estado inicial será então da seguinte forma:

$$|\Psi_0\rangle = |0\rangle^{\otimes n} |1\rangle . \tag{5.3}$$

Depois de aplicar a transformação de Hadamard, o estado passará a ser:

$$|\Psi_1\rangle = \sum \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{5.4}$$

No próximo passo, essa superposição será avaliada através da transformação U, de forma a obter

$$|\Psi_2\rangle = \sum \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{5.5}$$

Alice agora tem um conjunto de qubits no qual o resultado da avaliação da função de Bob é armazenado na amplitude do estado de superposição do qubit. Ela interfere

na superposição usando uma transformação Hadamard no registrador de consulta. Para determinar o resultado dessa transformação, é interessante primeiro calcular o efeito da transformação de Hadamard em um estado $|x\rangle$. Como temos duas opções para cada componente desse estado, podemos verificar separadamente o caso em que $x = 0$ e o que $x = 1$. Assim é possível ver que no caso de um qubit, temos que $H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}$. Portanto

$$H^{\otimes n}|x_1, ..., x_n\rangle = \frac{\sum_{z_1,...z_n}(-1)^{x_1z_1+...+x_nz_n}|z_1, ..., z_n\rangle}{\sqrt{2^n}}, \tag{5.6}$$

que pode ser expressa de forma mais sucinta através da seguinte equação

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x.z}|z\rangle}{\sqrt{2^n}}, \tag{5.7}$$

onde $x.z$ é o produto interno bit a bit de x e z módulo 2. Usando a equação (5.5) podemos agora avaliar $|\Psi_3\rangle$, tal que

$$|\Psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x.z+f(x)}|z\rangle}{2^n}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{5.8}$$

Alice agora observa o registrador de consulta. Observe que a amplitude para o estado $|0\rangle^{\otimes x}$ é $\sum_x (-1)^{f(x)}/2^n$. Vejamos os dois casos possíveis (f constante ou f balanceado) para diferenciar o que acontece. No caso em que f é constante, a amplitude para $|0\rangle^{\otimes x}$ é $+1$ ou -1, dependendo do valor que $f(x)$ assume. Como $|\Psi_3\rangle$ tem módulo um, segue que todas as outras amplitudes devem ser zero, e uma medição produzirá o valor 0 para todos os qubits no registro de consultas. Se f for balanceada, as contribuições positivas e negativas da amplitude para $|0\rangle^{\otimes x}$ se cancelam, deixando uma amplitude igual a zero. Assim, uma medição deve produzir um resultado diferente de 0 em pelo menos um qubit no registro de consulta. Portanto, se o resultado da medição de Alice nos dá o resultado onde todos os bits são zero, então a função é constante. Caso contrário, a função é balanceada.

Mostramos que um computador quântico pode resolver o problema de Deutsch com uma avaliação da função f em comparação com o requisito clássico para avaliações $\frac{2^n}{2} + 1$. Isso parece impressionante, mas há várias ressalvas importantes. Primeiro, o problema de Deutsch não é um problema especialmente importante, uma vez que não tem aplicações conhecidas. Em segundo lugar, a comparação entre algoritmos clássicos e quânticos é, de certa forma, uma maçã comparada a laranjas, pois o método de avaliação da função é bastante diferente no dois casos. Terceiro, se Alice tem permissão para usar um computador clássico probabilístico, então basta pedir para Bob avaliar $f(x)$ para alguns x escolhidos aleatoriamente, e ela pode determinar muito rapidamente com alta probabilidade se f é constante ou balanceada. Esse cenário probabilístico é talvez mais realista do que o cenário determinístico que estamos considerando. Apesar dessas ressalvas, o algoritmo

Deutsch-Jozsa contém a essência de algoritmos quânticos mais impressionantes. Um exemplo é o algoritmo de Bernstein-Vazirani.

5.3.2 Algoritmo de Bernstein-Vazirani

Um exemplo que pode ser visto como uma extensão do algoritmo Deutsch-Jozsa que foi abordado na última seção, é o algoritmo de Bernstein-Vazirani [16]. Através dele, mostrou-se que pode haver vantagens em usar um computador quântico como ferramenta computacional para problemas mais complexos do que o problema de Deutsch-Jozsa.

Agora, em vez de falar de função balanceada ou constante, como no problema anterior, a questão gira em torno de descobrir uma string através de um determinado número de tentativas. Seja essa string de tamanho n, qual a quantidade de vezes necessárias para acertar os bits dessa string sem ter nenhuma informação prévia? Uma abordagem clássica, temos o seguinte.

Seja uma string secreta $s = 01010001$. Imagine que somente Alice tem informação sobre ela e Bob quer tentar descobrir qual é essa string. Para tal, Bob pode usar strings auxiliares e enviar para Alice, que ficará encarregada de fazer um produto escalar dado por $f(x) = s.x \pmod 2$ entre os bits de cada string. Para descobrir o primeiro bit, Bob envia a string $x = 10000000$, de forma que depois que Alice realiza a operação entre as duas string, o resultado é enviado de volta para Bob. Se o resultado for 1, Bob já sabe que o primeiro bit é 1, pois era o único não nulo. Se for 0, o primeiro bit da string secreta é 0. Nesse exemplo, Bob enviará uma string auxiliar para Alice oito vezes até ter informação suficiente para reconstruir a string secreta. Dessa forma, é possível notar que quanto maior a string secreta, maior é o número de rodadas do jogo até que Bob saiba a string de Alice. No entanto, um caso interessante é pensar que Bob agora não tem mais n chances de jogar (nesse caso 8), mas um número reduzido.

Nesse caso, temos o fator sorte, de forma que não seria mais possível acertar a sequência com 100% de chance classicamente. No entanto, usando o algoritmo de Bernstein-Vazirani, seria possível implementar uma regra tal que essa string fosse descoberta com somente uma tentativa.

Seja uma string inicial x e uma string secreta s (que queremos descobrir). O oráculo agora, terá retorno definido por $\mathrm{U} = (-1)^{f(x)}$, onde $f(x) = s.x \pmod 2$. Novamente, é possível notar que o retorno dessa função será 0 ou 1, uma vez que ela faz o produto interno módulo 2 entre duas strings de bits, parecido com o caso anterior. O algoritmo pode ser representado como na figura (6):

O primeiro passo do algoritmo é aplicar a porta Hadamard em todos os bits da string inicial. Logo, dado uma sequência inicial $|\psi_0\rangle = |00...0\rangle$, o próximo estado será

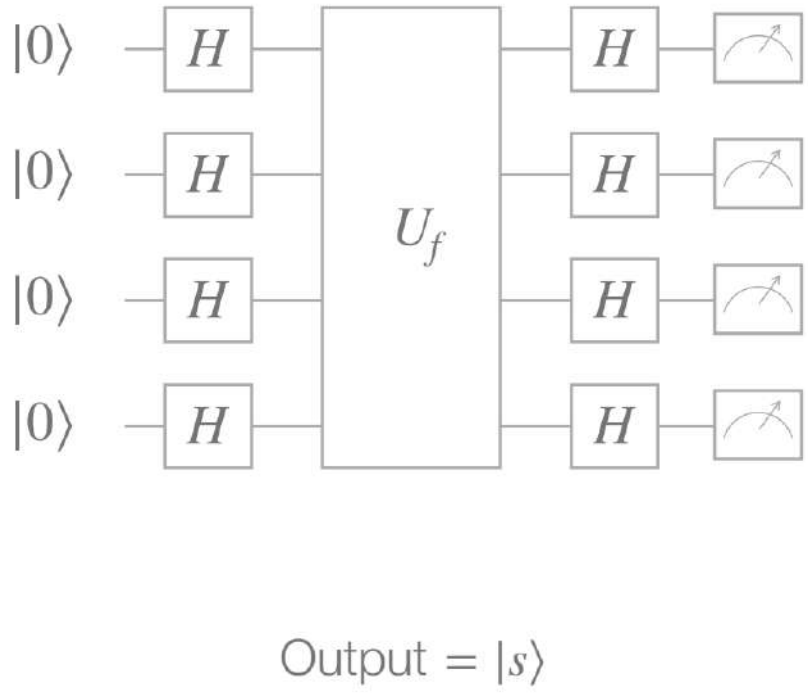

Figura 6 – Circuito representando o algoritmo de Bernstein-Vazirani. Uma string de zeros é fornecida. Logo depois, a porta Hadamard é aplicada, seguida do Oráculo e por fim aplicando Hadamard novamente. O resultado é a string que queriamos descobrir.

Fonte: Slide da disciplina de computação e informação quântica ministrada pelo professor Daniel Brod.

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \tag{5.9}$$

Diferente do caso do algoritmo de Deutsch–Jozsa, onde o termo de fase $(-1)^{a.x}$ aparece, aqui ele não está presente, uma vez que a string inicial é inteiramente formada por 0s. Logo, teremos sempre que $(-1)^{a.x} = 1$.

Depois, o oráculo será aplicado, onde vamos obter

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{s.x} |x\rangle \tag{5.10}$$

onde s é a string que queremos revelar. A próxima etapa é aplicar Hadarmard novamente em todos os bits do estado. Ao fazer isso, os qubits, antes nos estados $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ou $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, passarão para o estado $|0\rangle$ ou $|1\rangle$, respectivamente. Ao medir na base computacional, finalmente obteremos a string s, como queríamos.

Capítulo 6

O cassino quântico

6.1 Introdução ao cassino

Em vários ramos do conhecimento, é muito comum mapear problemas e conceitos em jogos e isso não é diferente na física. Quando se fala em mecânica quântica, a primeira coisa que vem a cabeça é sua peculiaridade, principalmente sua natureza probabilística. O que tem a mesma natureza e faz parte do cotidiano são alguns tipos de jogos, principalmente jogos de azar. Dessa forma, é muito útil como proposta pedagógica mapear comportamentos da teoria quântica para um cassino. No entanto, o que vamos explorar aqui é mais forte ainda do que somente mostrar comportamentos probabilísticos. Será mostrado que algumas estatísticas contrariam o senso comum e, a princípio, não deveriam ser possíveis. Para mostrar isso, vamos usar todo o aparato teórico visto até o momento, tanto de conceitos, quanto de algoritmos.

De fato, mapear em um cassino parece ser o caminho mais natural, já que qubits e observáveis podem ser mapeados em cartas e o ato de virar uma carta (medir). Para codificar as informações das 52 cartas, é possível usar 6 bits, já que com essa quantidade conseguimos exibir $2^6 = 64$ valores possíveis. Além disso, para casos de estados emaranhados, como já foi visto, um qubit para a cor e outro para o naipe pode também ser utilizado.

6.2 Jogo do vidente

6.2.1 O paralelo entre as caixas e o cassino

Na parábola do vidente o paralelo com o comportamento quântico é feito através de caixas. No entanto, em vez disso, vamos utilizar cartas e o ato de abrir a caixa estará associado com o ato de virar uma carta que inicialmente está voltada para baixo.

6.2.2 O caso clássico

Nesse cassino, temos alguns jogos e um deles consiste em adivinhar, entre três cartas, duas de naipes de cor igual (duas cartas pretas ou duas vermelhas). No entanto, parece que ninguém jamais é capaz de acertar. Isso parece bastante estranho e um jogador, depois de tentar uma quantidade enorme de vezes e não ganhar nenhuma vez, percebeu que tinha algo errado, já que estatisticamente não era para isso acontecer.

Depois de um tempo, se percebeu que, na verdade, todas as vezes que um jogador escolhia duas cartas com naipes de mesma cor, um laser escondido na parte de baixo da mesa se encarregava de pintar uma das cartas da outra cor, de forma que jamais alguém ganharia o jogo. Depois que essa informação foi exposta, o cassino precisou recuperar a confiança de seus clientes e, ao mesmo tempo, queria ficar mais próximo do lucro que costumava ganhar trapaceando. Esse, apesar se ser um exemplo de contextualidade, é uma contextualidade forçada, pois classicamente precisamos de uma interferência dinâmica no jogo, diferente de um caso quântico, que seria naturalmente contextual. Para trazer essa naturalidade ao jogo, o dono do cassino, que era físico, decidiu criar um cassino quântico, onde agora os jogos de adivinhação iriam seguir as leis da mecânica quântica. Será que dessa forma seria possível obter vantagem estatística sobre o comportamento clássico para não precisar mais trapacear?

Para isso, o físico, dono do cassino, pensou o seguinte: imagine que temos um número $n > 3$ de cartas para adivinhar e somente certos pares para serem medidos juntos. Particularmente, as cartas seriam colocadas em círculos, onde somente as adjacentes podem ser medidas juntas.

Ainda classicamente, vamos imaginar um número ímpar de medições relacionadas aos pares adjacentes de cartas, que denotaremos como $\{M_a | a = 1, ..., n\}$, tal que para todos os índices $\boldsymbol{a}$, M_a e $M_{a\oplus 1}$, serão medidos juntos, onde $\oplus$ representa a soma módulo n. Há pelo menos um caso onde temos cartas com naipes de cores iguais, pois como o número de cartas é ímpar e o primeiro e o último são adjacentes, ao menos uma vez isso acontecerá. Portanto, ao escolher um par de cartas aleatório, teremos uma chance de no máximo $1 - 1/n$ do resultado ser a favor da casa. Denotaremos isso por

$$R_n \leq 1 - \frac{1}{n}, \tag{6.1}$$

já que no máximo $n - 1$ pares podem ter resultados diferentes. Mas o que o dono do cassino quer saber é se com a teoria quântica, essa probabilidade é maior.

6.2.3 A vantagem quântica (com 5 cartas)

Vamos precisar de n operadores hermitianos para fazer as medições, dos quais os autovalores são 0 e 1, cada qual associado com uma cor. Sejam eles $\hat{X}_1, ..., \hat{X}_n$ e as medidas

denotadas novamente por $M_1, ..., M_n$. No caso de $n = 3$, que já foi visto, temos três operadores $\hat{X}_1, \hat{X}_2, \hat{X}_3$, que são comutativos dois a dois. Mas, nesse caso específico, eles acabam também sendo comutativos os três. Dessa forma, seria possível medir todos ao mesmo tempo de forma não-contextual. No entanto, se tivermos como hipótese $n > 3$, particularmente, podemos começar com $n = 5$, começamos a obter algo interessante.

Com isso em mente, o dono do cassino, foi buscar sobre o assunto na literatura, e encontrou um teorema proposto por Klyachko [14], que consiste no seguinte [7]. Vamos considerar que há uma base em que um sistema quântico é descrito por um espaço de Hilbert de dimensão 3, e todos os estados que vamos considerar deverão ter somente coeficientes reais. Portanto, esse sistema pode ser visto em um espaço Euclidiano de dimensão 3, onde os observáveis são projetores $\hat{X}_a = |l_a\rangle \langle l_a|$, e os vetores $\{|l_a\rangle : a = 1, ..., 5\}$ podem ser representados como

$$|l_a\rangle = (\sin\theta \cos\phi_a, \sin\theta \sin\phi_a, \cos\theta). \tag{6.2}$$

O angulo $\phi_a = \frac{4\pi a}{5}$, dependente de a, de forma que essa sequência de vetores formam um pentagrama. Conseguimos ver isso representado na figura (7), que é uma imagem mostrada em 2D, onde os vetores estão em 3D. Já o ângulo θ é escolhido de tal forma que os vetores adjacentes na sequência sejam ortogonais, ou seja, podemos dizer que $\langle l_a | l_{a\oplus 1}\rangle = 0$, sabendo que $\oplus$ representa a soma módulo 5. Por conta dessa ortogonalidade, observáveis adjacentes $\hat{X}_a, \hat{X}_{a\oplus 1}$ podem ser medidos juntos. A ortogonalidade é atingida quando $\cos\theta = \frac{1}{\sqrt[4]{5}}$. Podemos ver isso abrindo o produto interno entre dois vetores (6.2) adjacentes, isso nos dará $\sin^2\theta(\cos\phi_a \cos\phi_{a+1} + \sin\phi_a \sin\phi_{a+1}) + \cos^2\theta$. Sabendo que $\cos\phi_a \cos\phi_{a+1} + \sin\phi_a \sin\phi_{a+1} = \cos(\phi_a - \phi_{a+1})$ e que a diferença entre os ângulos ϕ_a é de $\frac{4\pi}{5}$, basta isolar o cosseno na equação para obter o resultado.

Agora, vamos considerar que temos um estado quântico $|\psi_1\rangle$ que está posicionado bem no eixo de simetria do pentagrama, de tal forma que o ângulo entre o vetor que representa esse estado e os vetores $|l_a\rangle$ que formam o pentagrama é θ. Na medição de qualquer par de observáveis adjacentes $\hat{X}_a$, $\hat{X}_{a\oplus 1}$, ou somente uma delas nos dará resultado 1, que é no caso em que os resultados são anti correlacionados, ou então ambos produzem o resultado 0. A probabilidade de resultados diferentes é $2\cos^2\theta$. No entanto, sabendo que o valor de $n = 5$ para o caso clássico nos daria $R_5 \leq 1 - \frac{1}{n} = \frac{4}{5}$ e para o caso atual, sabendo que $2\cos^2\theta = \frac{2}{\sqrt{5}}$, temos a seguinte violação na inequação (6.1):

$$R_{5,\text{quântico}} = \frac{2}{\sqrt{5}} = 0.89 \not\leq \frac{4}{5}. \tag{6.3}$$

De fato, com $n = 5$, a mecânica quântica traz uma violação no que já vimos. Pensando nisso, o dono do cassino percebeu que, usando essas características da natureza, ele poderia pensar em um jogo de 5 cartas na mesa, postas de forma circular, de forma que os

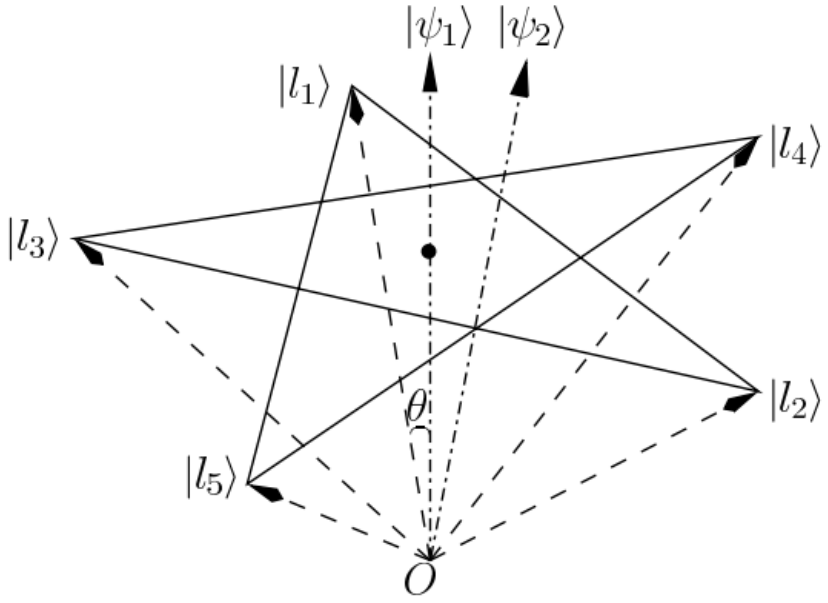

Figura 7 – Estados quânticos e observáveis usadas para ilustrar a prova de Klyachko.

Fonte: Imagem extraída de [7].

resultados 0 e 1 que vimos podem se tornar na verdade carta com naipe de cor vermelha e carta com naipe de com preta, assim ele conseguiria bolar o jogo já discutido, mas agora usando uma pequena vantagem oferecida pela mecânica quântica. Antes a chance do jogador ganhar era de 20% e agora passaria a ser 11%. Talvez essa seja uma vantagem pequena da casa e, além disso, o jogo estaria disponível somente com 5 cartas, o que não é algo muito produtivo em um cassino. Sabendo disso, seria possível generalizar esse modelo para qualquer número (ímpar) de cartas? E ainda, se for possível, seria oferecida uma vantagem estatística maior?

6.2.4 Generalização para qualquer quantidade de cartas

Os resultados obtidos por Klyachko podem ser generalizados da seguinte forma. É definido um número n (ímpar) de observáveis pelos projetores nos vetores $\{|l_a\rangle : a = 1, ..., n\}$, em que cada $|l_a\rangle$ é definido como na equação (6.2), só que dessa vez com o valor do ângulo sendo $\phi_a = \frac{n-1}{n}\pi a$ e com θ escolhido de forma que o $\langle l_a|l_{a\oplus 1}\rangle = 0$, onde $\oplus$ é a soma módulo n, pelos mesmos motivos anteriores. Essa condição de ortogonalidade é atingida quando $\cos^2\theta = \frac{\cos\frac{\pi}{n}}{1+\cos\frac{\pi}{n}}$. E esse conjunto de n vetores formam o que é conhecido como um $n/\frac{n-1}{2}$ polígono estelar [7, 15]. É possível notar que no caso em que $n = 5$, voltamos ao caso anterior. Os casos $\frac{5}{2}$, $\frac{7}{2}$ e $\frac{9}{2}$ podem ser vistos na figura (8). Agora, novamente, vamos preparar um estado quântico que estará posicionado bem no eixo de simetria do polígono estelar. Dessa forma então, seguindo o mesmo raciocínio anterior, vamos ter que:

$$R_n = R_{n,\text{quântico}} = \frac{2\cos\left(\frac{\pi}{n}\right)}{1+\cos\left(\frac{\pi}{n}\right)} \not\leq 1 - \frac{1}{n}. \tag{6.4}$$

Assim como no caso em que $n = 5$, temos agora o caso onde, para qualquer valor de n ímpar, temos a violação da inequação fornecida pelo caso clássico. E ainda, é possível mostrar que quanto maior o valor de n, mais a probabilidade quântica se aproxima de um, ou seja, 0% de chance de algum jogador ganhar, seguindo a equação, que pode ser vista com mais detalhe em [7]:

$$R_{n,\text{quântico}} \approx 1 - \frac{\pi^2}{4n^2}. \tag{6.5}$$

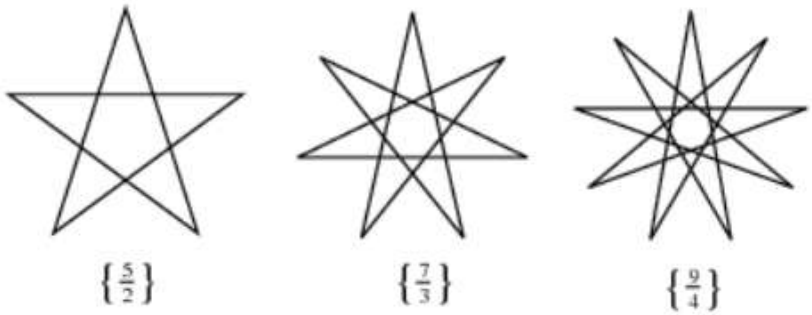

Figura 8 – Polígonos estelares para n = 5,7 e 9.

Fonte: Imagem extraída de [7].

Por tudo que foi visto, é importante ressaltar que, usando as correlações quânticas para n medidas, o dono do cassino pode alcançar algo muito próximo dos fins que alcançou trapaceando. Especificamente, ele pode construir uma previsão do jogo tal que os jogadores que acabam raciocinando classicamente, pensam que o jogo é justo, ou seja, eles acham que a chance de ganhar é razoável e que, portanto, é provável que algum jogador ganhe, quando na verdade não é, porque o clássico raciocínio não se aplica à realidade do jogo. Com um número pequeno de cartas, como já vimos, a probabilidade de um jogador ganhar é quase metade do caso clássico e conforme aumentamos o número de cartas no jogo, tanto o comportamento clássico quanto o quântico diminuem as chances do jogador ganhar, o clássico diminui linearmente e o quântico de forma quadrática.

6.2.5 Juntando tudo

Esse nosso jogo de cartas dentro do cassino, a parábola do vidente e o teorema mostrado estão relacionados uns com os outros. Na parábola, cada pretendente tem que adivinhar se um par de caixas está cheio ou vazio. Se a previsão sobre as duas caixas estiver correta, ele ganha, se não, ele perde. Da mesma forma, para o nosso jogo de cartas, elas estarão

viradas para baixo e o jogador precisa escolher duas que tem os dois naipes da mesma cor para ganhar. Sabendo disso, com que probabilidade o jogador que adivinha no caso clássico vai ganhar?

Supondo que ele sabe que o cassino é adversário e então ele pensa que a preparação do jogo é feita sob uma configuração clássica que torna sua tarefa tão difícil quanto possível. Como um bom jogador, conhecedor de jogos de azar, ele é levado a acreditar que a configuração é aquela em que apenas um par adjacente de cartas tem de fato a mesma cor, já que para um jogo com um número ímpar de cartas, se presume que em pelo menos um par, existe essa configuração. Assim, o jogador espera que sua probabilidade de ganhar seja a probabilidade de que ele adivinhou corretamente qual de todos os n pares é o correlacionado. De fato, a probabilidade de a previsão do jogador ser a realidade no caso clássico é da ordem de $\frac{1}{n}$ enquanto no caso quântico é da ordem de $\frac{1}{n^2}$. Sendo assim, vamos dizer que temos um número x (grande) de competidores. Se o operador da mesa do jogo escolher um número de cartas maior que ou igual a n e menor que ou igual a n^2, esses jogadores vão acreditar que é muito provável de pelo menos um deles ganhar, quando na verdade é muito provável justamente o oposto, que nenhum deles ganhe. Portanto, vimos que usando esses tipos de correlações, o dono do cassino consegue ainda tem muito lucro e agora sem trapacear. E ainda, que quanto maior o número de cartas na mesa, maior a chance de nenhum jogador ganhar.

6.2.6 O jogo na prática

Para termos uma noção da proposta, é interessante imaginar um jogo como esse aplicado a um cenário real. Vamos imaginar que temos o jogo de 5 cartas em que sempre há somente um par de cartas com as mesmas cores, ou seja, onde das 5 combinações, somente uma delas é boa para o jogador. Para participar do jogo, cada jogador precisa apostar um valor inicial.

Com o pensamento clássico, a casa calcula que o valor apostado por rodada, dará um lucro de 600% do valor investido pelo jogador, caso ele vença. No entanto, caso ele não acerte, perde todo o dinheiro apostado naquela rodada. Como classicamente, a probabilidade de acerto do jogador é de 20%, estima-se que a cada 5 tentativas, ele acertará uma só vez e cassino ganhará outras 4 vezes. Se fizermos as contas e o jogador apostar 100 reais a cada rodada, na média, ele sairá no lucro, já que perdendo 4 vezes o jogador perde 400 reais, mas ganhando uma, ganha 700!

É claro que, como todo jogo de azar, em algum subconjunto de tentativas, o cassino pode sair no lucro. No entanto, na média, se o jogo for jogado uma quantidade suficiente de vezes, o jogador sempre sairá na vantagem. Um exemplo disso, pode ser visto no seguinte gráfico representado na figura (9), que mostra a quantidade de dinheiro do jogador durante o jogo com as regras clássicas e as hipóteses descritas, o que seria esperado em um cenário

comum de jogo. Aqui o jogo descrito foi um bloco de 100 tentativas, onde em cada rodada, o jogador aposta 100 reais e, no fim, o jogador, que começou com 100 mil reais, conseguiu ter um lucro de aproximadamente 6 mil reais.

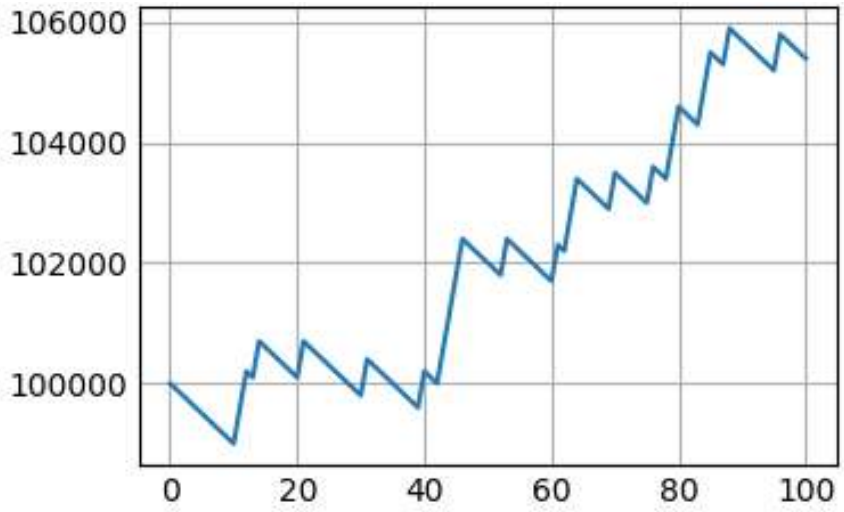

Figura 9 – Gráfico de uma simulação de 100 tentativas do jogador, onde o eixo x representa a quantidade de jogos, enquanto o eixo y, representa o dinheiro total do jogador.

No entanto, no caso do cassino usar o artifício da teoria quântica que descrevemos, ele poderia obter lucros enquanto o esperado era de que o jogador é que o obtivesse. Como foi visto, se seguirmos essas condições, a chance do cliente ter a sorte de ganhar, é agora, não mais 20%, mas os 11% no caso das 5 cartas. Nesse caso, se imaginarmos que ele tenha chegado novamente no cassino com 500 reais e jogue 5 rodadas do jogo, na média, ele estará perdendo dinheiro!

Com essas novas regras, ele precisaria de pelo menos cerca de 10 tentativas antes de obter seus 600% de lucro em média. Dessa forma, os 600%, apesar de serem um ótimo retorno, não serão mais suficientes para cobrir as apostas feitas. O que acontecerá em média, caso ele tenha o mesmo comportamento anterior, é perder 9 vezes, ou seja, cerca de 900 reais e ganhar uma vez, onde, nesse caso, ele ganhará os mesmos 600 reais de lucro (tendo 700 no retorno total no caso de vitória), de forma que no fim dessas 10 apostas, se o jogador entrar com 1000 reais no cassino sairá com cerca de 800, levando a um prejuízo de 200 reais no final.

A peculiaridade dessa história é que o jogador entra no jogo tendo a certeza de que jogando uma quantidade razoável de vezes, ele vai ter lucro com as apostas. No entanto, não é isso que acontece. Esse comportamento pode ser mostrado na figura (10), que assim como antes, mostrar um gráfico da quantidade de vezes jogadas e o dinheiro total do jogador, onde o jogador sairá no prejuízo.

Imagine agora um caso com mais peso estatístico, para que a comparação seja feita de

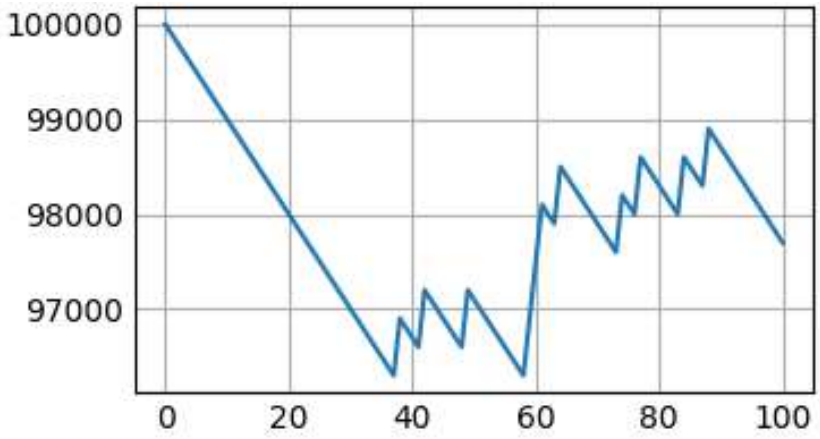

Figura 10 – Gráfico de uma simulação de 100 tentativas do jogador, onde o eixo x representa a quantidade de jogos, enquanto o eixo y, representa o dinheiro total do jogado.

forma precisa. Nesse caso mais geral, vamos pensar em um exemplo com 1000 jogadas, onde a diferença entre o comportamento clássico e quântico fica ainda mais evidente, excluindo o fator sorte. A diferença fica bastante clara no fim das 1000 rodadas, como pode ser visto na figura (11), onde o caso clássico está representado em azul e o quântico em verde. No primeiro caso, o jogador claramente sai no lucro, onde entra com 100 mil e sai com cerca de 140 mil. Já no segundo caso, ele entre com a mesma quantidade, mas sai com cerca de 70 mil, tendo um prejuízo de cerca de 30mil.

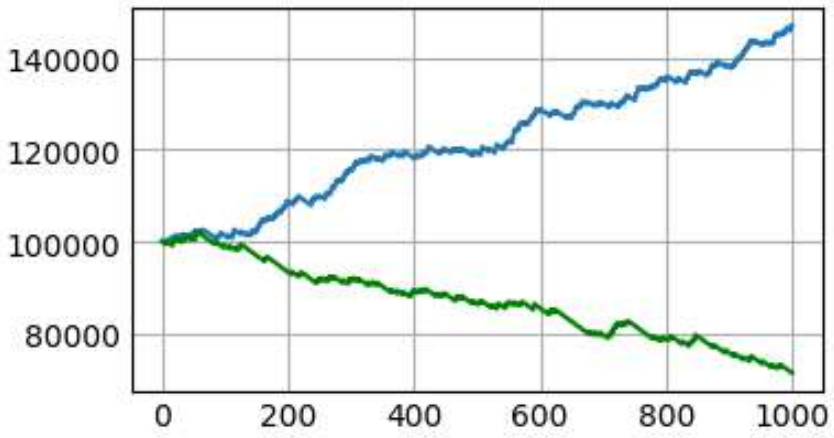

Figura 11 – Gráfico de uma simulação de 1000 tentativas do jogador, onde o eixo x representa a quantidade de jogos, enquanto o eixo y, representa o dinheiro total do jogador. O gráfico em azul representa o caso clássico e o gráfico verde é o caso quântico.

É importante ressaltar que para termos uma noção do comportamento do caso clássico e quântico, é importante ter uma amostragem de quantidades jogadas razoável, como

feita anteriormente. Jogando uma quantidade baixa, não seria possível distinguir de o jogador está tendo sorte, azar ou se existe um padrão de comportamento para aquele jogo. Isso pode ser facilmente notado no gráfico da figura (11). No inicio, durante as primeiras rodadas, os gráficos verde e azul se sobrepõem. No inicio, o jogador mesmo jogando om as regras quânticas acaba tendo sorte. Mas com o decorrer do jogo, a diferença fica bastante chamativa. Dessa forma, quando o usuário joga quantas vezes quiser, pode escolher jogar poucas vezes. Muitas vezes o fator sorte será levado em consideração, no entanto, o cassino terá lucros na média, ao usar o artifício quântico e não levantará nenhuma suspeita.

6.3 Adivinhação de strings de bits

Imagine agora, que temos um jogo envolvendo bolinhas pretas e brancas, onde dado uma sequência secreta secreta de 8 bolinhas, que só um computador do cassino sabe, o jogador precisa acertar essa sequência. No entanto, ele só tem um número determinado de chances de acertar. Classicamente, quantas tentativas seriam necessárias até acertar? Como vimos anteriormente, se consegue saber um bit de cada vez a cada tentativa de descobrir a sequência. Quanticamente, ele só precisaria fazer uma pergunta, e, usando o algoritmo de Bernstein-Vazirani, conseguirá descobrir a sequência.

Um outro jogo interessante de ilustrar é o mastermind, que tem um paralelo com o jogo acima das bolinhas. A diferença é que agora as bolinhas não seriam de duas cores, mas sim coloridas. Uma ideia para representar cada cor seria mapear cores em bits. Suponha que temos 4 cores disponíveis, que poderiam ser representadas por 2 bits. Suponha também que teremos agora 4 bolinhas para montar a sequência secreta. Uma forma de representar isso poderia ser através de uma string de 8 bits, onde as cores de cada bolinha estariam associadas aos bits 2 a 2 da string. Com esse mapeamento, seria, em tese, possível preparar esse jogo e, fixar um número de tentativas disponíveis para o jogador acertar. Com isso em mente, ver como o algoritmo de Bernstein-Vazirani soluciona o jogo de forma única, com somente uma rodada.

Um exemplo interessante sobre como implementar o algoritmo na prática pode ser visto no apêndice, onde uma integração com um computador quântico foi feito e um número de tentativas fixado para acertar uma string. O resultado pode ser interpretado por um microcontrolador, trazendo esse aparato teórico para a realidade.

Capítulo 7

Conclusões

Apesar de inicialmente o comportamento probabilístico e a não compatibilidade da mecânica quântica entre realismo, localidade e não contextualidade parecerem um problema para fins computacionais, é exatamente essa diferença que traz ganhos em algumas tarefas. O protocolo BB84 usa essas características para trazer uma forma da própria natureza de fazer distribuição de chaves criptográficas. O emaranhamento, que foi alvo de críticas iniciais, é o coração do protocolo de teletransporte. E os algoritmos de Deutsch–Jozsa e principalmente o de Bernstein-Vazirani fornecem uma boa ideia das vantagens computacionais quânticas para alguns problemas. A apresentação do cassino traz discussões sobre vantagens de usar as regras da mecânica quântica em um jogo de cartas em relação às regras da mecânica clássica e pode ser usado como ferramenta pedagógica.

Além disso, é possível perceber que, atualmente, estamos bem no meio de uma fronteira do conhecimento referente a muitos pontos da física moderna e de suas aplicações, como a computação quântica. Quando pensamos nisso, não há como deixar de fora a metáfora usada pelo cientista brasileiro Marcelo Gleiser no livro "A ilha do conhecimento"[19]. Nesse livro, ele compara o conhecimento humano com uma ilha e, como toda ilha, tem a sua borda, que é justamente a fronteira entre o que sabemos e o oceano do desconhecido. Esse desconhecimento é associado a novas perguntas que podemos fazer. Um exemplo disso é a própria mecânica quântica, que podemos associar a uma ilha muito pequena no início do século 20. Muito pouco se sabia sobre ela. A medida em que fomos conhecendo mais e respondendo esses questionamentos iniciais, mais a nossa ilha cresceu e ainda, com esse crescimento, a fronteira que a separa do desconhecido também aumentou, ou seja, quanto mais perguntas respondemos, a quantidade de novas só aumenta. Será que um dia o oceano irá secar? Há respostas para todas as perguntas? Quanto realmente sabemos sobre o mundo? Existe mesmo uma verdade absoluta? Será que a mecânica quântica não tem estranheza alguma, mas nós que somos grandes demais para compreender? Todas essas indagações são filosóficas demais para serem quantizadas, assim como o emaranhamento

era quando foi previsto... uma pequena fronteira dentre as milhares a serem exploradas.

Apêndice A

Implementação do algoritmo de Bernstein-Vazirani usando qiskit

O primeiro passo para a implementação do algoritmo e executar em um computador quântico, é criar uma conta na IBM através desse link https://quantum-computing.ibm.com/. Através disso, é possível gerar uma chave para se comunicar com a API responsável pelo qiskit.

Para salvar localmente as credenciais para futuras requisições, rodar esse comando quando for a primeira vez e passar a chave de API adquirida no passo anterior como parâmetro.

O código (em python) para implementar o algoritmo é o seguinte:

```
#import qiskit
from qiskit import *

#Pedir string secreta e quantidade de vezes que o algoritmo vai tentar
                                        descobrir
stringSecreta = input('Jogador 1: Digite a string secreta de 4 bits:')
quantidadeTentativas = int(input('Quantas vezes quer tentar'))


#circuito com 5 qubits (4 qubits zerados e 1 auxiliar) + 4 bits
                                        classicos pra exibir o resultado
circuito = QuantumCircuit(len(stringSecreta)+1,len(stringSecreta))

#Aplicar Hadamard nos 5 qubits
circuito.h(range(len(stringSecreta)))

#Aplicar X e H no qubit auxiliar
circuito.x(len(stringSecreta))
```

```
circuito.h(len(stringSecreta))

#Aplicar o oraculo
for i, bit in enumerate(reversed(stringSecreta)):
    if bit == '1':
        circuito.cx(i,len(stringSecreta))

#Aplicar novamente Hadamard nos 4 qubits
circuito.h(range(len(stringSecreta)))

#Escrever na string cl ssica
circuito.measure(range(len(stringSecreta)), range(len(stringSecreta)))

#Salvar a chave obtida localmente. Precisa ser executado na primeira vez
                                    . Depois, a credencial fica salva
                                    localmente
IBMQ.save_account('chave API')

#Carregar credencial salva localmente
IBMQ.load_account()

#Chamar provedor publico para conex o
provider = IBMQ.get_provider(hub='ibm-q')
provider.backends()

#Procura o computador quantico menos ocupado para rodar o algoritmo
backend = least_busy(provider.backends(filters=lambda x: x.configuration
                                    ().n_qubits <= 5 and x.configuration
                                    ().n_qubits >= 2 and not x.
                                    configuration().simulator and x.
                                    status().operational==True))

transpiled_bv_circuit = transpile(circuito, backend)

#Rodar com determinado numero de tentativas
job = backend.run(transpiled_bv_circuit, shots=quantidadeTentativas)

job_monitor(job, interval=2)
results = job.result()
resposta = results.get_counts()

#Exibir string obtida pelo algoritmo
print(list(reposta.keys())[0])
```

Referências

1 Eleanor Rieffel and Wolfgang Polak, Quantum computing : a gentle introduction (MIT Press, 2011).

2 Michael Nielsen and Isaac Chuang, “Computação quântica e informação quântica”, Editora Bookman (2005) .

3 L. Grover. In Proc. 28th Annual ACM Symposium on the Theory of Computation, pages 212-219, ACM Press, New York (1996).

4 P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings, 35th Annual Symposium on Foundations of Computer Science, IEEE Press, Los Alamitos, CA (1994).

5 C. H. Bennett et al., Phys. Rev. Lett. 70, 1895 (1993).

6 J. S. Bell, Physics 1, 195 (1964).

7 S. Kochen and E. P. Specker, "The problem of hidden variables in quantum mechanics", Journal of Mathematics and Mechanics 17, 59–87 (1967).

8 S. Abramsky and A. Brandenburger. “The sheaf-theoretic structure of non-locality and contextuality“. New J. Phys. 13, 113036 . arXiv:1102.0264 [quant-ph](2011).

9 A. Peres. Incompatible results of quantum measurements. Phys. Lett. A, 151(3-4):107–108, 1990.

10 E. F. Galvão. Foundations of quantum theory and quantum information applications (2002)

11 A. Einstein, B. Poldosky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, Phys. Rev., 47 (1935) 777-780.

12 Laura Sanders Science News quantum entanglement (2010).

13 Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA), Gilles Brassard (dept. IRO, Univ. de Montreal, H)C 3J7 Canada) "Quantum cryptography: Public key distribution and coin tossing"

14 A. A. Klyachko, M. A. Can, S. Binicio˘glu, and A. S. Shumovsky, Phys. Rev. Lett. 101, 020403 (2008).

15 H. S. M. Coxeter, Regular Polytopes, Dover Publications (1973).

16 Ethan Bernstein and Umesh Vazirani (1997) "Quantum Complexity Theory"SIAM Journal on Computing, Vol. 26, No. 5: 1411-1473

17 Mermin, N. D., Phys. Today 43, 9 (1990).

18 FAPESP A fórmula do emaranhamento.

19 Marcelo Gleiser, A ilha do conhecimento: Os limites da ciência e a busca por sentido.