UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS E TECNOLOGIAS - CCT
DEPARTAMENTO DE FÍSICA
GRADUAÇÃO EM LICENCIATURA PLENA EM FÍSICA

DAVI CARDOSO DA SILVA

INTRODUÇÃO À COMPUTAÇÃO QUÂNTICA

CAMPINA GRANDE - PB
2020

DAVI CARDOSO DA SILVA

INTRODUÇÃO À COMPUTAÇÃO QUÂNTICA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Licenciatura Plena em Física da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Física.

Orientador: Prof. Dr. Jean Paulo Spinelly da Silva

CAMPINA GRANDE - PB
2020

S586i Silva, Davi Cardoso da.
Introdução à Computação Quântica [manuscrito] / Davi Cardoso da Silva. - 2020.
27 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Física) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia , 2020.
"Orientação : Prof. Dr. Jean Paulo Spinelly da Silva , Departamento de Física - CCT."
1. Computação Quântica. 2. Mecânica Quântica. 3. Qubits. 4. Estados de Bell. I. Título
21. ed. CDD 539

Elaborada por Giulianne M. Pereira - CRB - 15/714 BC/UEPB

DAVI CARDOSO DA SILVA

INTRODUÇÃO À COMPUTAÇÃO QUÂNTICA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Licenciatura Plena em Física da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Física.

Orientador: Prof. Dr. Jean Paulo Spinelly da Silva

Aprovado em 16 de outubro de 2020.

Banca Examinadora

Agradecimentos

A Deus, por tudo que tem feito em meu favor, por toda a força que me deu durante todo tempo da graduação. Honra, glória e louvor sejam dados a Ele.

A minha mãe, Elisabete Galdino da Silva, e meu pai, João Cardoso de Andrade, que sempre preserverам por meus estudos, mesmo quando as condições eram poucas, estiveram sempre ao meu lado me apoiando; muito obrigado a vocês, que foram e sempre serão a minha base, por toda a vida.

Ao meu professor Jean Spinelly, pelo excelente e brilhante profissional que é, e pela oportunidade de ter desenvolvido esse trabalho ao seu lado. Você consegue ser inspiração não só minha, mas de muitos e muitos outros alunos que passaram por você.

Aos amigos feitos durante todo esse tempo, por isso, em nome de Weslley Balbino, Carlos Rhamon e Cleanderson Fidellis, que muito estiveram ao meu lado em incontáveis momentos, estendo meu muito obrigado a todos vocês.

INTRODUÇÃO À COMPUTAÇÃO QUÂNTICA

Davi Cardoso da Silva[1]

RESUMO

O presente trabalho tem por finalidade trazer uma abordagem relacional da Física Quântica com a computação, ressaltando as perspectivas que pareciam prever um futuro de limitações à performance da mesma, e que trouxeram assim a necessidade de se pensar em uma Computação Quântica. Importantes aspectos são mostrados, como por exemplo as condições que motivaram seu uso, como se aplica a teoria quântica aos algoritimos da computação, a representação matemática e física para tais aplicações, entre alguns outros, tendo como intuito, esclarecer a partir de uma abordagem introdutória, como Computação Quântica atua numa perspectiva Física.

PALAVRAS-CHAVE: Computação Quântica. Mecânica Quântica. Qubits. Estados de Bell.

[1]Graduando em Licenciatura em Física pela Universidade Estadual da Paraíba

INTRODUCTION TO QUANTUM COMPUTATION

Davi Cardoso da Silva[1]

ABSTRACT

This work aims to take a relational approach of Quantum Physics to computing, highlighting the perspectives that seemed to predict a future of limitations to their performance, what brought the need to think about Quantum Computing. Important aspects are shown, such as the conditions that motivated its use, how quantum theory is applied to computer algorithms, the mathematical and physical representation for such applications, among others, with the objective of explaining through fundamental concepts the role of Quantum Computing in a Physical perspective.

KEYWORDS: Quantum Computing. Quantum Mechanics. Qubits. Bell States.

[1]Undergraduate Degree in Physics from the State University of Paraíba

Conteúdo

1 Introdução

Em fins do século XIX, Lorde Kelvin, um dos mais destacados e respeitados físicos da época, fazendo uma avaliação da situação da Física, afirmou que todos os problemas já haviam sido resolvidos, restando apenas duas nuvens no horizonte. Essencialmente, ele se referia ao problema da emissão e absorção de calor pelo corpo negro, e às tentativas mal sucedidas de se anular o éter. O primeiro, tratava-se, podemos dizer assim, da Física Quântica; o segundo, da Teoria da Relatividade. Foi preciso uma boa reconsideração à tudo aquilo que era verdadeiro e bem estabelecido naquela época.

Tentando explicar a radiação do corpo negro, Max Planck lançou uma ousada hipótese afirmando que a energia não era algo contínuo, mas formada por pequenos pacotes. Cada pacote foi intitulado de *quantum* de energia. Para ele, essa hipótese era apenas um truque matemático que lhe permitiu resolver o problema que, por hora, ainda estava em aberto (PLANCK, 1900). Por mais que parte da literatura, como encontramos em POLITO (e inclusive para o próprio Planck) que a hipótese desses pacotes relacionados a energia, eram *"mero artificio formal"*(POLITO, 2017. p.170), mesmo assim, seria fundamental para o novo molde da Física que estaria por vir, a saber, a Física Quântica. Para a mesma, cerca de 25 anos foram gastos até que uma teoria dos *quanta* fosse estruturada de forma lógica, ou seja, a Mecânica Quântica.

No entanto, o século XX não trouxe apenas avanços nas ciências exatas, especificamente na Física. De fato, outras áreas se desenvolveram de forma igualmente incrível, e na tecnologia não foi diferente. Por exemplo, os primeiros modelos de computadores surgiram no entorno da segunda guerra mundial, com a maquina de Alan Turing servindo para descriptografia dos códigos nazistas, como foi demonstrado na eclosão da guerra e previsto anteriormente (TURING, 1936). Posteriormente, quase que no fim da década de 50, o ENIAC apareceu, com uma massa total equivalente a 30 toneladas, e com o funcionamento por válvulas (no caso dele, algo próximo a 17 mil). Os avanços que se pensavam obter naquele tempo, em termos de tecnologia da computação,

seriam inviáveis se a tecnologia permanecesse tal como no do ENIAC.

Logo na década de 60, o funcionamento via válvulas foi trocado pelos *transistors*. Esse e tantos outros procedimentos, como a implementação dos conceitos de Unidade Central de Processametnos (CPU), memória, linguagem de programação e etc, contribuíram para que os computadores diminuíssem de tamanho consideravelmente. Porém, à medida em que se buscou cada vez mais tornar os computadores portáteis, e também mais funcionais, a quantidade desses *transistors* foi aumentando enquanto o *hardware* diminuía, até chegarmos nos *NoteBooks*.

Na década de 60, Gordon Moore, um dos fundadores da industria de microprocessadores Intel, previu que a quantidade desses *transistors*, (microprocessadores) tenderia a dobrar num tempo equivalente a 18 meses; e mais, sem que isso viesse requerer o aumento do *hardware*, ou seja, esses microprocessadores seriam cada vez menores (MOORE, 1965). Delineando uma imagem do que a lei de Moore representa (figura 1), temos na década de 60 uma ordem de 10^3 *transistors* e para à última década, uma ordem de 10^9. Com poucas variações na curva de crescimento, Moore parece ter previsto o acontecimento já que a própria Intel tem por exemplo seu processador Core i7-6950X, que possui $4,7 \times 10^9$ *transistors*.

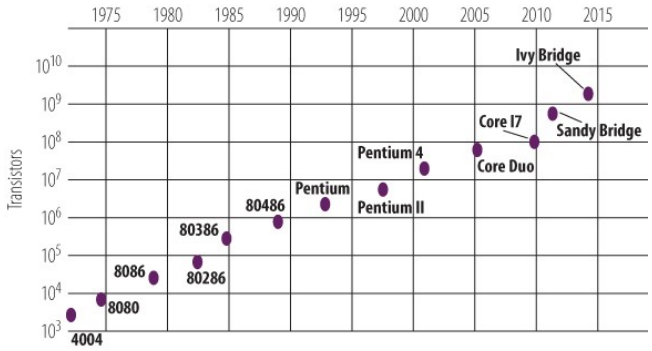

Figura 1: Lei de Moore: contagem de transistores e velocidade do processador Virtualization Essentials, 2 Edition. Fonte: IOL Training Center

Podemos nos apegar à seguinte suposição: Se o *hardware* foi reduzido ao mínimo, e estamos aumentando a quantidade de *transistors* por processadores, isso implica numa

redução dos mesmos a níveis quase que atômicos. E é daí que começa a ser gerada uma nova tendência no mercado da computação, a chamada Computação Quântica. Para a mesma, as leis da Física Clássica possivelmente irão chegar num limiar de não atenderem mais às necessidades desse novo tipo de computação. Podendo assim, abrir espaço para o uso da Física Quântica aplicada a esse mercado.

Neste trabalho analisamos de que forma a Física Quântica relaciona-se com a Computação Quântica e como alguns processos são aplicados, na tentativa de entender como muitos dos conceitos da Mecânica Quântica estão direta ou indiretamente ligados a Computação Quântica. Nosso objetivo, portanto, não aponta para o aprofundamento da teoria da computação, mas sim buscar uma entendimento dos processos quânticos aplicados à mesma.

Traçaremos uma linha da Física Clássica à Quântica, bem como analogias entre a Computação Quântica e a Clássica. Posteriormente a isso, temos breves explanações estruturais nas aplicações computacionais e seu paralelo matemático e como, apartir de simples sistemas em algorítimos, pôde se fundamentar uma boa base para a teoria da Computação Quântica. Além disso, discutmos as perspectivas promissoras nas mais diversificadas áreas do cotidiano, e como essas podem encontrar alguns obstáculos num futuro que pode não estar tão distante como pensamos.

2 Postulados da Mecânica Quântica

A Mecânica Quântica deve ser vista como uma teoria fundamental de fenômenos atômicos. Naturalmente, como os dados experimentais, nos quais ela está baseada, são derivados de eventos físicos que estão além da percepção humana direta, não é surpreendente que esta teoria envolva conceitos que não fazem parte de nossa experiência diária.

Nesta seção, iniciaremos fazendo uma discussão sobre a descrição clássica de um sistema físico e, em seguida, abordaremos como isso é feito do ponto de vista da Mecânica

Quântica.

2.1 Disposições gerais clássicas

Na mecânica clássica, o movimento de qualquer sistema físico é determinado se a posição, $\vec{r}$, e a velocidade, $\vec{v}$, de cada um de seus pontos são bem conhecidas como função do tempo. Em geral, para descrevermos um sistema, introduzimos as chamadas coordenadas generalizadas, $q_i(t)$, com $i = 1, 2, \ldots, N$, cujas derivadas com respeito ao tempo, $\dot{q}_i(t)$, são as denominadas velocidades generalizadas (SHANKAR, 1994. p.81). E, uma vez que $q_i(t)$ e $\dot{q}_i(t)$ são especificados, poderemos determinar, em qualquer instante, a posição e a velocidade de qualquer ponto do sistema. Neste caso, para encontrarmos $q_i(t)$ e $\dot{q}_i(t)$ e, consequentemente determinarmos a evolução do sistema, podemos utilizar as equações de Lagrange, as quais são dadas por (SHANKAR, 1994. p.80):

$$\frac{\partial \mathcal{L}}{\partial q_i} - \frac{d}{dt}\left(\frac{\partial \mathcal{L}}{\partial \dot{q}_i}\right) = 0 \ , \quad i = 1, 2, ..., N, \tag{2-1}$$

onde $\mathcal{L} = \mathcal{L}(q_i, \dot{q}, t)$ é a função conhecida como lagrangiana. Especificamente, quando a força que atua no sistema é derivada de um potencial, $V(q_i, t)$, tal função é expressa por $\mathcal{L} = T - V$, sendo T a energia cinética.

Também podemos descrever um sistema clássico em termos de $q_i(t)$ e do momento conjugado, p_i, para cada uma das coordenadas generalizadas, o qual é definido por

$$p_i = \frac{\partial \mathcal{L}}{\partial \dot{q}} \ . \tag{2-2}$$

Nesta situação, o comportamento do sistema deve ser estudado pelas equações canônicas de Hamilton-Jacobi, a saber (SHANKAR, 1994. p.88);

$$\frac{dq_i}{dt} = \frac{\partial \mathcal{H}}{\partial p_i} \qquad \text{e} \qquad \frac{dp_i}{dt} = -\frac{\partial \mathcal{H}}{\partial q_i} \ , \quad i = 1, 2, ..., N, \tag{2-3}$$

em que

$$\mathcal{H}(q_i, p_i, t) = \sum_{i=1}^{N} p_i \dot{q}_i - \mathcal{L}(q_i, \dot{q}, t) \ . \tag{2-4}$$

é a função denominada hamiltoniana.

As variáveis $q_i(t)$ e $p_i(t)$ (i = 1, 2, ... ,N) são chamadas de variáveis fundamentais da dinâmica, pois todas as quantidades físicas associadas ao sistema (energia, momento angular, etc.) podem ser expressas em termos delas. Por exemplo, no caso em que $V = V(q_i, t)$ a hamiltoniana, que é uma função de q_i, p_i e t, representa a energia total do sistema. Nesse sentido, podemos afirmar que o estado de uma sistema clássico, em um tempo t, é completamente especificado pelas N coordenadas generalizadas e por seus N momentos conjugados. Obviamente, como as equações diferenciais (**??**) são de primeira ordem, precisamos conhecer q_i, p_i em um instante t_0 para podermos prever, com certeza, os valores dessas quantidades e, consequentemente, de todas as outras, em um tempo t.

Se por um lado, toda pequena discussão feita acima nos remete ao fato de que classicamente conseguimos descrever o comportamento de um determinado sistema dado as condições vistas por outro, poderíamos pensar que, num estado quântico, tais perguntas seriam relevantes: (a) Como um estado de um sistema quântico pode ser descrito em função do tempo matematicamente? (b) Para esse estado, como podemos prever os resultados e observá-los em quantidades físicas? (c) Estando definido em t_0, como definir o mesmo em um tempo arbitrário t?

2.2 Os postulados

A Mecânica Quântica, conforme encontramos em algumas literaturas é uma teoria estruturada de forma axiomática (SHANKAR, 1994), e para além da especificidade dentro da Física, esse entendimento é tido por base também nas literaturas aplicadas a Computação Quântica (NIELSEN; CHUANG, 2010) como veremos mais à frente, ou seja, isto quer dizer que ela está fundamentada em postulados. Na sequência, enunciaremos tais postulados e, logo após, faremos as discussões sobre as questões levantadas na seção anterior.

Podemos, observar e sintetizar os postulados da seguinte forma (COHEN-TANNOUDJI; et al, 1977. p.215-222);

- **Primeiro postulado**: Para um tempo fixo t_0 o estado para um sistema físico pode ser definido especificando um ket $|\psi(t_0)\rangle$ pertencente ao espaço $\mathcal{E}$ [1].

- **Segundo postulado**: Cada quantidade física mensurável A é descrita por um operador $\hat{A}$ atuando em $|\mathcal{E}\rangle$; tal operador representa um observável.

- **Terceiro postulado**: O único resultado possível da medição de uma quantidade física A é um dos autovalores do correspondente observável $\hat{A}$.

- **Quarto postulado**: Quando A é medido em um estado normalizado $|\psi\rangle = \sum_n c_n |u_n\rangle$, onde $|u_n\rangle$ é o autovetor normalizado de $\hat{A}$ associado ao autovalor a_n e $c_n = \langle u_n | \psi\rangle^2$, a probabilidade de encontrar o autovalor não-degenerado[3] a_n é $\mathcal{P}(a_n) = |c_n|^2$.

- **Quinto postulado**: Se a medição da quantidade física A no sistema de estado $|\psi\rangle$ fornece o resultado a_n, o estado do sistema, imediatamente após a medição, é a projeção normalizada, $\hat{P}_n|\psi\rangle/\sqrt{\langle\psi|\hat{P}_n|\psi\rangle}$, de $|\psi\rangle$ no autosubespaço associado a a_n[4].

- **Sexto postulado**: A evolução temporal do vetor de estado $|\psi(t)\rangle$ é governada pela equação de Schrödinger: $i\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}(t)|\psi(t)\rangle$, onde $\hat{H}(t)$ é o operador associado à energia total do sistema, também chamado de operador Hamiltoniano.

Diferentemente da Mecânica Clássica, onde o estado de um sistema, em um instante t_0, é descrito $q_i(t_0)$ e $p_i(t_0)$, o primeiro postulado estabelece que, na Mecânica Quântica, tal estado é representado por um ket $|\psi(t_0)\rangle$, pertencente ao espaço estado $\mathcal{E}$. É importante destacar que, como $\mathcal{E}$ é um espaço vetorial, um vetor estado $|\psi\rangle$ pode ser escrito como $|\psi\rangle = \sum_n c_n |u_n\rangle$, em que $|u_n\rangle$ são os autovetores de um observável $\hat{A}$, que corresponde

[1] Como o espaço é vetorial, vale o princípio de superposição, onde: a combinação de vetores estados também é um vetor estado.

[2] Projeção de $|\psi\rangle$ na componente da base $\{|u_n\rangle\}$.

[3] Também podemos ter o mesmo princípio aplicado em outros espectros, como espectro discreto degenerado e espectro parcialmente contínuo.

[4] $\hat{P}_n \equiv |u_n\rangle\langle u_n|$ é o operador projetor no subespaço $\{|u_n\rangle\}$.

à quantidade A, associada aos autovalores a_n. Outro aspecto que difere da descrição clássica é a forma como as quantidades físicas podem ser previstas e observadas. De fato, a teoria quântica não prevê os resultados de forma exata, como seria na clássica. Na verdade, conforme afirmam os terceiro e quarto postulados, estando o sistema no estado $|\psi\rangle$, os resultados possíveis da medição de uma determinada quantidade física A são os autovalores a_n, sendo que cada valor é obtido com uma probabilidade $|c_n|^2$. No que diz respeito à evolução temporal, o sexto postulado afirma que para obtermos tal informação deveremos resolver a equação de Schrödinger.

3 0 ou 1, ou 0 e 1

Nos computadores atuais (entenda-se, segunda década do século XXI), ou ainda computadores clássicos no jargão dos físicos, a menor unidade de informação, que pode ser armazenada ou transmitida, é denominada *bit*, e este pode assumir apenas dois valores: zero ou um. Nesses computadores, um *bit* pode ser representado fisicamente pelos dois valores de tensão aplicados num fio (sintetizados por componentes eletrônicos dentro de chips ou microchips), pelas diferentes direções de magnetização em uma fita magnética, ou de outras formas, desde que seja possível identificar dois estados diferentes (SOUSA FILHO; ALEXANDRE, 2014. p.19).

Já nos computadores quânticos, diferentemente do *bit*, temos o *qubit*, que graças ao princípio da superposição, pode assumir os valores: zero ou um, ou ainda, representar simultaneamente esses dois valores. Fisicamente falando, a princípio, há diferentes sistemas que podem representar um *qubit*: íons aprisionados em armadilhas magnéticas; átomos e fótons armazenados em cavidades supercondutoras de eletricidade; átomos ocupando "vales" de uma rede cristalina óptica, "superfície" que curiosamente lembra uma caixa de ovos formada por ondas eletromagnéticas estacionárias, como registrado pela *IBM Research Division* (KITTEL, 2005. p.19); pontos quânticos (conjunto de elétrons confinados a dimensões nanométricas) e spin's nucleares. Contudo, como veremos mais a

frente, nem todas essas maneiras de representação são usáveis.

Os *qubits* se mostram muito mais eficientes que sua contra partida clássica. Realmente, como consequência dos diferentes aspectos que caracterizam os computadores clássico e quântico, enquanto n *bits* armazenam n informações, um conjunto constituído por n *qubits* consegue armazenar 2^n informações.

Formalmente, um *qubit* pode ser descrito por qualquer sistema quântico que possua dois autoestados distintos, os quais podem ser indicados pelos vetores ortonormalizados $|0\rangle$ e $|1\rangle$[5]. Então, assumindo que $|\alpha|^2$ e $|\beta|^2$ sejam as probabilidades de encontrarmos o sistema nos estados 0 e 1, respectivamente, o princípio da superposição estabelece que o vetor que representa um *qubit* deve ser dado por:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \ . \tag{3-5}$$

Naturalmente, como os vetores $|0\rangle$ e $|1\rangle$ são ortonormais, devemos ter $|\alpha|^2 + |\beta|^2 = 1$. Além disso, conforme vimos no quinto postulado, após uma medição que resulte nos estados 0 ou 1, a superposição de estados será levada, respectivamente, a $|\psi'\rangle = |0\rangle$ ou $|\psi'\rangle = |1\rangle$.

Assim como acontece no caso em que consideramos apenas um *qubit*, o estado de dois *qubits* pode ser escrito como uma combinação linear. Classicamente, teríamos as opções para medição dos bits como $00, 01, 10, 11$. Porém, quânticamente, podemos ter essas opções mais a sobreposição desses estados, na seguinte forma (NIELSEN; CHUANG, 2010. p.16):

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \ . \tag{3-6}$$

De fato, ao trabalharmos com um sistema de 2 *qubits*, em que um está no estado $|\varphi\rangle$ e o outro no estado $|\gamma\rangle$, dados por

$$|\varphi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle \quad \text{e} \quad |\gamma\rangle = \beta_0\,|0\rangle + \beta_1\,|1\rangle \ , \tag{3-7}$$

[5]Por definição, sendo $|0\rangle$ e $|1\rangle$ vetores ortonormais, as relações $\langle 0|0\rangle = \langle 1|1\rangle = 1$ e $\langle 0|1\rangle = \langle 1|0\rangle = 0$ devem ser satisfeitas.

o vetor que representa esse sistema é descrito pelo produto tensorial (COHEN-TANNOUDJI; et al, 1977. p.154)

$$\begin{aligned} |\varphi\rangle \otimes |\gamma\rangle &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\beta_0 (|0\rangle \otimes |0\rangle) + \alpha_0\beta_1 (|0\rangle \otimes |1\rangle) + \\ &\quad \alpha_1\beta_0 (|1\rangle \otimes |0\rangle) + \alpha_1\beta_1 (|1\rangle \otimes |1\rangle) \Rightarrow \\ |\varphi\rangle \otimes |\gamma\rangle &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \ . \end{aligned} \tag{3-8}$$

Este resultado mostra que, realmente, o vetor estado que descreve 2 *qubits* é do tipo apresentado na equação **??**.

Como implicações associadas aos estados de 2 *qubits*, podemos citar os chamados *estados separáveis* e os *estados emaranhados* (BARBOSA, 2019. p.22). Na sequência falaremos apenas do primeiro caso.

Supondo que, para o estado $|\psi\rangle$, a medição para o primeiro *qubit*, seja 0, esse estado se tornaria;

$$|\psi'\rangle = \frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \ , \tag{3-9}$$

ou ainda,

$$|\psi'\rangle = |0\rangle \otimes \left(\frac{\alpha_{00} |0\rangle + \alpha_{01} |1\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \right) \ . \tag{3-10}$$

Dada a possibilidade de reescrever $|\psi'\rangle$ desta última forma, o estado é chamado de *estado separável*. Outros exemplos poderiam ser mostrados, mas não é toda configuração com estado de 2 *qubits* que podem ser reescritos como nesse caso, para este, dizemos, como afirma Brumato (2010): *"é um estado não atingível por uma combinação linear de estados individuais dos Qubits"*. Para tal, assim como na Computação Clássica, que é regida por sistemas que possuem portas lógicas[6], temos em nossa situação as chamadas

[6]Operam em bits de entrada gerando bits de saídas, como por exemplo a porta negação clássica, ou, a porta NOT, que dependendo do bit de entrada inverte-o para gerar um de saída, se o bit de entrada for 0, gera como saída 1 e vice versa

portas lógicas quânticas, funcionando na variação de um estado qualquer de 2 *qubits* ou em múltiplos. O fato é que o uso dessas portas, como mostraremos, consegue nos gerar estados que dão suporte pra grande parte da teoria da Computação Quântica.

4 Portas e atuações nos estados $|\psi\rangle$

É de suma importância buscar um paralelo entre a Computação Clássica e a Computação Quântica, tendo em vista traçar variações nas duas abordagens, bem como melhorias, vantagens ou desvantagens. Ao falarmos das portas nessa sessão, traremos uma noção algébrica de seus respectivos funcionamentos atuando nos estados $|\psi\rangle$.

Assim como o uso da porta NOT, na Computação Clássica, resulta num bit inverso ao de entrada (SOUSA FILHO, 2014. p.110), somos tentados a supor que, na computação quântica, dado um estado $|0\rangle$ como entrada, resulte em um estado de saída $|1\rangle$. Então, considerando que $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, a contrapartida da porta NOT clássica resultaria para nós, quânticamente, em $|\psi'\rangle = \beta\,|0\rangle + \alpha\,|1\rangle$.

Devido à notação vetorial dos estados quânticos, as portas que representam as modificações nesses estados, são descritas por operadores lineares. Assim, assumindo que $\hat{X}$ é o operador associado à porta NOT, temos que $\hat{X}\,|0\rangle = |1\rangle$, $\hat{X}\,|1\rangle = |0\rangle$ e, por conseguinte,

$$|\psi'\rangle = \hat{X}\,|\psi\rangle = \alpha\hat{X}\,|0\rangle + \beta\hat{X}\,|1\rangle \Rightarrow |\psi'\rangle = \beta\,|0\rangle + \alpha\,|1\rangle \ . \tag{4-11}$$

Podemos, ainda, escrever a relação acima em termos das matrizes que representam os vetores e o operador na base $\{|e_i\rangle\} = \{|0\rangle\,, |1\rangle\}$, como segue:

$$\psi' = X\psi \ . \tag{4-12}$$

em que

$$\psi' = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \ , \quad \psi = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad \text{e} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \ , \tag{4-13}$$

onde ψ' e ψ são, respectivamente, as matrizes constituídas pelas componentes dos vetores $|\psi'\rangle$ e $|\psi\rangle$, na referida base, enquanto que os elementos da matriz X são dados por $X_{ij} = \langle e_i|e_j\rangle$.

Existem infinitas portas que podem ser aplicadas aos *qubits*, desde que sejam unitárias, essa é a única restrição para se construir tais portas (VON ZUBEN, 2007. p.43). É importante lembrar que uma porta unitária T, qualquer, é de fato unitária se a matriz que a representa obedecer a seguinte relação: $T^\dagger T = I$, onde $T^\dagger$ é definida como a matriz transposta e conjugada de T (GRIFFITHS, 2011. p.330). Essa única restrição consegue deixar fechada uma relação já citada, de que $|\alpha|^2 + |\beta|^2 = 1$. Observe que para a porta X, fazendo $X^\dagger X$, de fato conseguimos obter I. A porta X nos serviu de comparativo em detrimento da porta clássica, no entanto, outras portas de extrema importância para algumas aplicações - também para o uso do Teleporte Quântico, como veremos mais a frente -, tendo em vista a formação de algorítimos para a Computação Quântica, são as portas *Z-FLIP*, *Hadamard* e a porta *C-NOT*, representadas respectivamente pelas matrizes (operadores):

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{e} \quad U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{4-14}$$

Em tese, a porta X troca por 1; a porta Z nada faz com o 0 e inverte o sinal do 1; a porta *Hadamard*, quando tivermos 0, torna 0 + 1 e quando for 1, torna 0 - 1. Essas portas atuam para *qubits* únicos. A porta *C-NOT* atua em sistemas de 2 *qubits*, mantem o primeiro *qubit* sempre que tivermos 0, e troca o segundo quando tivermos 1 (semelhante à função da porta *NOT*).[7]

A atuação dessas portas nos sistemas de *quibits* nos traz à tona a discussão lançada anteriormente de que, apesar de termos os Estados Separáveis (para o caso de 2 *qubits*), nem todo estado poderia ser reescrito de tal forma. Na verdade, portas escolhidas corretamente e postas sobre algorítimos são capazes de nos gerar novos estados,

[7]Vale a pena lembrar que os números na notação usual estão nos Ket's, por conveniência, apenas para mera síntese do funcionamento das portas, usamos os números como seguem na discussão.

diferentemente dos Estado Separáveis. A Figura 2 mostra esse processo, onde as linhas

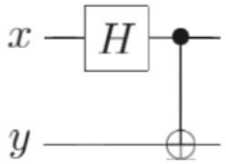

Figura 2: Algorítimo de 2 *qubits*, utilizando as portas de *Hadamard* e *C-NOT*.

x e y são, na verdade, os *qubits* que individualmente podem ser 0 ou 1; como resultado de saída temos então $|\psi_{xy}\rangle$. Os estados criados a partir desse algorítimo são chamados de Estados de Bell (NIELSEN; CHUANG, 2010. p.26), e estão dispostos como visto na Tabela 1:

Entrada	Saída (Estados de Bell)
$\|00\rangle$	$\|\psi_{00}\rangle = \frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
$\|01\rangle$	$\|\psi_{01}\rangle = \frac{\|01\rangle + \|10\rangle}{\sqrt{2}}$
$\|10\rangle$	$\|\psi_{10}\rangle = \frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
$\|11\rangle$	$\|\psi_{11}\rangle = \frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$

Tabela 1: Estados de Bell gerados dado as entradas dos *qubits* a partir das portas lógicas quânticas *Hadamard* e *C-NOT*.

Observando $|\psi_{00}\rangle$, uma outra forma possível para reescrevê-lo seria:

$$|\psi_{00}\rangle = \frac{(|0\rangle \otimes |0\rangle) + (|1\rangle \otimes |1\rangle)}{\sqrt{2}} \ . \tag{4-15}$$

Note que, no caso dos Estados Separáveis tínhamos um termo que ainda estava num estado de sobreposição (como vimos pela equação 3-10), claramente nesse novo caso não temos o mesmo acontecendo. Uma curiosidade desses estados é que os mesmos possuem uma propriedade intrínseca a eles, a de que os resultados de medição estarão sempre correlacionados; por isso são chamados de Estados Emaranhados ou *"Estados*

Maximamente Emaranhados" (RIGOLIN, 2008. p.4). Esses estados foram de muita serventia para aplicações na Computação Quântica bem como para gerar expectativas para se trabalhar com n *qubits*, como por exemplo a especulação da quantidade dos estados gerados por esses, que resulta 2^n estados, sendo n o número de *qubits* a se trabalhar. Veremos em seguida um importante circuito usado como aplicação das relações vistas até agora.

5 Aplicação dos Estados de Bell: Teleporte Quântico

O Teleporte foi uma das promessas experimentais na área de informação quântica. Descoberto por Bennett e seus colegas (BENNETT; et al, 1993), foi obtido experimentalmente em 1997, pela equipe de Dik Bouweester, da Universidade de Oxford. Sendo bastante divulgado na mídia mundial, gerou uma esperança de ter relações com o teletransporte das ficções científicas. A diferença é que nessa situação fictícia, há o transporte de matéria, no Teleporte, há apenas o transporte de informação quântica.

Nessa seção, trataremos esse fenômeno de maneira formal.

A representação do sistema capaz de efetuar o Teleporte é vista na Figura 3:

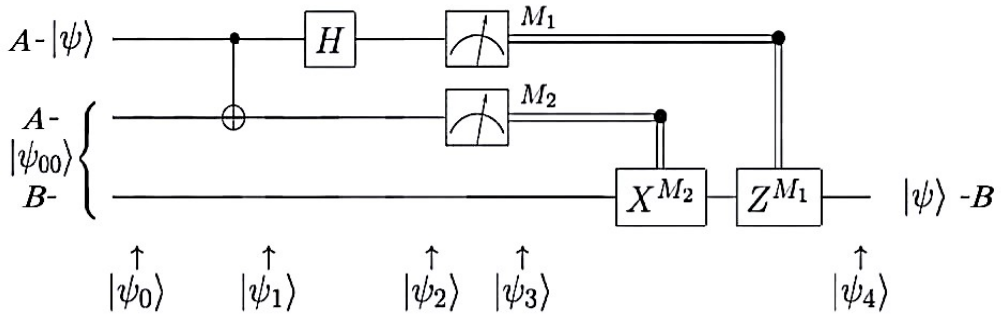

Figura 3: Sistema capaz de gerar o Teleporte Quântico - As linhas únicas que saem de $|\psi\rangle$ (laboratório A) e de $|\psi_{00}\rangle$ (laboratórios A e B) indicam um *qubit*, a linha vertical indica a operação *C-NOT*, seguida da operação *Hadamard*. M_1 e M_2 são medidas feitas colapsando o estado $|\psi_2\rangle$, as linhas duplas indicam um bit clássico, ou 0 ou 1. Apartir dessas medidas, serão feitas ou não as operações *NOT* e *FLIP*, garantindo que o estado $|\psi_4\rangle$ que chega ao laboratório B, seja de fato o estado inicial $|\psi\rangle$ teleportado.

Vamos supor que o estado $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ está num laboratório A, e que pretendemos transportà-lo ao laboratório B. Além disso, vamos admitir que também existe um estado de Bell $|\psi_{00}\rangle$[8] compartilhado aos dois. Desse modo, o estado de entrada do sistema é: $|\psi_0\rangle = |\psi\rangle \otimes |\psi_{00}\rangle$, ou seja:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle \otimes (|00\rangle + |11\rangle) + \beta\,|1\rangle \otimes (|00\rangle + |11\rangle)\right] \ . \tag{5-16}$$

A primeira operação, que é a porta *C-Not*, mantem ou muda o primeiro *qubit* (que é na verdade um Estado de Bell), se o *qubit* de controle, que se encontra no estado $|\psi\rangle$, for $|0\rangle$ ou $|1\rangle$, respectivamente. Assim, após essa atuação, o sistema atinge o estado:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle \otimes (|00\rangle + |11\rangle) + \beta\,|1\rangle \otimes (|10\rangle + |01\rangle)\right] \ . \tag{5-17}$$

A segunda operação, que é a porta de Hadamard (H), transforma $|0\rangle$ em $(|0\rangle + |1\rangle)/\sqrt{2}$ e $|1\rangle$ em $(|0\rangle - |1\rangle)/\sqrt{2}$. Logo, levando em conta que essa porta atua apenas em $|\psi\rangle$, após tal operação o estado acima torna-se:

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha\,(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + \beta\,(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle)\right] \ . \tag{5-18}$$

Como consequência, fazendo os produtos e reagrupando os termos, obtemos:

$$\begin{aligned} |\psi_2\rangle \ = \ & \frac{1}{2}\left[|00\rangle \otimes (\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle \otimes (\alpha\,|1\rangle + \beta\,|0\rangle)\right. \\ & \left. + |10\rangle \otimes (\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle \otimes (\alpha\,|1\rangle - \beta\,|0\rangle)\right] \ . \end{aligned} \tag{5-19}$$

A terceira operação será as medições M_1 e M_2 feitas pelo laboratório A, que indicará exatamente o que o laboratório B executará: se atuará somente a porta X, somente a porta Z, ou as duas, ou nenhuma delas.

Uma vez que os *qubits* possuem apenas dois estados independentes, as medições M_1 e M_2 poderão resultar em 00, 01, 10 ou 11. Caso o primeiro resultado seja encontrado em A, o Teleporte ocorrerá sem a necessidade de nenhuma outra operação em B; porém, se o resultado for o segundo, o laboratório B precisará executar a operação X; já se for

[8] Um dos Estados de Bell, ver Tabela 1.

o terceiro, a operação Z deverá ser realizada; finalmente, se o quarto valor for medido, as operações X e Z serão necessárias. A Tabela 2 sintetiza os possíveis resultados das medições M_1 e M_2, os estados $|\psi_3\rangle$ e as devidas operações que devem ser realizadas nesse estado para que haja o Teleporte.

Medições M_1 e M_2 em A	Chegada das medições em $\|\psi_3\rangle$ em B	Operações necessárias para teleportar
0 e 0	$\alpha\|0\rangle + \beta\|1\rangle$	
0 e 1	$\alpha\|1\rangle + \beta\|0\rangle$	X
1 e 0	$\alpha\|0\rangle - \beta\|1\rangle$	Z
1 e 1	$\alpha\|1\rangle - \beta\|0\rangle$	X e Z

Tabela 2: Sintetização do Estado $|\psi_3\rangle$ após as medições M_1 e M_2 usando ou não as portas X e Z para gerar $|\psi_4\rangle$.

É importante destacar que, após as medições M_1 e M_2, o que temos é um Estado Teleportado , a saber, $|\psi\rangle$, que é então perdido (tendo em vista que as medições levaram ao colapso o estado $|\psi_2\rangle$).

Essa configuração, não tão atual (final da década de 90), apesar de simples, serviu de grande inspiração para cientistas continuarem os estudos da computação quântica. Para aquela época não se esperaria tanto interesse pela área, que geraria anos mais tarde institutos de pesquisas, cujo estudos se popularizaram através de divulgações em mídias como o The New York Times, dando destaque a temática. Na oportunidade, duas equipes de cientistas trabalharam com trigêmeos de átomos carregados presos em campos magnéticos. Também não se pensava que o experimento do Teleporte, realizado a uma distância ínfima, teria um alcance chegaria a distâncias de 100km, sem perda da informação transportada, como chegou a mostrar uma das edições da revista *Nature* (VALIVARTHI; et al, 2016). Sem dúvida, os Estados de Bell aplicados a algoritmos e gerando circuitos, ainda que simples como esse, possibilitaram novas abordagens para a Computação Quântica e um avanço significativo na virada do milênio.

6 Considerações Finais

Neste trabalho analisamos uma aplicação simples da Computação Quântica, associando os Estados de Bell a algoritmos, e esclarecendo alguns conceitos nem um pouco triviais encontrados em muitas publicações, apresentando assim, o algorítimo do Teleporte de forma mais acessível ao leitor interessado neste tema.

Conceber *qubits*, o item primordial para a Computação Quântica, é uma tarefa capaz e testada teórica e praticamente. Mas em tese, as maneiras mais usuais de se fazer isso são, através do spin eletronico ou por polarização de fótons (BRUMATTO, 2010). O grande e talvez maior problema é a instabilidade dos mesmos, conhecido como *descoerência*. Esta, ocorre quando não se tem uma sistema capaz de manter os *qubits* estáveis para as operações desejadas, gerando um colapso generalizado nos estados de todo o sistema quântico. A estabilidade de um sistema com poucos *qubits*, que possuem dimensões atômicas, podem requerer salas amplas com inúmeros recursos para o total isolamento do sistema, o que gera um custo financeiro muito elevado. A solução para esse problema, já vem sendo pensada por meio de estudos, como por exemplo os estudos sobre as *medidas projetivas*, que trabalham nas possíveis resoluções da descoerência, e com a possibilidade de se trabalhar com sistemas abertos.

Na indústria financeira e nas comunicações com os sistemas de criptografia, nas indústrias com aumento da eficiência em problemas de busca, na saúde com sistemas de otimização de processos, na área militar com o Ghost Imaging (DEYANG DUAN, 2013), como testou o governo americano no ano de 2013, entre outras aplicações, a Computação Quântica tem boas perspectivas para um futuro possivelmente não tão distante. Isso gera motivação em grandes empresas como a IBM, Google, D-Wave, Microsoft, entre outras, para que hoje estejam investindo milhões de dólares em pesquisas e implementações. Talvez, porque as expectativas sobre a Computação Quântica hoje são muito mais abrangentes do que se pensava anos atrás.

A Computação Quântica além de se mostrar promissora, encontra pela frente inúmeros

avanços a serem alcançados (assim como foi na Computação Clássica em seus primórdios) Tais avanços podem gerar melhorias incontestáveis ao homem, e que essas aconteçam e a Física possa ser crucial para o processo.

7 Referências

ARRUDA, L.G.E. **Computação Quântica baseada em medidas projetivas em sistemas abertos**. Instituto de Física de São Carlos - USP (Tese de Doutorado), 2011.

BARBOSA, L.V. **Entanglement Witnesses with Tensor Networks - Characterizing entanglement in large systems**. Universidade Federal de Minas Gerais - (Dissertação de Mestrado), 2019.

BENNETT, C.H.; et al. **Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels**. Phys. Rev. Lett. 70, 1895 Published 29 March 1993. Disponível em: https://doi.org/10.1103/PhysRevLett.70.1895.

BRUMATTO, H.J. **Introdução à Computação Quântica**. Unicamp, 2010.

CHANG, K. **Scientists Teleport Not Kirk, but an Atom**. The New York times, June 17, 2004. Disponível em: https://www.nytimes.com/2004/06/17/us/scientists-teleport-not-kirk-but-an-atom.html.

COHEN-TANNOUDJI, C.; DIU, B.; LALOE, F.**Quantum Mechanics**. New York: Wiley-Interscience Publication, 1977. 898 p.

DEYANG DUAN.; SHAOJIANG DU.; AND YUNJIE XIA. **Multiwavelength ghost imaging**. Phys. Rev. A 88, 053842 Published 25 November 2013. Disponível em:https://doi.org/10.1103/PhysRevA.88.053842.

GRIFFITHS, D. J. **Mecânica Quântica**. 2e, Pearson, 2011.

GOLDSTEIN, F.P.; CHAVES, G.L; ZILLI, P.K. **Breve introdução à Computação Quântica**. Campinas, 2005.

KITTEL, CHARLES. **Introduction to Solid State Physics**. New York, John Wiley

& Sons. 2005.

MOORE,

E.G. **Cramming more components onto integrated circuits**.**Electronics**, Volume 38, Number 8, April 19, 1965. Disponível em: https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf.

NIELSEN, M.A.; CHUANG, I.L. **Quantum Computation and Quantum Information.**. Cambridge: Cambridge University Press, 2010. 676 p.

PLANCK, M. **On an improvement of Wiens spectral distribution, Verhandlungen der Deutschen Physikalischen Gesellschaft, 2, 202204**. Also published in Plancks collected papers: Physikalische 170 Abhandlungen und Vortrage, 1, pp. 687689, Braunschweig: Friedr.Vieweg und Sohn. English Translation: Plancks Original Papers in Quantum Physics, (1972), annotated by H. Kangro, pp. 3845. London: Taylor and Francis.

POLITO, A. M. M. **Radiação de Corpo Negro e os Primórdios da Física Quântica**. Physicae Organum. Brasília, vol.3, n.2. 2017

RIGOLIN, G. **Emaranhamento Quântico**. Revista Phisicae, 7 - 2008.

SHANKAR, R. **Principles of Quantum Mechanics. Second Edition** . New York, 1994. 2nd ed. 2011. 676 p.

SOUSA FILHO, G.F.; ALEXANDRE, E.M. **Introdução à computação**. 2a Edição. João Pessoa. Editora da UFPB, 2014. 143 p.

TURING, A.M. **On computable numbers, with an application to the Entscheidungsproblem**. J. of Math, v. 58, n. 345-363, p.5, 1936.

VALIVARTHI, R.; PUIGIBERT, M.; ZHOU, Q.; et al. **Quantum teleportation across a metropolitan fibre network**. Nature Photon 10, 676680 (2016). Disponível em: https://doi.org/10.1038/nphoton.2016.180.

VON ZUBEN, F.J. **Computação Quântica**. Material baseado nas notas de aula do Prof. Leandro Nunes de Castro (UniSantos/SP). Reprodução de conteúdo autorizada pelo autor. Edições realizadas pelo Prof. Romis R. F. Attux em 2007.

A Teorema No Cloning

Supondo que exista uma operação que consiga fazer: $|\psi\rangle \otimes |S\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$, ou seja, levar um Estado $|S\rangle$ a um estado $|\psi\rangle$, essa operação deve ser capaz de fazer isso a qualquer estado, chamaremos essa operação de $\hat{U}$. Vejamos essa operação num estado $|\psi\rangle$ e num estado $|\varphi\rangle$.

$$\hat{U}\left(|\psi\rangle \otimes |S\rangle\right) = |\psi\rangle \otimes |\psi\rangle \ . \tag{A-20}$$

$$\hat{U}\left(|\varphi\rangle \otimes |S\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle \ . \tag{A-21}$$

Tomando o produto direto entre as duas relações acima, temos:

$$[\langle\psi| \otimes \langle S|\, \hat{U}^{\dagger}][\hat{U}\,|\varphi\rangle \otimes |S\rangle] = [\langle\psi| \otimes \langle\psi|][|\varphi\rangle \otimes |\varphi\rangle] \ . \tag{A-22}$$

Sabemos que, $\hat{U}^{\dagger}\hat{U} = I$, e que, $\langle S|\ S\rangle = 1$, ficamos com:

$$\begin{aligned} \langle\psi|\ \varphi\rangle &= \langle\psi|\ \varphi\rangle\,\langle\psi|\ \varphi\rangle \\ \langle\psi|\ \varphi\rangle &= |\langle\psi|\ \varphi\rangle|^2 \ . \end{aligned} \tag{A-23}$$

A igualdade acima é verdade se:

$$\langle\psi|\ \varphi\rangle = 0$$

$$\langle\psi|\ \varphi\rangle = 1$$

Portanto, não se clona um estado inicial, o que conseguimos é sempre um estado ortogonal ou paralelo a ele.