

UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
FÍSICA-LICENCIATURA

GABRIEL GUSTAVO BLUM

AS IMPLICÂNCIAS DO ENTRELAÇAMENTO QUÂNTICO NA COMPUTAÇÃO

CERRO LARGO

2022

GABRIEL GUSTAVO BLUM

AS IMPLICÂNCIAS DO ENTRELACAMENTO QUÂNTICO NA COMPUTAÇÃO

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção de grau de Licenciado em Física pela Universidade Federal da Fronteira Sul (UFFS) - Cerro Largo

Orientador: Thiago de Cacio Luchese

CERRO LARGO

2022

Bibliotecas da Universidade Federal da Fronteira Sul - UFFS

Blum, Gabriel Gustavo

As implicações do entrelaçamento quântico na
computação / Gabriel Gustavo Blum. -- 2022.

45 f.:il.

Orientador: Doutor Thiago de Cacio Luchese

Trabalho de Conclusão de Curso (Graduação) -
Universidade Federal da Fronteira Sul, Curso de
Licenciatura em Física, Cerro Largo, RS, 2022.

1. Criptografia Quântica. 2. Entrelaçamento Quântico.
3. Computação Quântica. 4. Desigualdades de Bell. 5.
Teletransporte. I. Luchese, Thiago de Cacio, orient. II.
Universidade Federal da Fronteira Sul. III. Título.

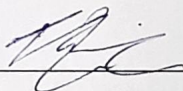
GABRIEL GUSTAVO BLUM

AS IMPLICÂNCIAS DO ENTRELAÇAMENTO QUÂNTICO NA COMPUTAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Física - Licenciatura da Universidade Federal da Fronteira Sul (UFFS), como requisito para obtenção do título de licenciado em Física.

Este trabalho de conclusão de curso foi defendido e aprovado pela banca em: 01/04/2022

BANCA EXAMINADORA



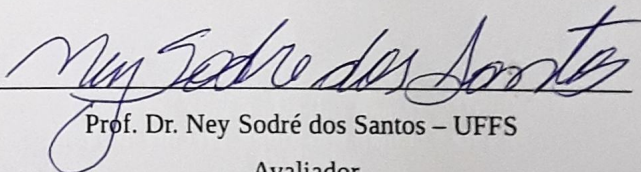
Prof. Dr. Thiago de Cacio Luchese – UFFS

Orientador



Prof. Dr. Márcio do Carmo Pinheiro – UFFS

Avaliador



Prof. Dr. Ney Sodr  dos Santos – UFFS

Avaliador

Dedico esse trabalho aos meus pais, pois esses nunca mediram esforços para que eu pudesse concluir o meu curso.

AGRADECIMENTOS

Quero agradecer primeiramente a Deus e aos meus pais, pelo privilégio do dom da vida, pois se não fossem eles eu não teria escrito essas palavras.

Agradeço também, de modo especial, ao meu orientador, o professor Dr. Thiago de Cacio Luchese, e em nome deles a todos os demais professores, que foram de suma importância para construção do meu conhecimento, alicerce para minha posterior formação.

Agradeço à banca avaliadora, pela sua disposição e contribuição.

Agradeço à instituição de ensino superior, a Universidade Federal da Fronteira Sul (UFFS), campus Cerro Largo-RS, pelo acolhimento e apoio.

Agradeço também a todos os meus colegas de curso, que foram de grande importância nessa longa jornada da graduação. Agradeço pelo apoio, pelas brincadeiras, e também pelos momentos de estudo e compartilhamento de conhecimento.

Por último, mas não menos importante, agradeço a todos os meus amigos, que de uma ou outra forma vieram a contribuir para que eu pudesse escrever esse trabalho.

A todos vocês, o meu mais singelo agradecimento!!!!

E lembrem-se...

“Por mais árdua que seja a batalha, não desanime, e use o desejo da vitória como energia para seguir em frente” Gabriel G. Blum

*“Se a mecânica quântica não te assustou, então
você não a entendeu ainda.”*

(Niels Bohr)

RESUMO

No início, os computadores eram gigantescos e necessitavam de salas inteiras para sua instalação e funcionamento. Entretanto, com o passar dos anos, esses foram aperfeiçoados e hoje cabem na palma da mão. Porém, chegamos ao limite de diminuição desses dispositivos, sendo tais limitações impostas por restrições físico-químicas dos materiais utilizados em sua construção, de modo que, ao tentar diminuir ainda mais o tamanho dos componentes, eles podem perder sua principal função de ser semicondutores. Essa pesquisa tem por objetivo principal investigar de modo qualitativo as implicações do estudo do entrelaçamento quântico na construção de computadores quânticos que, em resumo, teriam grande poder de processamento, alta velocidade e ocupariam espaços ínfimos. Esse trabalho visa também perquirir a implicação do entrelaçamento quântico no âmbito da segurança e criptografia de dados virtuais onde, por meio de particularidades desse fenômeno, é impossível a violação e espionagem de dados. Por meio do estudo das literaturas disponíveis, percebe-se que a computação quântica mudará os aspectos atuais em relação à computação. Fundamentados nos princípios do entrelaçamento quântico, computadores super velozes e com alto nível de segurança poderão ser desenvolvidos. O presente trabalho poderá servir como introdução a temática para pessoas com interesse de estudo na área, bem como material de estudo para o público em geral.

Palavras chave: Entrelaçamento quântico. Computação. Criptografia.

ABSTRACT

In the beginning, computers worked perfectly and needed all computers for their installation and installation. However, over the years, these were perfected and today chillin in the palm of your hand. However, we have reached the limit of such devices, being even more established in the physical devices of the materials used in their construction, when trying to reduce the main component of the taman hoele dos mais o taman. The main objective of this time is to investigate the qualitative research of the process, phyllody and the research of the qualitative way of antication and in the construction of computers which, in summary, will have great velocarian power and in a quantum process. This work also aims at the implication of entanglement in the scope of security and encryption of virtual data where, through specific data of this phenomenon, a data and data breach is impossible. Through the study of the available literature, it is clear that quantum computing will change current aspects of computing. Based on the principles of quantum entanglement, super-fast computers with a high level of security can be developed. This work can serve as an introduction to people interested in studying the area, as well as study material for the general public.

Keywords: Quantum entanglement. computing. Cryptography.

LISTA DE QUADROS E FIGURAS

QUADRO 1 - Transformação de decimal para binário e sua representação no byte.....	13
FIGURA 1 - Representação dos resultados do experimento da Dupla Fenda.....	18
FIGURA 2 - Esquema experimental para detecção da orientação dos spins.....	27
FIGURA 3 - Esquema do experimento do grupo Zeilinger.....	32
FIGURA 4 - Esquema do experimento de Hardy.....	34
FIGURA 5 - Teletransporte de um estado quântico.....	36
QUADRO 2 - Tempo de fatoração por um algoritmo clássico e pelo algoritmo de Shor.....	39

LISTA DE ABREVIATURAS E SÍMBOLOS

BBO	Beta Barium Borate
BS	Beam Splitter
CHSH	Experimento para verificação das desigualdades de Bell
ENIAC	Electronic Numerical Integrator And Computer
HWP	Half-wave plate
MQ	Mecânica quântica
ULA	Unidade lógica e aritmética
PBS	Polarizing beam splitter
$ \Psi\rangle$	Operador da função de onda
$ \psi ^2$	Densidade de probabilidade da função de onda
\hbar	Constante de Planck reduzida (normalizada)
λ	Conjunto de variáveis ocultas
∇	Gradiente da função de onda

SUMÁRIO

1	INTRODUÇÃO.....	12
2	COMPUTAÇÃO QUÂNTICA: COMO TUDO COMEÇOU.....	15
3	EQUAÇÃO DE SCHRODINGER.....	16
	3.1 O EXPERIMENTO DA DUPLA FENDA.....	17
4	FORMULAÇÃO DE DIRAC E O ESPAÇO DE HILBERT.....	19
5	ENTRELAÇAMENTO QUÂNTICO.....	21
6	PARADOXO EPR E AS DESIGUALDADES DE BELL.....	24
	6.1 COMPROVAÇÃO EXPERIMENTAL DA DESIGUALDADE CHSH	30
	6.2 O EXPERIMENTO DE HARDY.....	33
7	TELETRANSPORTE: A POSSIBILIDADE DE SUPERPROCESSAMENTO..	35
8	IMPLICÂNCIAS NO PROCESSAMENTO DE DADOS E CRIPTOGRAFIA..	37
	8.1 PROCESSAMENTO QUÂNTICO.....	38
	8.2 CRIPTOGRAFIA E SEGURANÇA.....	39
9	CONCLUSÃO.....	42
	REFERÊNCIAS.....	43

1 INTRODUÇÃO

Nós humanos, somos seres racionais, e esse fato é o principal que nos diferencia dos demais animais, estamos em constante evolução intelectual (PORFÍRIO). Os últimos dois séculos em especial apresentaram um crescimento significativo no nosso conhecimento, principalmente no que tange o ramo de tecnologia. O primeiro computador eletrônico entrou em funcionamento em Fevereiro de 1946, sendo desenvolvido pela Electronic Control Company. Suas dimensões eram enormes e seu peso era de aproximadamente trinta toneladas, ficou conhecido como ENIAC, do inglês *ELETRONIC NUMERICAL INTEGRATOR AND COMPUTER*, e podia apenas ser usado por técnicos e profissionais da área. (BARBOSA, p.12)

Um computador é uma máquina que tem por principal objetivo facilitar e automatizar nossas tarefas. Ele pode ser dividido basicamente em duas partes: seu *hardware* e seu *software*. O hardware consiste na sua composição física, suas peças e a sua arquitetura, ou seja, de que forma foi construído. Já o software pode ser definido como sendo um “intérprete”, ou seja, ele é uma forma de dicionário, com o qual o ser humano consegue se comunicar com a máquina. (FILHO et al., 2008, p. 132-133)

Passados apenas pouco mais de 3/4 de século, muita coisa mudou em relação ao ENIAC. Hoje (2022), computadores cabem na palma de nossa mão e são manuseados pelo público em geral, sem a necessidade de uma formação específica na área. Entretanto, apesar de todas as evoluções quanto a parte estrutural, pouco mudou se olharmos o modo como ocorre seu funcionamento. Computadores, resumidamente, são máquinas que trabalham com arranjos de combinações, conforme será visto adiante.

Neste trabalho será abordado especificamente questões referentes ao funcionamento do processador, parte principal de um computador e responsável pela realização de tarefas impostas pelo usuário. Toda e qualquer requisição feita por um agente externo passa pelo processador, de modo que é possível dizer com certo grau de precisão que o processador é o cérebro do computador.

Por mais complexo que possa parecer, o processador nada mais é do que uma máquina de arranjos: o processador é constituído por uma série de transistores que são ligados de uma forma estratégica para permitir seu pleno funcionamento. Na computação clássica, esses transistores têm apenas duas possibilidades, ou estão “abertos” ou “fechados”. Na tecnologia da informação chamamos isso de binário, uma vez que cada transistor, individualmente, pode estar em apenas um de dois estados possíveis, ou aberto (valor 0), ou fechado (valor 1). Por

incrível que pareça, com apenas essas duas opções conseguimos representar e processar toda a informação existente atualmente. (BARBOSA, p.52-55)

A cada um desses transistores é dado o nome de “bit”. O bit, na informática, é a menor unidade de informação que pode ser processada/armazenada. Ou seja, 0 ou 1, aberto ou fechado, “é” ou “não é”. Com um bit de informação podemos armazenar apenas dois estados diferentes, o que não seria muito usual para o processamento de dados e armazenamento de informações, entretanto esse bits são organizados em grupos de oito, ao qual dá-se o nome de byte. Com o arranjo de oito bits pode-se representar duzentos e cinquenta e seis estados diferentes. Para termos uma ideia de como isso funciona, segue abaixo um quadro com a representação em binários dos números decimais do zero ao dez.

QUADRO 1 - Transformação de decimal para binário e sua representação no byte

Decimal	Binário	Estado do byte(8 bits)
0	0	00000000
1	1	00000001
2	10	00000010
3	11	00000011
4	100	00000100
5	101	00000101
6	110	00000110
7	111	00000111
8	1000	00001000
9	1001	00001001
10	1010	00001010

Fonte: Elaborado pelo autor

Para os entusiastas em matemática e que ficaram curiosos como essa tabela foi desenvolvida, segue um algoritmo de conversão de decimais para binários. O primeiro passo é obter o quociente da divisão do decimal a ser convertido:

$$\text{Quociente} = \text{decimal} / 2 \quad (1)$$

- 1- Se o resto da divisão inteira for diferente de 0, anota-se seu valor binário correspondente como sendo 1. Caso contrário anota-se 0.
- 2- Reserva-se apenas a parte inteira do quociente.

3- O processo 1 tem que ser realizado até o quociente ser menor que um.

4- Por fim anota-se a sequência do binário obtido em ordem inversa.

Veja, como exemplo a conversão do decimal 10:

$$\text{Quociente 1} = 10/2 \quad (2)$$

$$\text{Quociente 1} = 5 \quad (3)$$

Resto = 0 -----> binário 0.

$$\text{Quociente 2} = 5/2 \quad (4)$$

$$\text{Quociente 2} = 2 \quad (5)$$

Resto = 0,5 -----> binário 1.

$$\text{Quociente 3} = 2/2 \quad (6)$$

$$\text{Quociente 3} = 1 \quad (7)$$

Resto = 0 -----> binário 0.

$$\text{Quociente 4} = \frac{1}{2} \quad (8)$$

$$\text{Quociente 4} = 0,5 \quad (9)$$

Resto = 0,5 -----> binário 1.

Pegando o binário do fim pro início, obtém-se que o número dez em binário se torna 1010.

A partir dessa representação fica mais fácil ver que com um conjunto de oito bits podemos representar duzentos e cinquenta e seis estados e podemos exibir no máximo o número duzentos e cinquenta e cinco. Da mesma forma que os números, as letras e todos os parâmetros de imagens e até mesmo o som são codificados e transformados em binários, para que o processador possa interpretá-los e realizar a tarefa ao qual foi requisitada. Segundo Barbosa, nos processadores atuais, esse conjunto de instruções que diz como o processador vai realizar determinada tarefa é feito pela unidade aritmética e lógica (ULA).

Os processadores atuais, em sua grande maioria, possuem arquitetura de sessenta e quatro bits, ou seja, conseguem processar sessenta e quatro bits de informação a cada ciclo. Além desse quesito, o que delimita o quanto de tarefas simultâneas um computador/processador consegue realizar e qual será a velocidade de processamento dessas depende de dois principais fatores: a arquitetura e o *clock*. (BARBOSA, p.14-19)

Fazendo uma analogia simples, vamos imaginar que o processador seja um caminhão e as atividades a serem realizadas sejam o transporte de terra. Nesse raciocínio a arquitetura

do processador estaria relacionado com o volume de terra que conseguimos transportar por viagem, já o clock seria quantas viagens conseguimos realizar em um determinado intervalo de tempo. Logo, podemos chegar a uma relação muito simples:

$$\text{Quantidade de processamento} = \text{clock} \times \text{arquitetura} \quad (10)$$

No entanto, por maiores que tenham sido as evoluções desde a descoberta do computador, mais especificamente na construção de processadores, estamos chegando hoje a um limite físico-químico dos materiais utilizados em sua composição. Como já comentado, o processador é construído a partir de um conglomerado de milhões de transistores que são ligados e arranjados de modo a serem cada vez mais velozes, consumir menos energia e ser mais eficientes na realização das tarefas. Atualmente, encontram-se no mercado processadores com uma litografia de nove nanômetros. Porém, quando as dimensões envolvidas são muito pequenas acredita-se que o tunelamento quântico passe a ocorrer, ou seja, a barreira de potencial se torna pequena o suficiente para possibilitar que alguns elétrons troquem de níveis de potencial, fazendo com que o transistor passe a ser um condutor e perca sua principal função de ser uma espécie de interruptor, ora fechado, ora aberto. Com base nisso, estuda-se atualmente outras formas de construção dos processadores.

Nos últimos anos, muito se tem falado dos computadores quânticos, aos quais são atribuídas velocidades e poder de processamento que seriam impossíveis nos computadores clássicos. Dessa forma, passa-se a descrever um pouco sobre o entrelaçamento quântico e as suas implicações no processamento de dados computacionais.

2 COMPUTAÇÃO QUÂNTICA: COMO TUDO COMEÇOU

A computação quântica é um avanço muito significativo e promissor no que diz respeito à nossa incessante busca por tecnologia. Com o desenvolvimento desta tecnologia, buscamos alcançar um novo nível, superando todos os patamares que conhecemos hoje sobre processamento de dados e realização de tarefas computacionais.

O tema foi inicialmente sugerido pelo físico Richard Feynman em uma de suas palestras¹ no ano de 1959. Como já era entendido pela Mecânica Quântica, a matéria em pequena escala não responde mais às leis clássicas da física, ou seja, ao estudarmos e

¹ A palestra tinha por tema “There is plenty of room down there – an invitation for a new field of Physics”, essa tornou-se o segundo texto mais citado de Richard Feynman, sendo considerada como a primeira palestra sobre tecnologia e a engenharia em escala atômica. (SCHULZ, 2018, P. 1)

tentarmos compreender o mundo quântico, estamos mexendo com leis diferentes, de modo que podemos esperar resultados diferentes. (SCHULZ, 2018, p. 4)

Ao entrarmos no âmbito da Mecânica (MQ) Quântica e suas implicações no processamento computacional, novos conceitos e concepções são necessárias. Desse modo, visando seguir uma sequência lógica para o desenrolar desse tema, vamos tratar de algumas abordagens da MQ, bem como suas aplicabilidades no desenvolvimento de computadores quânticos. Começando por um olhar sobre a equação de Schroedinger, buscaremos compreender seu significado, bem como sua fundamentação física no que diz respeito a sua aplicabilidade no emprego de novas tecnologias. Na sequência, é de suma importância compreendermos um pouco o teorema das desigualdades de Bell, (conjunto de equações as quais descreviam a mecânica quântica como realista e local) para, dessa forma, ao final do trabalho, podermos explorar possíveis aplicabilidades do entrelaçamento quântico² no processamento computacional, bem como no âmbito da segurança e criptografia de dados.

3 EQUAÇÃO DE SCHROEDINGER

Diferente dos corpos a nível macro, as partículas a nível quântico não obedecem às leis da física clássica. No início do século XX, tampouco era possível descrever ou prever sua dinâmica ao longo do tempo, de modo que qualquer tentativa de descrever o estado futuro de um sistema pós interação se mostrava totalmente falha. Essa problemática permaneceu até Erwin Schroedinger propor sua equação³, que tinha por objetivo descrever com precisão um sistema de partículas quânticas, utilizando para isso alguns postulados e uma matemática precisa.

Vamos imaginar um elétron, o qual está livre para se mover nas três dimensões. O seu estado em um instante de tempo t pode ser perfeitamente descrito por uma quantidade complexa chamada de *função de onda*. Essa será representada pelo símbolo $\Psi(x,y,z,t)$, em que (x,y,z) são as coordenadas espaciais. (DONNANGELO; CAPAZ, 2009, p. 40)

Para um sistema clássico, ao falarmos em “estado” de uma partícula nos referimos ao feito de conseguir prever, com certo grau de precisão, a velocidade e posição de um determinado corpo que, somado às forças atuantes nesse mesmo corpo permitem a descrição

² Todo e qualquer sistema que pode estar em um estado de superposição de dois estados auto tratáveis. (YABU-UTI, 2007)

³ A equação de Schroedinger como ficou conhecida, foi proposta em 1926 pelo físico austríaco Erwin Schroedinger com o objetivo de mostrar a descrição da dinâmica quântica. Juntamente com o físico inglês Paul Dirac, Schroedinger foi agraciado com o Prêmio Nobel de Física em 1933. (DONNANGELO; CAPAZ, 2009, p. 41)

completa do sistema, sendo possível prever o movimento futuro e passado desse através das condições iniciais. Do mesmo modo, buscou-se o mesmo feito para um sistema quântico, o qual por ser um sistema ondulatório (diferente de um sistema clássico, que pode ser descrito a partir de uma equação horária do movimento), precisava de uma função temporal e espacial: a função de onda. A função de onda é uma representação matemática abstrata do estado de um sistema, que somente tem significado no contexto de uma teoria quântica. (DONNANGELO; CAPAZ, 2009, p. 42)

A partir disso, temos então que a equação de onda pode representar simultaneamente os aspectos corpusculares e ondulatórios de uma partícula em um sistema, de modo que a sua intensidade é definida como sendo a densidade de probabilidade de encontrarmos a partícula em determinada região do espaço, sendo essa densidade dada por $|\Psi|^2$.

A equação de Schroedinger, que descreve a função $\Psi(x,y,z,t)$, é a seguinte (GRIFFITHS, 2011, p.1):

$$i \hbar \frac{\partial \Psi}{\partial t} = - \frac{\hbar^2}{2m} \nabla^2 \Psi + V\Psi \quad (11)$$

De acordo com Carvalho:

Se a energia potencial for conhecida, pode-se utilizar a equação de Schroedinger para se obter a função de onda. Como esta é uma equação diferencial, a sua solução geral depende de constantes de integração. Uma das condições que nos vai permitir determinar o valor dessas constantes está relacionada com o significado físico da função de onda. Na verdade, como já foi referido, a intensidade da função de onda representa a densidade de probabilidade de se encontrar a partícula numa dada posição (CARVALHO, 2001, P. 2)

Essa interpretação probabilística permite até mesmo conciliar a teoria ondulatória da luz proposta por Maxwell com a afirmação de Isaac Newton de que a luz é formada por corpúsculos, dessa forma comportando-se como matéria. Com o objetivo de explicitar esse comportamento dual, abordaremos o experimento de Young, que mais tarde ficou conhecido como “experimento da dupla fenda”.

3.1 O EXPERIMENTO DA DUPLA FENDA

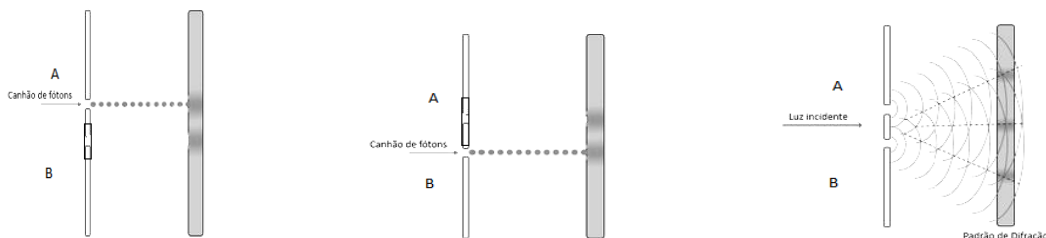
O experimento de Young, ou experimento da dupla fenda como ficou popularmente conhecido, consiste em um canhão emissor de fótons (as partículas associadas à luz)

direcionado para um anteparo que possui duas fendas, uma denominada de A e a outra de B. Essas fendas, por sua vez, possuem tamanho aproximado do comprimento de onda da luz emitida pela fonte. Após desse anteparo é instalado um segundo anteparo, o qual tem por finalidade detectar todo e qualquer fóton que passar por qualquer uma das fendas. Dessa forma, inicia-se o experimento. Primeiramente o canhão é acionado deixando-se aberto apenas a fenda A, conforme Figura 1. O que se observa é um padrão de comportamento corpuscular, onde os fótons estão mais concentrados logo atrás da fenda A e alguns, em menor quantidade, nas suas periferias, de modo que quanto mais afastado da parte logo atrás da fenda A menos densa é a quantidade de fótons detectados. De maneira semelhante, em um segundo processo de medida, fecha-se a fenda A e abre-se a B. Analogamente ao resultado anterior, observa-se uma densidade bem alta de fótons logo atrás da fenda B, densidade essa que diminui à medida que se afasta da parte logo atrás de B. Ambos esses resultados provam a natureza corpuscular da luz.

Em uma terceira parte do experimento, deixa-se as duas fendas abertas. O canhão é então acionado e, após passado algum tempo, observa-se uma detecção de fótons totalmente díspar aos dois primeiros casos: nesse são observadas faixas mais densas de colisões seguidas de faixas mais ralas, alternadamente (Ver Figura 1). Tal resultado só pode ser explicado ao se admitir uma natureza ondulatória aos fótons, uma vez que se trata de interferência ora construtiva, ora destrutiva.

Com o intuito de tentar detectar por qual das fendas cada fóton está passando, foram instalados dois sensores, um em cada uma das fendas. Manteve-se novamente as duas fendas abertas. Porém, diferentemente do que aconteceu no caso anterior, não obteve-se o resultado de comportamento ondulatório (interferência), mas sim duas faixas mais densas de colisões: a soma daquelas que ocorreram nas partes um e dois do experimento.

FIGURA 1 - Representação dos resultados do experimento da Dupla Fenda.



Fonte: (Responde Aí e adaptado pelo autor)

Dessa forma, além de evidenciar a dualidade onda partícula, salienta-se a relevância do processo de medida para determinar um dado resultado:

As manifestações dos aspectos corpuscular (nesse caso, fótons com trajetória definida) e ondulatório ocorrem em experimentos distintos. A configuração experimental é um elemento essencial para a descrição do sistema. O físico dinamarquês Niels Bohr cunha um termo, o “phenomenon”, que se refere a observações obtidas sob condições especificadas, incluindo uma descrição do aparato experimental. Para ele, as condições de medida constituem um elemento inerente a qualquer fenômeno ao qual o termo ‘realidade física’ possa ser atribuído.(DAVIDOVICH, p.7)

Assim, concluímos que a observação destrói o comportamento ondulatório do sistema, de modo que ao detectarmos por qual dos caminhos (fendas) nosso fóton passou, perdemos seu comportamento probabilístico, sendo assim não ocorre o fenômeno da interferência. Ao fazermos uma medição no sistema, as duas funções de onda de probabilidade colapsam para um único resultado, perdendo-se o efeito de superposição.

A partir desse fato, com Einstein incomodado com o resultado dessa teoria, surge uma grande batalha com o objetivo de destruir seus alicerces. Porém, mais tarde, convencido da sua consistência, Einstein a aceita, mas ainda considera-a como sendo incompleta, almejando dessa forma, uma teoria que permitisse uma descrição determinista⁴ das condições experimentais. Esse tipo de teoria ficou conhecida como *realidade objetiva*. (DAVIDOVICH, p.8)

4 FORMULAÇÃO DE DIRAC E O ESPAÇO DE HILBERT

A equação de Dirac⁵ é uma equação relativística da mecânica quântica (relatividade restrita), que descreve com certo grau de exatidão partículas elementares de spin $\frac{1}{2}$, como o elétron. A formulação de Dirac, como ficou conhecida, tem por objetivo representar o estado de um sistema através de um vetor em um espaço complexo de n -dimensões. O estado de um sistema pode ser representado por um vetor coluna de n componentes complexas, denominado “ket” e representado por $|\Psi\rangle$. A cada “ket” que é representado, corresponde um

⁴ A palavra “determinismo” é de uso relativamente recente. Encontra-se em certos textos de filósofos alemães do século XIX, para exprimir uma idéia que já está presente, de fato, sob outras denominações, como predeterminado ou predeterminismo (pra determinismus) e particularmente em Leibniz (*determinação e razão determinante, para delineatio*) (Lalande, 1980 [1926], p. 222-3; Leibniz 1966 [1705], 1962 [1710]). (PATY, 2004, p. 468)

⁵ Foi proposta por Paul Dirac em 1928, e tem como principal característica ser uma equação algébrica de primeira ordem, representada em um espaço de Hilbert por um vetor normado completo.(SOBRAL, João; Machado, Renato, 2019)

vetor linha de n -dimensões denominado “bra” e representado por $\langle \Psi |$, de modo que suas componentes são o complexo conjugado da componente correspondente do vetor coluna “ket”. (PIQUEIRA, 2011, p. 2)

Segundo Piqueira, dessa forma temos a seguinte implicação: caso o “ket” seja representado pela matriz coluna:

$$|\Psi\rangle = [x_1, x_2 \dots x_n]^T \quad (12)$$

Então o “bra” será representado pela matriz linha com as componentes dadas pelo seu complexo conjugado, conforme segue:

$$\langle \Psi | = [x_1^* x_2^* \dots x_n^*] \quad (13)$$

De um modo mais conciso, temos que o “bra”⁶ é igual ao conjugado da matriz transposta da “ket”:

$$\langle \Psi | = (|\Psi\rangle)^{*T} \quad (14)$$

Para que o espaço vetorial H_n seja um espaço de Hilbert n -dimensional, precisamos definir o produto interno como sendo uma aplicação do produto cartesiano $H_n \times H_n$ inserido no conjunto dos números complexos o qual deve para todo $|x\rangle, |y\rangle, |z\rangle \in H_n$ e todo c_1 e $c_2 \in \mathbb{C}$, satisfazer as seguintes condições (PIQUEIRA, 2011, p. 2):

$$I) \langle x | y \rangle = \langle y | x \rangle^* \quad (15)$$

$$II) \langle x | x \rangle \geq 0, \langle x | x \rangle = 0 \iff |x\rangle = 0 \quad (16)$$

$$III) \langle x | c_1 y + c_2 z \rangle = c_1 \langle x | y \rangle + c_2 \langle x | z \rangle \quad (17)$$

Após definido o produto interno, a norma de um vetor no espaço vetorial H_n é dada por:

$$\|x\| = \sqrt{\langle x | x \rangle} \quad (18)$$

Vamos considerar o espaço H_n como tendo dimensões finitas, dessa forma é possível considerar um conjunto $E = \{ |e_1\rangle, |e_2\rangle, \dots, |e_n\rangle \}$ de kets ortonormais, ou seja, que são mutuamente ortogonais e unitários, de maneira que todo $x \in H_n$ pode ser escrito como (PIQUEIRA, 2011, p. 2):

$$|x\rangle = x_1 |e_1\rangle + x_2 |e_2\rangle + \dots + x_n |e_n\rangle \quad (19)$$

Ou seja, o conjunto E é uma base de H_n .

Desse modo, na base E , temos que o produto interno de dois vetores $\langle x | y \rangle$ pode ser escrito como:

⁶ Os termos “bra” e “ket”, foram escolhidos pois originam-se da divisão da palavra *bra-ket*, do inglês, que significa colchete em dois pedaços. (PIQUEIRA, 2011, p. 2)

$$\langle x | y \rangle = x_1^* y_1 + x_2^* y_2 + \dots + x_n^* y_n \quad (20)$$

Deste raciocínio nasce o primeiro postulado da Mecânica Quântica, o *princípio da superposição*, o que implica que qualquer partícula ou sistema, até ser medido, está em um estado de superposição e é representado por uma combinação linear dos elementos de uma base ortonormal, de modo que cada elemento da base tem uma certa probabilidade de ser medido de acordo com a função de onda. A partir desse postulado, nasce uma nova forma de unidade fundamental de informação, o “bit quântico”, ou *qubit*. Diferente do bit clássico, que possui apenas duas possibilidades, aberto (0) ou fechado (1), o *qubit* possui uma infinidade de possibilidades, as quais estão ligadas à superposição de elementos da base, representando um dado estado construído.

Para explicitar, imaginamos dois sistemas, um clássico e um quântico. Cada um consiste em uma caixa dentro da qual há uma moeda. Como se pode imaginar, antes de abrir a caixa do sistema clássico existem apenas duas alternativas para a moeda estar acomodada: ou sua cara (G) está virada para cima ou sua coroa (C). Porém, no sistema quântico, antes da abertura da caixa, a moeda estará em um sistema de superposição de cara e coroa, o qual podemos representar pelo qubit $| \text{moeda} \rangle$ conforme segue $| \text{moeda} \rangle = c_1 | G \rangle + c_2 | C \rangle$ em que c_1 e c_2 são números complexos tais que $| c_1 |^2 + | c_2 |^2 = 1$, de maneira que somente ao medirmos o estado da partícula (abirmos a caixa) o sistema $| \text{moeda} \rangle$ irá colapsar em uma das possibilidades e este colapso acontecerá de acordo com as possibilidades ditadas por c_1 e c_2 . A probabilidade de obter $| G \rangle$ será $| c_1 |^2$ e a de obter $| C \rangle$ será $| c_2 |^2$.

5 ENTRELAÇAMENTO QUÂNTICO

Entendemos por emaranhamento ou entrelaçamento quântico todo e qualquer sistema que pode estar em um estado de superposição de dois estados auto tratáveis. Este estado de superposição pode ser local, ou seja, podem ocorrer na mesma cavidade⁷ quântica, estando desse modo acoplados espacialmente, ou ser do tipo não local, ou desacoplado, esse ocorre em cavidades distintas e pode ser resultado de átomos que tenham escapado de uma mesma cavidade e estar conectados por um canal quântico, que pode ser o vácuo ou um cabo de fibra óptica, por exemplo. (YABU-UTI, 2007)

⁷ Microcavidades ópticas limitam a luz em volumes pequenos através de recirculação ressonante. Em dispositivos ópticos quânticos, as microcavidades podem fazer os átomos ou pontos quânticos a emitir fótons espontâneos em uma direção desejada ou podem prover um ambiente onde mecanismos dissipativos, tais como emissão espontânea, são superados de forma que o emaranhamento quântico da radiação e matéria seja possível. (BARBOSA, 2010)

O conceito de emaranhamento quântico teve sua discussão iniciada no ano de 1935 e foi citado primeiramente no famoso trabalho de Einstein, Podolski, Rosen. Schroedinger define entrelaçamento quântico como:

Quando dois sistemas cujos estados conhecemos através de seus representantes (funções de onda) entram em interação física temporária, devido a forças conhecidas entre eles e, depois da interferência mútua, os sistemas voltam a se separar, então eles não podem ser mais descritos da mesma forma que anteriormente, a saber, associando a cada um deles um representante próprio. Através da interação os dois representantes se tornam emaranhados. (apud CAMARGO, 2007, p. 4)

A partir dessa definição, é perceptível que para haver entrelaçamento quântico entre dois sistemas, é preciso que esses, em algum dado momento, tenham sofrido interação mútua. Essa interação resulta em um emaranhamento tal que, após a interação, não é possível afirmar que os subsistemas resultantes sejam independentes um do outro, pois mesmo que estejam separados espacialmente, os subsistemas permanecem “interagindo”, o que nos leva a um dos aspectos mais intrigantes da mecânica quântica, o princípio da não localidade.

Após essas alegações feitas por Schroedinger, Einstein ficou bastante “controverso”, pois esse princípio violaria sua teoria da relatividade, que diz que nada pode viajar mais rápido do que a luz. Um sistema emaranhado e que não ocorre em uma mesma localidade deveria também respeitar essa lei. Porém o princípio da não localidade diz que, por maior que seja a distância espacial que separa um subsistema emaranhado, ao realizar a medição de um dos componentes emaranhados o segundo irá colapsar simultaneamente. Assim, Einstein classificou o princípio da não-localidade como *ação fantasmagórica à distância*. (NETO, 2018, p.7)

Vamos imaginar um sistema emaranhado composto por dois elétrons, cada um deles possuindo uma orientação específica do seu spin, podendo esse ser *up* ou *down*. Dessa forma para um par de partículas fica fácil compreender que possuímos quatro possibilidades de estados: $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$. Assim, um estado geral desse sistema será, por consequência, uma combinação qualquer dos estados básicos, (NOVAIS; STUART, 2016, p. 116), ficando:

$$|\Psi\rangle = a|\uparrow\uparrow\rangle + b|\uparrow\downarrow\rangle + c|\downarrow\uparrow\rangle + d|\downarrow\downarrow\rangle \quad (21)$$

Analisando um dos possíveis estados, representado por $|\Psi\rangle = a|\uparrow\uparrow\rangle + b|\uparrow\downarrow\rangle$ e utilizando uma técnica matemática denominada fatoração, podemos representar essa combinação como sendo $|\Psi\rangle = |\uparrow\rangle (a|\uparrow\rangle + b|\downarrow\rangle)$. Podemos assim verificar que para o primeiro elétron temos uma orientação de seu spin bem definida: para cima ou spin up. Por

outro lado, nada podemos afirmar sobre a orientação do segundo elétron, de modo que este último está em uma superposição de spin up e spin down. Em contrapartida, ao tentarmos analisar um sistema cuja combinação pode ser representada por $|\Psi\rangle = b|\uparrow\downarrow\rangle + c|\downarrow\uparrow\rangle$ não temos nenhuma informação concreta a respeito da orientação de cada um dos spins, de maneira que tanto o primeiro como o segundo elétron estão em um estado de superposição. Em momento algum, até realizarmos a medida, podemos dizer com precisão qual a orientação de cada um dos spins. O que podemos, apenas, é representar a probabilidade de o spin ser up, representado por $|b|^2$, ou down, representado por $|c|^2$. Assim, temos um correlacionamento entre os dois elétrons, no qual o estado de um interfere no estado do outro. (NOVAIS;, STUDART, 2016, p. 116-117)

É importante destacar que, mesmo pelo fato do sistema estar emaranhado, é possível determinarmos o estado de posição como um todo, porém para os spins individuais o mesmo não é possível.

Para uma melhor compreensão, seja a seguinte situação. Possuímos novamente um sistema composto por dois elétrons em um estado emaranhado. Esses estão separados por uma distância espacial muito grande, supomos que um está aqui na Terra e o outro na Lua. Como vimos anteriormente um dos estados desse sistema pode ser representado por $|\Psi\rangle = b|\uparrow\downarrow\rangle + c|\downarrow\uparrow\rangle$. Matematicamente temos definido que ao medirmos o elétron que está na lua possuímos uma probabilidade de $|b|^2$ de encontrarmos o spin do elétron orientado para cima, e de $|c|^2$ de sua orientação estar para baixo. Suponhamos, então, que é realizada uma medida do elétron que está na terra e essa resulta em uma orientação “para cima”. Automaticamente o sistema de superposição será quebrado e o elétron que está na lua terá sua orientação “para baixo”. Dessa forma, o que antes era um processo aleatório no elétron da lua passa a ser um processo determinístico. Fica evidente, assim, a correlação entre um e outro, de modo que qualquer interação com qualquer uma das partículas leva o sistema todo ao colapso. (NOVAIS; STUDART, 2016, p. 118)

Como citado anteriormente, esse efeito foi definido por Einstein como sendo uma ação fantasmagórica.

Com o objetivo de dar sequência a esta revisão, no capítulo seguinte vamos entender um pouco os fundamentos da inseparabilidade dos estados quânticos, começando por uma abordagem das desigualdades de Bell.

6 O PARADOXO EPR E AS DESIGUALDADES DE BELL

Vivemos em um mundo macroscópico, o que leva a maioria das pessoas a acreditar em uma realidade absoluta, ou seja, a realidade é a mesma para qualquer indivíduo e não depende da subjetividade de cada um. Segundo Machado (2013, p.9) as coisas são do jeito que são e não tem nenhuma relação com o observador. Este, por sua vez, observa para obter informações sobre o sistema no qual está interessado.

Porém, com o avanço dos estudos da mecânica quântica, algumas dessas “certezas” têm sido questionadas, nos conduzindo a um caminho oposto ao que pensávamos sobre a “realidade”. A mecânica quântica tem por principal característica ser uma ciência estatística, de modo que todo e qualquer determinismo é impossível, como sugere o princípio da incerteza proposto por Heisenberg.

Pascual Jordan afirma que “observações não somente perturbam o que vai ser medido, elas o produzem [...] Nós compilamos o elétron a assumir uma posição bem definida [...] Nós próprios somos os responsáveis por produzir os resultados das medições que observamos”. (CHAVES, 2020, p. 1)

Essa alegação não foi aceita por muitos físicos, inclusive alguns dos defensores da mecânica quântica. Para contestá-la, em 1935, Einstein, Podolsky e Rosen, publicaram um estudo, baseado em três hipóteses aparentemente naturais, o qual ficou conhecido como “Paradoxo EPR”. A primeira das hipóteses referia-se ao realismo. Segundo eles, a realidade física existe, com a alegação de que “não é preciso observar a lua para saber que ela está lá em cima”. A segunda é a do livre arbítrio, onde o observador escolhe o sistema físico que irá observar. A terceira hipótese trazida em seu artigo diz respeito ao princípio da localidade, onde, segundo eles, é impossível que sistemas físicos separados por uma grande distância espacial tenham qualquer interação e possam influenciar-se mutuamente. (CHAVES, 2020)

Nas palavras de Machado (2013, p.10), Einstein, Podolsky e Rosen propuseram em seu artigo uma definição para a realidade física. “Se, sem perturbar-se um sistema, nós pudermos prever com precisão (i.e. com a probabilidade igual à unidade) o valor de uma quantidade física, então existe um elemento de realidade física correspondente a esta quantidade física.”

Para uma melhor compreensão do paradoxo EPR, conjecturas a seguinte situação. Possuímos um sistema isolado, o qual é formado por uma partícula. Instantes depois fragmentamos essa em duas, de modo que o momento linear total do sistema é conservado. Definimos então que o momento linear da partícula 1 seja p_1 e sua posição x_1 , enquanto o

momento da partícula 2 é p_2 e sua posição é x_2 . Assim segundo Machado (2013, p.11), podemos escrever:

$$P = p_1 + p_2 \quad (22)$$

$$X = x_1 - x_2 \quad (23)$$

Partindo da premissa de que $[x_a, p_b] = i\hbar\delta_{ab}$, prova-se que X e P comutam.

$$[X, P] = XP - PX \quad (24)$$

$$= (x_1 - x_2) \cdot (p_1 + p_2) - (p_1 + p_2) \cdot (x_1 - x_2) \quad (25)$$

$$= x_1p_1 + x_1p_2 - x_2p_1 - x_2p_2 - p_1x_1 + p_1x_2 - p_2x_1 + p_2x_2 \quad (26)$$

$$= x_1p_1 - p_1x_1 - (x_2p_2 - p_2x_2) = [x_1, p_1] - [x_2, p_2] \quad (27)$$

$$= i\hbar - i\hbar = 0 \quad (28)$$

Assim, concluímos que X e P podem ser definidos simultaneamente.

Dessa maneira, podemos pensar no seguinte estado:

$$|\Psi\rangle = |P=0, X=a\rangle \quad (29)$$

Desse modo definimos “a” como sendo a distância conhecida entre as duas partículas x_1 e x_2 , de modo que, a partir da partícula x_2 , podemos encontrar a posição da partícula x_1 , pois $a = x_1 - x_2$ e assim, $x_1 = x_2 + a$. De modo análogo, o mesmo princípio pode ser aplicado para o momento. Ao obtermos p_2 saberemos, por consequência, o valor de p_1 , pois $p_2 = -p_1$. Logo, podemos obter p_1 e x_1 sem medir diretamente essas grandezas e, assim, entende-se que existe um elemento de realidade física tanto associado para a posição, quanto para o momento. (MACHADO, 2013, p.11)

É importante salientar que, independente da distância que encontram-se as partículas 1 e 2 a teoria se aplica. Frisando que, pela teoria da relatividade, é impossível que uma informação propague-se instantaneamente de uma partícula a outra, o teorema EPR é verificado, de modo que o princípio da localidade não é violado.

Einstein-Podolsky-Rosen dessa forma concluíram, em seu artigo, que a mecânica quântica era incompleta e incapaz de fornecer uma descrição da realidade. Assim, segundo Henrique:

Surgiram teorias que buscavam complementar a Mecânica Quântica com parâmetros adicionais. Para estados emaranhados, esses parâmetros seriam propriedades comuns dos membros do sistema que não seriam tratadas pela Mecânica Quântica. Estas teorias ficaram conhecidas como *Teorias de Variáveis Ocultas*. (HENRIQUE, 2014, p. 2)

Einstein acreditava que as partículas possuem variáveis ocultas em seu interior, as quais explicariam os diferentes resultados na realização de um experimento quântico: por exemplo, uma variável escondida que determina o resultado final de um experimento, ou seja, um pré-determinismo.

Surgiram, paralelamente a essas outras teorias. Dentre essas podemos destacar a do físico Niels Bohr, o qual afirmava que a incerteza quântica é radical, ou seja, ele acreditava que as coisas são intrinsecamente aleatórias, desse modo não existindo a mera possibilidade de se presumir um evento futuro, indo contra a ideia de um determinismo quântico.

A discussão entre a existência ou não das variáveis ocultas permaneceu viva por muitos anos, até que em 1964 John S. Bell, um famoso físico Irlandês, afirmou que a teoria das variáveis ocultas locais é restrita a certas desigualdades, que nem sempre são obedecidas pela mecânica quântica. Essas desigualdades ficaram conhecidas como *as desigualdades de Bell*.

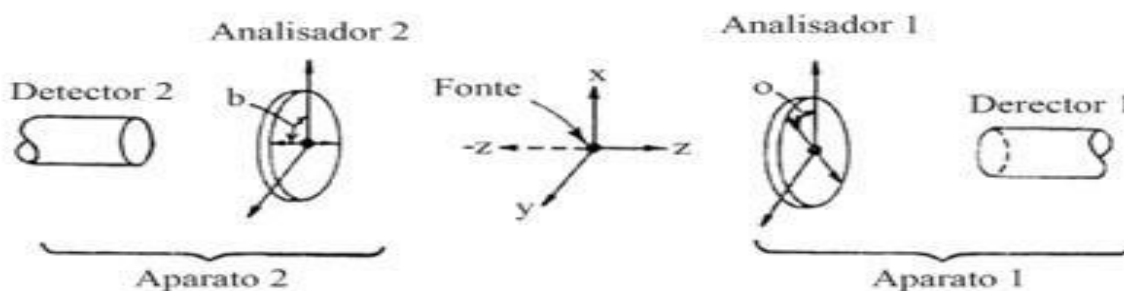
Bell parte da premissa da teoria proposta por Einstein-Podolsky-Rosen, onde é destacado a independência de sistemas físicos distantes espacialmente, mesmo que esses tenham tido interação mútua e em uma mesma localidade em um momento anterior. Bell formula um modelo de descrição mais completo, com o auxílio de variáveis adicionais àquelas usadas pela teoria quântica. Ele demonstra que um modelo desse tipo leva a desigualdades que não poderiam ser previstas usando o modelo estatístico da teoria quântica.

Para entendermos as desigualdades de Bell mais facilmente, partimos da premissa de que possuímos um sistema com uma partícula méson π . Sabemos que essa possui um momento angular nulo. Imaginamos então que essa partícula é dividida em duas partículas de spin $\frac{1}{2}$. Desse modo, pela conservação do momento angular, fica claro que o sistema deve estar em um estado singlete, dessa maneira podendo ser representado por:

$$|0\rangle = \frac{1}{\sqrt{2}} (|+\rangle |-\rangle - |-\rangle |+\rangle) \quad (30)$$

Utilizando-se de um aparato experimental, o qual pode ser visto Figura 2, é realizada uma série de medidas da orientação de cada um dos spins das partículas, os quais, por convenção, podem possuir apenas duas orientações: ou spin up (1), ou spin down (-1). Assim, após uma série de medidas é encontrada uma sequência de “1” e “-1”.

FIGURA 2 - Esquema experimental para detecção da orientação dos spins.



Fonte: (BISPO, DAVID, FREIRE, 2013 p.4)

Vamos chamar o detector 1 de a e o 2 de b . Dessa forma podemos representar a média dos produtos das orientações de a e b como sendo $P(a, b)$. Essa definição nos leva a três conclusões:

- 1- Se ambos os detectores estiverem alinhados, ou seja, possuírem a mesma orientação, é esperado que o produto entre a e b seja -1 .
- 2- Se os detectores estiverem orientados de maneira oposta, ou seja, possuírem entre eles um ângulo de 180° , é esperado que o produto entre a e b seja 1 .
- 3- Caso ambos estejam em uma orientação arbitrária, nada pode se afirmar sobre o produto de a e b .

Analisando o experimento a partir de uma visão clássica, na qual segundo Einstein, a mecânica quântica teria que ser complementada com variáveis ocultas para prever com certo grau de realidade a natureza, definiremos λ como sendo o conjunto de variáveis ocultas necessárias para que possamos prever o valor da partícula 1 e da partícula 2 com exatidão. Após um montante de medições e com o conjunto de variáveis ocultas λ variando estatisticamente conforme $p(\lambda)$, onde $p(\lambda)$ é a probabilidade de obter λ e, ainda, após termos definido que o spin da partícula 1 pode ser representado por $A(a, \lambda)$ e o spin da partícula 2 por $B(b, \lambda)$, podemos concluir que a média dos produtos das medições será (MACHADO, 2013, p.14-16):

$$P(a, b) = \int p(\lambda) A(a, \lambda) B(b, \lambda) \quad (31)$$

Como definimos acima, o sistema possui um momento angular total nulo. Assim:

$$B(b, \lambda) = -A(b, \lambda) \quad (32)$$

Isso implica que:

$$P(a, b) = - \int p(\lambda) A(a, \lambda) A(b, \lambda) d\lambda \quad (33)$$

Do mesmo modo, se tomarmos uma terceira direção arbitrária e denominarmos essa de “c”, aplica-se tudo que foi aplicado a “a” e “b”:

$$P(a, c) = - \int p(\lambda) A(a, \lambda) A(c, \lambda) d\lambda \quad (34)$$

Logo:

$$P(a, b) - P(a, c) = - \int p(\lambda) [A(a, \lambda) A(b, \lambda) - A(a, \lambda) A(c, \lambda)] d\lambda \quad (35)$$

Sabendo que $A(a, \lambda)$, $A(b, \lambda)$ e $A(c, \lambda)$, podem valer somente ± 1 , então:

$$[A(b, \lambda)]^2 = 1 \quad (36)$$

e pode-se assim escrever:

$$P(a, b) - P(a, c) = - \int p(\lambda) [A(a, \lambda) A(b, \lambda) - A(a, \lambda) [A(b, \lambda)]^2 A(c, \lambda)] d\lambda \quad (37)$$

De modo que:

$$P(a, b) - P(a, c) = \int p(\lambda) A(a, \lambda) A(b, \lambda) [A(b, \lambda) A(c, \lambda) - 1] d\lambda \quad (38)$$

Aplicamos agora o módulo à igualdade acima, obtendo:

$$| P(a, b) - P(a, c) | \leq \int | p(\lambda) A(a, \lambda) A(b, \lambda) [A(b, \lambda) A(c, \lambda) - 1] | d\lambda \quad (39)$$

Como $p(\lambda) \geq 0$,

$$| [1 - A(b, \lambda) A(c, \lambda)] | \geq 0 \quad (40)$$

e:

$$| A(a, \lambda) A(b, \lambda) | = 1 \quad (41)$$

Nossa desigualdade é reduzida a:

$$| P(a, b) - P(a, c) | \leq \int p(\lambda) [1 - A(b, \lambda) A(c, \lambda)] d\lambda \quad (42)$$

ou:

$$| P(a, b) - P(a, c) | \leq 1 + P(b, c) \quad (43)$$

Expressamos até aqui a desigualdade proposta por John Bell que, em suma, deve ser obedecida para toda e qualquer teoria de um realismo local.

Como é sabido da mecânica quântica que $P(a,b) = -a \cdot b$ (MACHADO, 2013, p.15), alicerçados nisso podemos demonstrar que a desigualdade de Bell é violada para determinadas orientações. Utilizamos como exemplo três vetores, a , b e c .

Os vetores a e b são perpendiculares entre si, e ambos formam um ângulo de 45° em relação ao vetor c .

Desse modo e segundo Machado (2013, p.14-16):

$$|P(a, b) - P(a, c)| = |-a \cdot b + a \cdot c| \quad (44)$$

$$|P(a, b) - P(a, c)| = 0 + \frac{\sqrt{2}}{2} \quad (45)$$

Como $|P(a, b) - P(a, c)| \leq 1 + P(b, c)$:

$$1 + P(b, c) \geq \frac{\sqrt{2}}{2} \quad (46)$$

$$1 - b \cdot c \geq \frac{\sqrt{2}}{2} \quad (47)$$

$$1 - \frac{\sqrt{2}}{2} \geq \frac{\sqrt{2}}{2} \quad (48)$$

Obtemos $\sqrt{2} \leq 1$. O que não é verdade!

Desse modo conclui-se que, ao menos no caso considerado, “a predição estatística da mecânica quântica é incompatível com a predeterminação separável”, ou seja, a ideia de Einstein de completar a mecânica quântica com variáveis que impusesse o realismo, ou a localidade, é impraticável. Desse modo, uma das duas compreensões acerca da realidade teria que ser descartada. (BELL, 1964, p.199)

Bell sugere, então, duas alternativas para a contradição encontrada. Na primeira delas, ele sugere que há uma interação que se propaga instantaneamente entre as duas partículas. Porém, a partir dessa, deve-se admitir uma violação da relatividade restrita proposta por Einstein. Assim sendo, Bell ficou mais convencido de sua segunda alternativa, onde afirma que “certamente a situação é diferente se as predições quanto mecânicas são de validade limitada”. (FREIRE, v.8. 1991, p. 217)

Para realização do experimento que verificasse as desigualdades de Bell, outras hipóteses e desenvolvimentos em relação às considerações iniciais foram necessários. Ainda assim, Bell tem todo o mérito pela sua descoberta, pelo fato de tornar mensurável um debate que foi travado durante trinta anos e que tinha cunho quase que exclusivamente epistemológico. Clauser utiliza as seguintes palavras para assinalar esse deslocamento da discussão: “[...] a discussão, na maior parte dos 30 anos subsequentes, foi realizada mais nas festas e coquetéis entre físicos que na corrente principal da moderna pesquisa. A partir de 1965, contudo, a situação mudou dramaticamente”. (FREIRE, v.8. 1991, p. 212)

6.1 COMPROVAÇÃO EXPERIMENTAL DA DESIGUALDADE CHSH

É importante esclarecer que nem as desigualdades de Bell, nem sua versão mais simples a CHSH, expressam propriedades exclusivas da mecânica quântica e podem, portanto, ser aplicadas a quaisquer grandezas que assumam valores definidos. (CASSINELLO; GÓMEZ, 2017, p. 135)

Para entendermos a desigualdade CHSH vamos definir quatro grandezas, A, B, C e D, sendo que cada uma delas está associada a uma das polarizações de um cristal de Calcita. De modo resumido e segundo Cassinello e Gómez (p.135), cada uma dessas grandezas está relacionada com uma dada orientação do cristal de Calcita. Para cada uma das grandezas analisadas, é verificado a polarização dos fótons ao atravessarem o cristal, de modo que se possuíssem uma posição horizontal é definido a esse o valor +1 e inversamente se for medido uma orientação vertical é definido-lhe o valor -1. Desse modo, após uma série de medidas, é esperado detectar uma aleatória lista de valores “+” e “-”. Em acordo com a teoria do realismo local, proposta por Einstein, é esperado que essas grandezas tenham valores pré-determinados mesmo antes de ser efetuada a medição.

Em consonância com isso, utiliza-se a seguinte expressão:

$$S = (A + C) \cdot B + (A - C) \cdot D \quad (49)$$

Sabendo que cada grandeza pode valer 1 ou -1, é matematicamente comprovado que o valor da expressão S pode ser 2 ou -2. Vejamos:

1 - Se $A = 1$ e $C = 1$

$$A + C = 2 \quad (50)$$

$$A - C = 0 \quad (51)$$

$$S = \pm 2 \text{ pois } B = \pm 1. \quad (52)$$

2- Se $A = -1$ e $C = -1$

$$A + C = -2 \quad (53)$$

$$A - C = 0 \quad (54)$$

$$S = \pm 2 \text{ pois } B = \pm 1. \quad (55)$$

3 - Se $A = -1$ e $C = 1$

$$A + C = 0 \quad (56)$$

$$A - C = -2 \quad (57)$$

$$S = \pm 2 \text{ pois } D = \pm 1. \quad (56)$$

4 - Se $A = 1$ e $C = -1$ (60)

$$A + C = 0 \quad (58)$$

$$A - C = 2 \quad (59)$$

$$S = \pm 2 \text{ pois } D = \pm 1. \quad (60)$$

É possível verificar que em todos os casos, apenas uma parte da equação sobrevive, de modo que o resultado sempre é 2 ou -2.

Independentemente do resultado ser 2 ou -2, utilizamos para o cálculo a seguir sempre seu valor absoluto, ou seja seu módulo, que no caso será sempre 2 (CASSINELLO; GÓMEZ, 2017).

Por conveniência temos que:

$$| \langle S \rangle | = | \langle A \times B \rangle + \langle C \times B \rangle + \langle A \times D \rangle - \langle C \times D \rangle | = 2 \quad (61)$$

Temos que $\langle A \times B \rangle$ é o valor médio dos produtos de A e B, obtido em diversas medições, assim podemos utilizar a seguinte expressão, diretamente compatível com os valores experimentais (CASSINELLO; GÓMEZ, 2017):

$$\langle A \times B \rangle = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N_{++} + N_{--} + N_{+-} + N_{-+}} \quad (62)$$

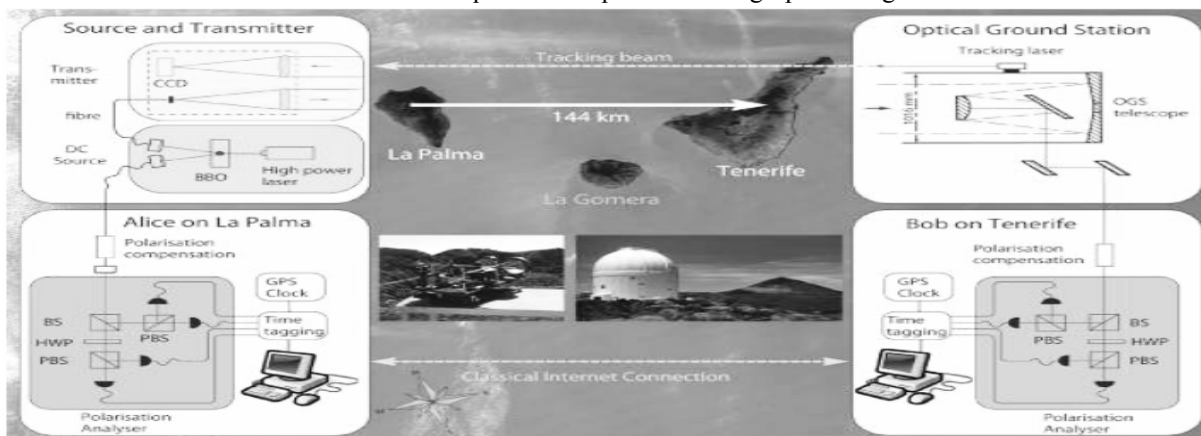
Por definição, temos que o primeiro sinal diz respeito ao valor da polarização de A e o segundo da polarização de B, assim “N” indica o número de vezes que foi obtido tal combinação. Por conseguinte temos que calcular o valor médio das grandezas, de modo que quando o valor médio de A e B é positivo soma-se o valor à equação e caso contrário, subtrai-se. Por fim, o resultado dessas somas e subtrações é dividido pelo valor total de medições.

A partir de agora, aplicamos o formalismo da mecânica quântica às grandezas A, B, C, e D, de maneira que podemos escolher apropriadamente as direções de polarização do nosso experimento. (CASSINELLO; GÓMEZ, 2017, v. 1, p. 135-139)

Um dos maiores experimentos que comprovam as desigualdades de Bell foi realizado no ano de 2007 nas ilhas Canárias, pelo grupo Zeilinger. Instalou-se um sistema em uma das ilhas, o qual tem por propriedade produzir fótons entrelaçados. Esses, por sua vez, são originados de um único laser com comprimento de onda de cerca de 355 nm e, após chocam-se sobre um cristal de conversão paramétrica conhecido como BBO, que decaem em um único par degenerado em energia, de comprimento de onda de aproximadamente 710 nm cada, de modo a ficarem entrelaçados pelo seu modo de produção.

Na ilha de La Palma, Alicia (uma personagem hipotética) mede a polarização de um dos fótons. Benito (outro personagem), que está em Tenerife, uma ilha que dista 144 km de La Palma, faz o mesmo com o outro fóton do par. Vejamos, na Figura 3, o esquema do experimento realizado pelo grupo Zeilinger.

FIGURA 3 - Esquema do experimento do grupo Zeilinger



Fonte: (ZEILINGER et al, 2007, p.6)

Como é possível perceber na imagem, o fóton a ser medido por Alícia inside primeiramente sobre o dispositivo indicado na imagem pela sigla BS, esse na verdade é um espelho semi-refletor, de modo que possui uma probabilidade de 50% de deixar o fóton passar, como de refleti-lo. O dispositivo HWP tem por objetivo girar todo e qualquer fóton que nele incidir: No caso determinado, o mesmo está calibrado para girar a polarização de todo e qualquer fóton 45° em relação a sua incidência. Por sua vez, os PBSs nada mais são do que dispositivos polarizadores, ou seja, eles deixam passar em sua totalidade os fótons orientados horizontalmente, e bloqueiam todos que estejam orientados verticalmente.

Assim Alícia, ao fazer sua medição, mede aleatoriamente a variável A ou a variável C, sendo que cada uma delas pode assumir dois valores possíveis, 1 ou -1.

Benito, por sua vez, utiliza-se do mesmo detector de Alícia, com a diferença que, o detector de Benito tem uma orientação de $22,5^\circ$ em relação ao de Alícia. Semelhantemente ao processo de Alícia, Benito poderá detectar o fóton medido em B ou D, podendo esse do mesmo modo, assumir valor 1 ou -1.

Vale destacar aqui mais uma vez, que a probabilidade de detectar o fóton em uma posição ou outra é completamente aleatória, é o acaso que decidirá se o fóton será refletido no refletor BS sendo detectado em A ou B, ou se atravessará, sendo assim detectado em C ou D.

Por um canal clássico (rede de internet), Benito e Alícia transmitem os tempos de detecção de seus fótons, e comparam-nos. Conhecida a distância entre as duas ilhas, chega-se ao tempo de voo entre elas, que fica em torno de 0.000487 segundos, e, a partir desse descobre-se os pares de fótons entrelaçados. Esses, por sua vez, são comparados um a um e examinados em qual das grandezas A, B, C ou D foram detectados. (CASSINELLO; GÓMEZ, 2017, v. 1, p. 145-149)

Utilizando-se do artifício matemático apresentado anteriormente, calcula-se para cada uma das estações (La Palma e Tenerife), os valores correspondentes a cada uma das medidas $\langle A \times B \rangle$, $\langle C \times B \rangle$, $\langle A \times D \rangle$ e $\langle C \times D \rangle$.

A coleta de dados do experimento realizado pelo grupo Zeilinger durou 221 segundos, e foram verificados 7058 eventos de coincidência no total. Deste modo foi possível obter $|\langle S \rangle|$ (ZEILINGER et al, 2007), conforme segue:

$$|\langle S \rangle| = |\langle A \times B \rangle + \langle C \times B \rangle + \langle A \times D \rangle - \langle C \times D \rangle| \quad (63)$$

$$|\langle S \rangle| = ((-\sqrt{2} - \sqrt{2} - \sqrt{2}) + (-\sqrt{2})) / 2 = 2\sqrt{2} \quad (64)$$

Obteve-se então o resultado:

$$|\langle S \rangle| = 2\sqrt{2} \approx 2.8 \quad (65)$$

Sendo esse maior do que 2.

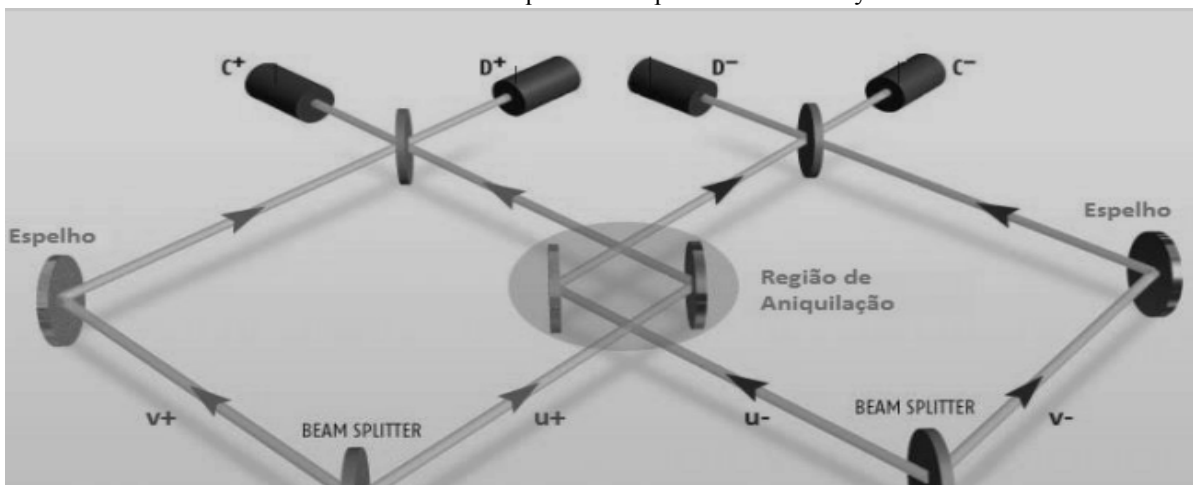
Esse resultado demonstrou a violação do limite realista local para mais de treze desvios padrões. Desse modo, comprova-se que a predição quântica viola a desigualdade, de modo que um dos fótons é detectado na fonte, no momento que o segundo fóton está a apenas alguns metros de distância. Como os dois locais de medição estão separados por 144 Km de distância comprova-se que a predição quântica viola a desigualdade. Assim, conclui-se inevitavelmente que as quatro grandezas por nós definidas não têm valores definidos antes da medição, tampouco antes da realização do experimento, de maneira que conforme avalia o experimento a medida de um fóton, afeta o seu par correlacionado simultaneamente. (ZEILINGER, 2007, p.5)

6.2 O EXPERIMENTO DE HARDY

Outro importante experimento⁸ mental ao que tange às desigualdades de Bell foi proposta em 1992 pelo físico Lucien Hardy. Esse experimento teve como objetivo provar que a mecânica quântica não é uma teoria física local. Resumidamente, o experimento consiste em uma fonte de pares de partículas e dois sensores denominados de interferômetros de Mach-Zehnder, um para pósitron (MZ +) e um para elétrons (MZ -). Esses sensores são instalados em pontos estratégicos, de modo que há uma sobreposição dos dois caminhos, aos quais podem ser configurados de maneira independente e aleatória.

⁸ O paradoxo de Hardy, como ficou conhecido, é uma extensão do experimento mental proposto por Elitzur e Vaidman (1991) por demonstrar a possibilidade de medição sem interação. (PIMENTA, p. 2)

FIGURA 4 - Esquema do experimento de Hardy



Fonte: (PIMENTA)

David Mermin definiu o experimento de Hardy como sendo muito intuitivo, além de possuir uma enorme beleza e simplicidade:

Mas a importância adicional e a grande beleza do experimento de Hardy está no que ele nos diz, como uma dedução extremamente simples e direta da teoria quântica elementar, sobre o mundo que a teoria descreve na ausência de interações hipotéticas e não detectáveis que destroem correlações. (...) A brilhante refutação das hipóteses [subjacentes às derivações da desigualdade de Bell] permanece, em sua simplicidade básica, como uma das mais estranhas e bonitas pérolas que podemos encontrar no extraordinário solo da mecânica quântica. (MERMING, 1994, p.62 apud FASSARELLA, 2019, p.1)

O experimento consiste em tentar detectar o entrelaçamento quântico em um par de partículas, mais especificamente um pósitron e um elétron emitidos por uma mesma fonte. Ele ocorre da seguinte forma: em determinado momento o experimentador aciona a fonte emissora de partículas, essas duas partículas têm, cada uma delas, dois caminhos possíveis para percorrer. O pósitron pode seguir pelo caminho C + ou D +, já o elétron possui como alternativas os caminhos C - e D -. Cada par desses caminhos é denominado de interferômetro de Mach-Zehnder. Os dois interferômetros estão interseccionados na região de aniquilação e ao final de cada um deles há um detector de partículas.

Em consonância com a teoria do realismo local, é esperado que todos os pares de partículas detectadas tenham relação apenas com a configuração da fonte antes da emissão delas, e não com a configuração dos detectores após sua emissão. Do mesmo modo, a

localidade implica que o resultado de umas das medições efetuadas por um dos detectores não irá interferir na medida da outra partícula. (FASSARELLA, 2019)

Nota-se que, se houvesse um pré determinismo antes das partículas atingirem os sensores, seria impossível encontrar um elétron e um pósitron na posição D- e D+, respectivamente, pois para isso, esses teriam que percorrer os caminhos u^+ e u^- , eliminando-se na região de aniquilação.

Desse modo, podemos concluir que o experimento CHSH, bem como o experimento de Hardy, provam a violabilidade das desigualdades de Bell a partir de uma predição quântica, de modo que o realismo local é refutado, ou seja, abandona-se a teoria da conjunção do realismo com a localidade, que diz que os parâmetros de um sistema são mensuráveis, dessa maneira possuindo sempre um estado definido em todos os instantes de tempo e, também, que a medida em um sistema jamais interfere no resultado de um sistema adjunto deste. Ou seja, mesmo em um sistema entrelaçado, ao qual há uma sobreposição de estados, não ocorre o fenômeno de dependência.

Em suma, prova-se também que as trajetórias Bohmianas⁹ não são invariantes de Lorentz, de maneira que se faz necessária para essa o uso de um referencial especial. Ou seja, será necessário aceitar a ação fantasmagórica à distância, sendo impraticável a complementação da mecânica quântica com variáveis ocultas, de modo que o que fazemos em uma parte do sistema, afeta instantaneamente a outra parte dele, mesmo que essa esteja a milhares de anos luz de distância. (CASSINELLO; GÓMEZ, 2017, v. 1, p. 151)

Essa propriedade magnífica do entrelaçamento quântico nos permite teletransportar estados quânticos. É essa possibilidade que se estuda e busca-se a sua implementação no processamento de dados computacionais.

7 TELETRANSPORTE: A POSSIBILIDADE DE SUPERPROCESSAMENTO

Inicialmente o termo “teletransporte” pode soar estranho à maioria dos leitores, em especial àqueles não familiarizados com a mecânica quântica. Mas, como veremos a seguir, esse é totalmente plausível e pode ocorrer em casos específicos, conforme experimentos já demonstraram. Voltaremos ao ano de 1993, onde teve início toda a discussão a respeito da

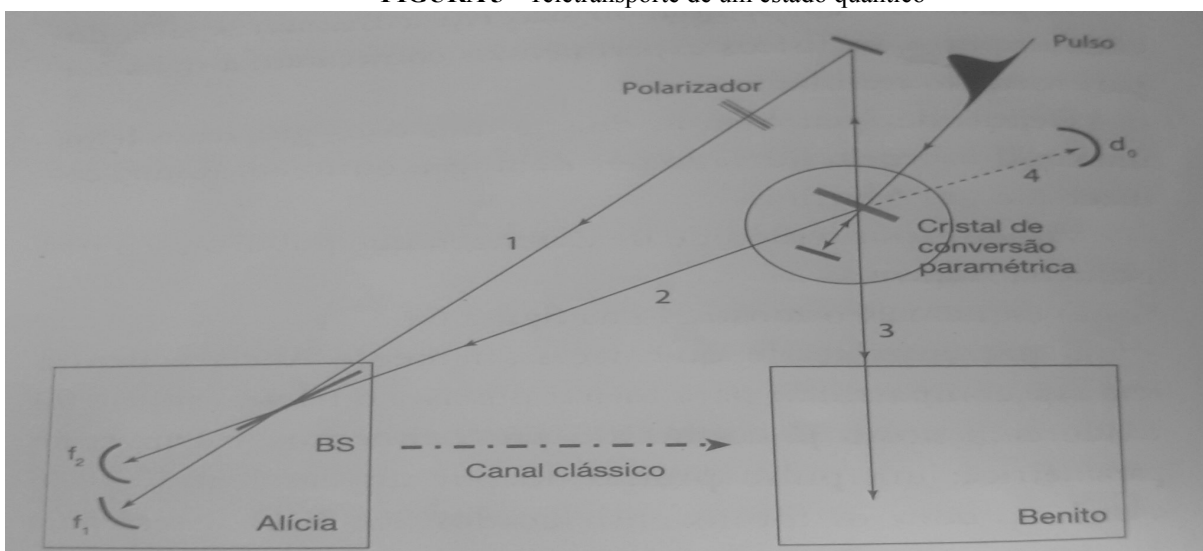
⁹ A interpretação bohmiana da MQ não-relativística envolve as variáveis ocultas, baseada na existência de partículas descrevendo trajetórias no espaço segundo uma lei de movimento que pode ser obtida a partir da função de onda (BOHM, 1957 apud BATISTA, NETO, 2008, P. 59).

computação quântica. Foi quando Charles Bennett¹⁰ mostrou que é possível transferir estados quânticos por meio de partículas que estejam em um estado entrelaçado.

Por conveniência e por já estarmos familiarizados, retornamos aos nossos personagens, Benito e Alícia. Imaginamos que Benito deseja enviar informações do estado de seu sistema para Alícia, porém ele não dispõe de nenhum tipo de canal clássico para fazê-lo. Bennet sugeriu que, caso Alícia e Benito possuíssem um par qualquer de partículas em um estado entrelaçado, Benito pode entrelaçar a informação do estado que quer teletransportar, junto a sua partícula que está entrelaçada com a de Alícia. Desse modo, ao Alícia realizar a medida da partícula dela, receberá junto a informação do sistema que Benito queria "teletransportar" a ela.

Em meio a toda essa teoria, surgem questões filosóficas a respeito de ser fisicamente correto admitir que houve teletransporte da partícula, sendo que só seu estado quântico foi compartilhado. Porém podemos alicerçar essa tese no seguinte fato: sabe-se que todos os fótons, elétrons, e partículas elementares são idênticas, o que as diferencia umas das outras é seu estado quântico. Desse modo, ao transferirmos o estado quântico de uma partícula para outra estamos, na verdade, materializando essa em outro sistema. De fato, então, ocorre o fenômeno do teletransporte (CASSINELLO; GÓMEZ, 2017, v. 1, p. 173). Essa proposta de Bennett foi comprovada experimentalmente no ano de 1997 e ficou conhecida como método Zeilinger.

FIGURA 5 - Teletransporte de um estado quântico



Fonte: O Mistério Quântico (CASSINELLO; GÓMEZ, 2017, p. 174)

¹⁰ Charles Henry Bennett (Nova Iorque, 1943) é um físico, criptógrafo e cientista da computação estadunidense. É um dos descobridores do teletransporte quântico. (SOBRAL, João; Machado, Renato, 2019)

Na Figura 5 temos a representação do esquema experimental que foi usado para comprovação do teletransporte quântico. Como já mencionado, para satisfazer as condições iniciais e ser possível o teletransporte de um estado quântico é preciso haver um par de partículas previamente entrelaçadas. Esse processo ocorre no cristal de conversão paramétrica ao ser atravessado por um pulso de partículas, mais especificamente fótons. Esses fótons, denominados de 2 e 3, após serem entrelaçados, são direcionados, um a Benito, e outro a Alícia, respectivamente. Alícia possui como fóton a ser teletransportado o fóton 1 que, nesse caso, não é um fóton independente, mas sim criado simultaneamente quando é gerado o pulso inicial. Juntamente com o fóton 1, é criado também seu co-irmão, o fóton 4, que tem por finalidade avisar que o fóton 1 foi criado. Para que Alícia consiga entrelaçar o fóton 1 com o fóton 2 que receberá, é preciso que os dois cheguem simultaneamente ao espelho semi-refletor BS que ela possui. Desse modo, os dois saem juntos do espelho, sendo que há apenas uma detecção, ou em f_1 , ou em f_2 . Embora fácil de se entender, esse processo é intensamente delicado, tendo em vista que é muito difícil fazer com que os fótons cheguem exatamente ao mesmo instante, sendo necessário para isso um ajuste muito fino em cada uma de suas trajetórias.

Ressalto aqui novamente que, apesar de haver transferência do estado quântico da partícula, nenhuma energia ou matéria é transportada. Ou seja, o que é transportado é apenas a informação necessária para que a partícula se “materialize” em outro lugar. Vale destacar também que, pelo teorema da não-clonagem,¹¹ é impossível duplicar perfeitamente um estado quântico arbitrário, de modo que se faz necessário, nesse caso, que, ao a informação do estado ser transportada, a partícula primária deve se desintegrar, possibilitando que a segunda se materialize.

8 IMPLICÂNCIAS NO PROCESSAMENTO DE DADOS E CRIPTOGRAFIA

Com base na sessão anterior, surge uma das principais razões para o estudo da mecânica quântica e sua aplicação no processamento de dados. A partir da equação de onda e da densidade de probabilidade de estados, do teletransporte e do entrelaçamento quântico, busca-se criar algoritmos para processamento, manipulação e análise de dados, os quais baseiam-se na densidade de probabilidade. Diferente de um computador clássico, onde teríamos que analisar todas as possibilidades uma a uma e ver qual satisfaz as condições

¹¹Esse teorema foi proposto em 1982, para estados puros, por W. K. Wootters e W. H. Zurek e posteriormente em 1996, estendidos a estados mistos por H. Barnum, C. Caves, C. Fuchs, R. Jozsa e B. Schumacher. (OLIVEIRA, 2008, p.23)

exigidas, no sistema quântico analisamos apenas o todo. Em outras palavras, analisamos a densidade de probabilidade de um certo evento ocorrer (condição ser verdadeira) e, dessa forma, teremos máquinas muito mais velozes, com poder de processamento jamais visto.

Todavia, para o processamento quântico ocorrer de forma satisfatória, o sistema (computador) tem de estar totalmente isolado do meio externo, de modo que qualquer interação faria com que todo o sistema colapsasse, quebrando o princípio da superposição de estados e, desse modo, tornando-o inútil. Destarte, esses são totalmente isolados do meio externo para evitar qualquer interação com partículas externas ao sistema, necessitando ser mantidos a temperaturas próximas ao zero absoluto e a pressões quase nulas. Dessa maneira eles não são manipulados diretamente pelo usuário (humano), antes, são comandados via um interceptador, geralmente um computador clássico.

8.1 PROCESSAMENTO QUÂNTICO

Alicerçado no princípio do teletransporte e no entrelaçamento quântico, estuda-se a aplicabilidade do funcionamento de computadores, sendo que o fenômeno do teletransporte é algo essencial no processamento quântico, de modo que tudo processado em um dado lugar do processador, ocorre simultaneamente em outro. Com isso temos a possibilidade de reduzir em muitas vezes o tempo de processamento, sendo que não é preciso mais analisar o todo para ter o resultado final.

Entre as diversas aplicabilidades de um computador quântico, vale a pena destacar a sua velocidade na efetuação de cálculos envolvendo números. Por exemplo, a fatoração de números muito grandes. Sabemos que a fatoração de números muito grandes não é uma tarefa nada fácil, até mesmo para os computadores clássicos mais atuais e potentes. A fatoração tem sua dificuldade aumentada exponencialmente, conforme maior for o número que desejamos fatorar.

À primeira vista isso não parece ser muito instigante, mas vale ressaltar que a fatoração de números extremamente grandes em seus produtos primários é uma das principais bases de transações comerciais secretas de todo o mundo. Desse modo, além de possibilitar a realização de tarefas com enorme rapidez se comparado a um computador clássico, o computador quântico pode também ser muito útil no âmbito da criptografia de dados, como veremos mais adiante.

Segundo Cassinelo e Gómez (2017), desde 1993 foram criados alguns algoritmos quânticos, especialmente para o processamento de dados envolvendo números. Dentre eles vamos destacar aqui o algoritmo de Grover. Vamos imaginar que desejamos buscar um

número de telefone dentro de uma lista que contém milhares de números que não nos interessam. Com a utilização do algoritmo de Grover podemos reduzir o tempo de procura em comparação a um computador clássico à sua raiz quadrada. Ou seja, imaginamos que um computador clássico leve 10^6 segundos (aproximadamente 11,5 dias) para encontrar o número, com o auxílio do algoritmo de Grover esse tempo seria reduzido para 10^3 segundos, pouco mais que 16 minutos.

Paralelo a isso, destacamos agora o algoritmo de Shor, que diferentemente do de Grover, é usado para a fatoração de números muito longos. Como vimos, fatorar números muito grandes pode ser uma tarefa bastante árdua e demorada, até mesmo para os melhores computadores (clássicos) disponíveis atualmente (2022) no mercado. Porém, com o algoritmo de Shor rodando em um computador quântico podemos reduzir esse tempo absurdamente, conforme Quadro 2

QUADRO 2 - Tempo de fatoração entre um algoritmo clássico e o algoritmo de Shor

Comprimento do número a ser fatorado (em bits)	Tempo de fatoração por algoritmo clássico	Tempo de fatoração por algoritmo de Shor
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quatrilhões de anos	4,8 horas

Fonte: (FRANCESE, 2008)

8.2 CRIPTOGRAFIA E SEGURANÇA

Por fim, mas não menos importante, destaca-se aqui a aplicação da propriedade do entrelaçamento na criptografia de dados e na segurança ao que tange a violação de informações. Como é de nosso conhecimento, vivemos em uma sociedade que é cada vez mais regida pela era da informação, a maior parte dessa sendo virtual, ou seja, utilizamos de artifícios computacionais para o armazenamento dessas informações. Isso nos trouxe imensuráveis benefícios, como a velocidade e praticidade na realização de tarefas. Porém junto desses, surge o lado ruim, a violação e espionagem de dados. Na computação clássica muitos são os artifícios para impedir ataques hacker, ocasionadas por vírus ou ransomwares. Porém, por mais que evoluímos nessa questão, novas técnicas e artimanhas são criadas a cada dia, alicerçadas no princípio que chamamos de “engenharia reversa”. Resumidamente em um

computador clássico tudo pode ser desfeito, ou seja, por mais seguro que possa ser, sempre haverá um meio de quebrar a criptografia.

Tendo isso em vista, estuda-se atualmente a criptografia quântica, baseada também no fenômeno do entrelaçamento.

A criptografia quântica teve suas discussões iniciadas no ano de 1984, por Brassard e Bennett, esses sendo os responsáveis por criar o protocolo que ficou popularmente conhecido como BB84. Para entendermos o protocolo BB84 precisamos compreender o fenômeno de polarização da luz. Podemos manipular os feixes luminosos, fazendo com que suas ondas vibrem em apenas uma direção. Para isso utilizamos um aparelho denominado polarizador. Imaginamos então que consigamos enviar apenas um fóton polarizado, com orientação inicial $\leftarrow\rightarrow$. Imaginemos agora que instalamos um polarizador diagonalmente, teremos probabilidade de $1/2$ (50%) de o fóton passar pelo polarizador. Esse é o princípio no qual se baseia a criptografia quântica, pois ao fazermos uma medida no sistema, no nosso caso utilizando um polarizador, estamos, de certa forma, mesmo que em pequena escala, influenciando o sistema medido. Por isso podemos afirmar que, nos utilizando da criptografia quântica, seria impossível alguém espionar os dados ou alguma mensagem secreta pois, ao fazer isso, o sistema colapsa, sendo esse percebido pelo emissor e pelo receptor da mensagem. (CASSINELLO; GÓMEZ, 2017, v. 1, p. 204 - 205)

Para uma melhor compreensão dessa teoria vamos supor o seguinte experimento. Alícia deseja enviar uma mensagem secreta a Benito porém, por questões de segurança, eles decidem não usar nenhum canal clássico para isso. Alícia decide então utilizar fótons de luz para enviar a mensagem. Ela possui em seu poder um laser emissor de fótons e também um filtro polarizador. Ela fica livre para escolher a polarização de cada um dos fótons que quer enviar a Benito. Ela possui como alternativas uma polarização reta (vertical ou horizontal) ou uma polarização cruzada (diagonal). Benito, por sua vez, possui também um filtro polarizador com o qual consegue medir a direção do fóton recebido. (CASSINELLO; GÓMEZ, 2017, v. 1, p. 204-205) Para que a troca de informação ocorra de maneira satisfatória, é preciso que se defina algumas regras.

Vamos supor que Alícia envie um fóton no sentido vertical \uparrow , esse terá como valor binário 1. Caso o fóton seja polarizado no sentido horizontal \leftrightarrow , valerá 0. A mesma regra vale para uma polarização diagonal, definiremos que \nearrow valerá 1 e \searrow valerá 0. Vamos supor que o primeiro fóton enviado por Alícia esteja orientado verticalmente \uparrow . Caso Benito coloque seu detector no modo vertical, obterá 1 com 100% de certeza; caso ele seja colocado no modo cruzado, poderá obter tanto 1 como 0, com 50% de chance para cada.

Após sucessivas medidas, Benito possui uma sequência de zeros e uns. Nesse momento, por um canal clássico, Alícia e Benito comparam as orientações aos quais foram feitas a polarização e a sucessiva detecção do fóton. Cada uma das orientações são comparadas respectivamente, de modo que ao final é excluída todas as bases discordantes. Assim, ao final, eles possuirão uma sequência de 0 e 1 totalmente iguais, e esta será então a chave secreta deles. Vamos agora entender o porque esse método é considerado inviolável e de que maneira o sistema se quebra ao ser feita a tentativa de espionagem por um intruso.

Como mencionado, tanto a polarização inicial do fóton feita por Alícia como a respectiva orientação do detector feita por Benito ocorrem de forma aleatória, havendo uma probabilidade de 50% de Benito acertar qual a polarização do fóton que foi enviado.

Imaginamos então que Bob, um espião, tente interceptar os fótons enviados por Alícia para assim tentar decifrar a mensagem. Porém, para fazer isso, Bob deve medir a orientação de cada um dos fótons que ele interceptar de modo que, ao fazer isso, ele estará forçando uma polarização a esse fóton. Desse modo, a lista de 0 e 1 anotados por Benito e a respectiva orientação de seu detector, não baterão com a orientação do polarizador de Alícia. Assim, há uma probabilidade de $1/4$ (25%) de cada um dos fótons que Benito receber ter tido sua orientação alterada.

Desta maneira, destaca a inviolabilidade das informações criptografadas por meio de uma chave quântica. Vale ressaltar também, que a impossibilidade de clonagem impede que uma informação, ou estado quântico dela seja reproduzida 100% igual ao original, de modo que para isso acontecer, a informação (estado) original seria perdida.

9 CONCLUSÃO

Diante dos argumentos trazidos neste trabalho a partir das literaturas estudadas, podemos concluir que a mecânica quântica trouxe revoluções inimagináveis, em contraposto ao que afirmava a física clássica até meados do ano de 1920. Diversas teorias, que na época eram consideradas como "fantasmagóricas" ou "alucinações" dos físicos que as defendiam, foram comprovadas e hoje formam o alicerce do que conhecemos como a "nova física", ou mecânica quântica. Em especial, com essa pesquisa foi possível constatar que o entrelaçamento quântico é indispensável para o futuro aprimoramento das tecnologias, sobretudo na produção de computadores, tendo em vista que os computadores clássicos estão em um ponto de saturação, de modo que não podem mais ser diminuídos. Dessa maneira, a computação quântica tornou-se um dos principais focos de estudo relacionados à mecânica quântica, embora esteja apenas em um estado inicial. Pode-se perceber que o fenômeno do entrelaçamento quântico mudará os rumos do que hoje conhecemos sobre processamento e segurança de dados.

Embasados nas implicações da violação das desigualdades de Bell, almeja-se a construção de computadores com poder de processamento absurdamente alto se comparados aos modelos clássicos atualmente disponíveis. Com a utilização de fenômenos decorrentes do entrelaçamento quântico será mudado por completo a forma de proteger nossas informações, onde por meio de particularidades de alguns fenômenos, como a impossibilidade de cópia e o indeterminismo quântico, teremos uma criptografia inviolável.

Porém, mesmo diante de um grande avanço nesse setor, atualmente ainda são poucos os computadores quânticos em funcionamento pelo mundo e acredita-se que pelo menos em um futuro próximo, esses não serão fabricados em larga escala, nem tampouco serão utilizados pelo público em geral. Sua construção e, principalmente, seu uso requerem grandes cuidados. Esses computadores têm de ser isolados ao máximo do meio externo, evitando assim que qualquer interferência, seja ela de classe magnética, térmica, ou elétrica, possa causar alteração no sistema e, deste modo, levando a perder sua eficiência, ou mesmo fazendo que seja inviável por completo seu funcionamento.

Nesse contexto, pensando em uma continuação dessa pesquisa, seria conveniente analisar de que forma é construído (hardware) um computador quântico, bem como investigar as expectativas dos pesquisadores em relação a estes projetos.

REFERÊNCIAS

CARVALHO, Maria Inês Barbosa de. **Equação de Schrödinger**. Física dos Estados da Matéria, Faculdade de Engenharia da Universidade do Porto, p. 1-18, 1 fev. 2001.

PIQUEIRA, José Roberto Castilho. **Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e teletransporte**. Revista Brasileira de Ensino de Física, Escola Politécnica, Universidade de São Paulo, São Paulo, SP, Brasil, ano 2011, v. 33, n. 4303, ed. 4, p. 1-8, 21 nov. 2011.

MACHADO, Rodrigo Rodrigues. **Demonstrações do Teorema de Bell**. Orientador: Carlos Eduardo Aguiar. 2013. 39 p. Monografia de CONCLUSÃO DE CURSO (Licenciatura em Física) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, Brasil, 2013.

CASSINELLO, Andrés; GÓMEZ, José Luis Sánchez. **O mistério quântico**. In: O MISTÉRIO quântico. São Paulo-SP: Crítica, 2017. v. 1, cap. 5 - 7, p. 135-205. ISBN 978-85-422-1143-6.

YABU-UTI, Bruno Ferreira de Camargo. **Emaranhamento Quântico entre átomos localizados em cavidades distintas**. Orientador: José Antonio Roversi. 2007. 75 p. Tese de Mestrado (Mestre em Ciências.) - Universidade Estadual de Campinas, Campinas-SP, 2007.

HENRIQUE, Franciele Renata. **O paradoxo de Einstein-Podolsky-Rosen**. Instituto de Física de São Carlos - Universidade de São Paulo, São Carlos, SP, Brasil, ano 2014, p. 1-4, 1 jun. 2014.

SCHULZ, Peter A. **Há mais história lá embaixo - um convite para rever uma palestra**. Revista Brasileira de Ensino de Física: Universidade Estadual de Campinas, Faculdade de Ciências Aplicadas, Limeira, SP, Brasil, ano 2014, v. 40, ed. 4, p. 1-5, 1 jun. 2014.

OLIVEIRA, Thiago Prudêncio de. **Teletransporte quântico de estados térmicos**. Orientador: Tarcísio Marciano da Rocha Filho. 2008. 65 p. Dissertação de mestrado (Mestre em física) - Universidade Federal de Brasília, Brasília-BR, 2008.

BISPO, Wilson Fábio de; DAVID, Denis Francis Gilbert; FREIRE, Olival. **As contribuições de John Clauser para o primeiro teste experimental do teorema de Bell: uma análise das técnicas e da cultura material.** Revista Brasileira de Ensino de Física, Escola Politécnica, Universidade de São Paulo, São Paulo, SP, Brasil, ano 2011, v. 35, n. 3603, ed. 3, p. 1-7, 19 set. 2013.

JOHN, Bell. **On the Einstein Podolsky Rosen Paradox, Physics 1 (1964).** Reproduzido em J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge U. Press 1987.

ZEILINGER, A. *et al.* **Free-Space distribution of entanglement and single photons over 144 km.** Nature Physics 3, [s. l.], ano 2007, ed. 481, 1 jan. 2007.

PORFÍRIO, Francisco. **"Diferenças entre o ser humano e os demais animais".** *Brasil Escola.* Disponível em <https://brasilecola.uol.com.br/filosofia/diferencas-entre-ser-humano-os-demais-animais> Acesso em 11 de abril de 2022.

CHAVES, Rafael. **“Estará a Lua no céu quando ninguém está olhando?”** **CIÊNCIA FUNDAMENTAL. O que pensam os jovens cientistas no Brasil?** Disponível em: <https://cienciafundamental.blogfolha.uol.com.br/2020/07/01/estara-a-lua-no-ceu-quando-ninguem-esta-olhando>. Acesso em 11 de abril de 2022.

PATY, Michel. **A noção de determinismo na física e seus limites.** *Scientle Studia*, São Paulo, v.2, n. 4 , p. 465-92, 2004.

BARBOSA, Luiz Sérgio. **Arquitetura e organização de computadores.** Universidade do estado do Amazonas, Humaitá-AM.

DONNANGELO, Raul José; CAPAZ, Rodrigo Barbosa. **Introdução a mecânica quântica.** Centro de educação a distância do estado do Rio de Janeiro-RJ v.1, 2ª edição, 2009.

DAVIDOVICH, Luiz. **Einstein e a mecânica quântica.** Instituto de Física. Universidade do Rio de Janeiro, RJ.

SOBRAL, João; Machado, Renato. **Computação quântica: Aspectos físicos e matemáticos - Uma abordagem algébrica**. Universidade do Oeste do estado do Paraná-PR, 1º ed., 2019.

NETO, José Nogueira. **Conceitos Gerais sobre o Emaranhamento com Aplicação em Moléculas Quânticas**. Orientadora: Profa. Dra. Liliana Sanz de la Torre. Universidade Federal de Uberlândia, Uberlândia - MG, 2018.

NOVAIS, Marcel; STUDART, Nelson. **Mecânica Quântica Básica**. São Paulo: Editora Livraria da Física v.1 2016.

FREIRE, Olival. **Sobre as desigualdades de BELL**. Instituto de Física, Salvador -BA, v.8 n.3, 1991.

PIMENTA; Elsa Bifano. **Paradoxo de hardy**. Disponível em:<https://www.ifi.unicamp.br/~maplima/fi001/2020/artigo/ParadoxodeHardy.pdf> Acesso em 11 de Fevereiro de 2022.

FASSARELLA, Lúcio. **O Experimento de Hardy: a mais simples prova da violação do realismo local EPR**. Revista Brasileira do ensino Física. vol.41 no.4 São Paulo 2019 Epub June 13, 2019.

BATISTA; Rodrigo, NETO; José. **A Mecânica Quântica de David Bohm David Bohm 's Quantum Mechanics**. VÉRTICES, v.10 N.1/3 2008.

FRANCESE, João. **Criptografia Quântica**. Trabalho Final de rede I. Engenharia da Computação e Informação, Universidade Federal do Rio de Janeiro-RJ, 2008.

DUALIDADE Onda-Partícula: dupla-fenda de Young-Blog Responde AÍ. Disponível em: <https://www.respondeai.com.br/conteudo/quimica/estrutura-atomica/dualidade-onda-particula-e-principio-da-incerteza/1130> Acesso em: 12 de Abril 2022.

BARBOSA, Vilmar da Paixão de Souza. **Estudos das propriedades ópticas de um espelho do tipo DBR em microcavidades semicondutoras**. Universidade Federal do Amazonas. Manaus, 2010.