

**Universidade Paulista - UNIP**

**Geovani Moreira de Souza**

**Iniciando na Computação Quântica**

**Limeira  
2019**

**Universidade Paulista - UNIP**

**Geovani Moreira de Souza**

Iniciando na Computação Quântica.

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da computação sob a orientação do professor **Me. Nome do Professor**.

**Limeira  
2019**

Iniciando na Computação Quântica.

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da Computação sob a orientação do professor **Me. Nome do Professor.**

Aprovada em **XX** de **XXXXX** de 201**X**.

### **BANCA EXAMINADORA**

---

**Prof. Dr. Nome completo**

---

**Prof. Me. Nome completo**

---

**Prof. Esp. Nome completo**

## DEDICATÓRIA

Acima de tudo a Deus, por ter me dado sabedoria, saúde e disposição para a realização deste trabalho.

Aos meus pais, que me deram toda a estrutura.

Agradeço também a minha irmã Aline, sempre ajudando no que esta ao seu alcance.

A minha noiva Rosilene. Obrigado meu amor, por tudo. Obrigado pelo seu carinho, sua atenção, sua alegria com as minhas conquistas e seu ombro em cada momento difícil que você me ajudou a atravessar.

Obrigado ao professores, pela paciência, pelo amor a ciência da computação, sem vocês esse curso não seria minha paixão.

Meu sinceros agradecimentos a todos que que contribuíram para que eu subisse mais um degrau na vida.

Muito obrigado!

*“Se, a princípio, a ideia não é absurda,  
então não há esperança para ela”.*

(Albert Einstein)

## RESUMO

A Computação Quântica é construída sobre a teoria da mecânica quântica, na qual não muito transparente ao entendimento dos seres humano. A muitos séculos os físicos veem dedicando suas vidas para tronar as previsões da mecânica quântica mais palpáveis com a junção da ciência da computação e a teoria da informações tivemos grandes transformações na concepção da mecânica quântica nas quais descrevo neste trabalho.

Palavra-Chave: Mecânica, Computação, Quântica.

## **ABSTRACT**

Quantum Computation is built on a theory of quantum mechanics that is not very transparent to the understanding of human beings. For many centuries physicists have been devoting their lives to thriving as more palpable quantum mechanics tests with a junction of computer science and an information theory that we have had major transformations in the mechanics.

Key Words: Mechanics, Computing, Quantum.

## LISTA DE FIGURAS

FIGURA 1- SPIN DO ELETRÔN.....	14
FIGURA 2 CENÁRIO .....	24



## Sumário

1. INTRODUÇÃO.....	10
1.1 Objetivo.....	10
1.2 Justificativa.....	10
1.3 Metodologia.....	10
2. MECÂNICA QUÂNTICA.....	11
<b>2.1. Definição de mecânica quântica.....</b>	<b>12</b>
<b>2.1.1. Dualidade onda partícula.....</b>	<b>12</b>
<b>2.1.2. Superposição de estados.....</b>	<b>13</b>
<b>2.1.3. Emaranhamento de estados quânticos.....</b>	<b>14</b>
3. COMPUTAÇÃO QUÂNTICA.....	16
<b>3.1. Simulações "eficientes" versus "ineficientes".....</b>	<b>17</b>
<b>3.2. Bit Quântico.....</b>	<b>18</b>
<b>3.3. Portas de um qubit único.....</b>	<b>21</b>
<b>3.7. Porta (<math>\sqrt{NOT}</math>).....</b>	<b>22</b>
<b>3.8. Circuitos quânticos.....</b>	<b>22</b>
<b>3.9. O que da pra fazer com algoritmos quânticos?.....</b>	<b>23</b>
4. MODELO DE APRESENTAÇÃO DINÂMICA.....	23
CONCLUSÃO.....	25
Referências.....	26

## **1. INTRODUÇÃO**

O campo da computação quântica é na verdade, um subcampo da informação quântica, que inclui criptografia quântica e comunicação quântica.

A computação quântica se desenvolveu nas últimas duas décadas, de uma ideia visionária a uma das áreas mais fascinantes da mecânica quântica **(Cuffaro, 2015)**.

### **1.1 Objetivo**

O objetivo desse trabalho é despertar o interesse do público em geral, sobre a Computação Quântica. A minha proposta é dar uma visão geral e bastante ampla desta área de estudo tão nova da computação.

Utilizando ferramentas da computação gráfica em uma apresentação bastante intuitiva e dinâmica, para que possa facilitar o entendimento do assunto abordado, principalmente ao estudante e até mesmo o profissional da área da Ciência da Computação.

### **1.2 Justificativa**

A Computação Quântica já é algo real e logo estará por toda parte, a mecânica quântica, a base da computação quântica é uma área cheia de mistérios e de difícil compreensão e com pouco material de fácil entendimento para quem deseja iniciar nessa área.

### **1.3 Metodologia**

A primeira etapa traz uma revisão dos princípios básicos da mecânica quântica que são fundamentais para computação quântica, será apresentado no capítulo 2.

Introdução ao conceito da computação quântica e seus principais fundamentos de forma bem explicativa e de fácil entendimento, e isso será feito no capítulo 3.

Desenvolvimento da apresentação dinâmica com auxílio de ferramentas de computação gráfica, que se encontra no Capítulo 4.

## **2. MECÂNICA QUÂNTICA**

A Mecânica Quântica é umas das teorias da física mais bem estabelecida atualmente e curiosamente a mais misteriosa, ela trata de descrever o comportamento das partículas nas menores escalas de tempo, energia, e tamanho (Junior, Junior, & Bromberg, 2011).

Foi desenvolvida durante o período de 1900 a 1920, os físicos tiveram grande sucesso na aplicação da mecânica quântica para entender uma gama surpreendente de fenômenos em nosso mundo.

Mas, embora esses desenvolvimentos tenham avançado a nossa compreensão do mundo natural, a compreensão em relação a mecânica quântica ainda era pouca. Isso começou a mudar nas décadas de 1970 e 1980, quando alguns pioneiros foram inspirados a perguntar se algumas das questões fundamentais da ciência da computação e da teoria da informação poderiam ser aplicadas ao estudo de sistemas quânticos. Ao em vez de olharem para os sistemas quânticos puramente como fenômenos a serem explicados como encontrados na natureza, eles os encaravam como sistemas que podem ser projetados. O mundo quântico deixou de ser considerado apenas como apresentado, mas podendo ser criado. Isso resultou em uma nova perspectiva que inspirou um ressurgimento do interesse nos fundamentos

da mecânica quântica e também muitas novas questões combinando física, ciência da computação e teoria da informação (Nielsen & Chuang, 2010).

## **2.1. Definição de mecânica quântica**

A mecânica quântica é uma estrutura matemática ou um conjunto de regras para a construção de teorias físicas. Por exemplo, existe uma teoria física conhecida como eletrodinâmica quântica que descreve com precisão a interação de átomos e luz. A eletrodinâmica quântica é construída dentro da estrutura da mecânica quântica, mas contém regras específicas não determinadas pela mecânica quântica. O relacionamento da mecânica quântica com teorias físicas específicas, como a eletrodinâmica quântica, é semelhante ao relacionamento do sistema operacional de um computador com software de aplicativos específico - o sistema operacional define certos parâmetros e modos básicos de operação, mas deixa em aberto como tarefas específicas são executadas pelos aplicativos. As regras da mecânica quântica são simples, mas mesmo os especialistas as acham contra intuitivas (Nielsen & Chuang, 2010).

Desde então, os físicos lutam com a mecânica quântica em um esforço para tornar suas previsões mais palpáveis. Um dos objetivos da computação quântica e da informação quântica é desenvolver ferramentas que aprimorem a intuição sobre a mecânica quântica e tornem suas previsões mais transparentes para as mentes humanas.

Conhecer os conceitos básicos da Mecânica Quântica é fundamental para entendimento da Computação Quântica, Alguns desses conceitos serão mostrados a seguir.

### **2.1.1. Dualidade onda partícula**

No começo do século 19, o experimento dupla-fenda de Thomas Young mostrou que havia fenômeno de interferência, ele indicou que a luz consistia de ondas.

Este fato foi crucial para que fosse aceito a teoria ondulatória da luz, pois durante os séculos 17 e 18 a teoria que estava em vigor para a luz era a teoria corpuscular proposta por Newton. No início do século 20, as descobertas dos efeitos, fotoelétrico e Compton mostrando que em diferentes condições a luz pode comportar-se como partículas discretas. Estes resultados aparentemente contraditórios tornou necessário levar-se em conta a natureza quântica da luz (Machado ).

### **2.1.2. Superposição de estados.**

A superposição é uma situação na qual um sistema quântico pode se encontrar. Uma partícula pode ter uma energia alta ou pode ter uma energia baixa ou pode ter energia alta e baixa ao mesmo tempo, se uma partícula está no estado de superposição ela não tem suas propriedades bem definidas, isso quer dizer que não tem como saber qual é exatamente a energia de uma partícula em superposição, o que existe são possibilidades que podem ser medidas em algum experimento, cada uma dessas possibilidades tem uma probabilidade diferente de ser medidas quando realizamos um experimento, isso significa que nenhuma dessas possibilidades já estava determinada antes do experimento a partícula realmente estava em um estado de superposição a sua energia era todas as possibilidades ao mesmo tempo. (Instituto de Pesquisas Científicas)

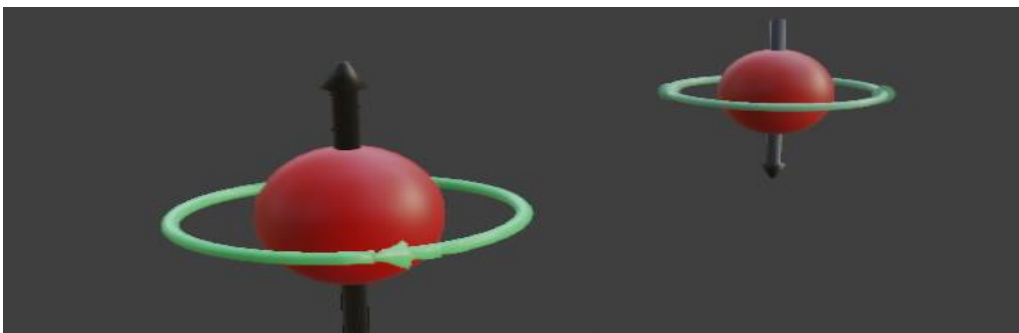
A superposição não é uma incerteza ou um desconhecimento de nossa parte acerca das propriedades de um sistema, a incerteza na superposição faz parte da teoria da física quântica em que vimos no texto a cima, a superposição é fundamental e não uma forma de erro experimental, ou seja, só é possível medir a energia de uma partícula em superposição quando medimos manualmente a energia daquela partícula, antes disso todos os valores de energia eram possíveis ao mesmo tempo .

O sistema mais simples que possuem propriedades quânticas interessantes é o exemplo de uma partícula sozinha ela possui apenas uma propriedade interessante que pode assumir dois valores, em um elétron essa propriedade é conhecida como Spin (O SPIN QUE MOVE O MUNDO, 2010), uma espécie de campo magnético, o spin do elétron. pode ser descrito usando apenas dois valores que podem ser representados por uma seta para cima ou para baixo o que é mais importante nesse exemplo é que nesse estado de superposição, o spin não está com metade apontando para cima e outra metade apontando para baixo, o spin está indeterminado, é impossível de atribuir um valor correto para direção do spin do elétron quando ele está em superposição, não tem com saber se está para cima ou se está para baixo até onde se sabe ele esta nos dois.

Se fizermos um experimento para determinar o estado do elétron temos uma probabilidade de medir o spin para cima ou medir para baixo, não conseguimos observar a superposição diretamente, é como se toda vez que olharmos para um elétron ele escolhesse automaticamente um spin para cima ou para baixo, é impossível ver diretamente esse estado de superposição (Moreira & Victoria)

### 2.1.3. Emaranhamento de estados quânticos

Figura 1- Spin do elétron.



Fonte: Autoria Própria: criada no software Blender 2.8

Existe vários estados possíveis para o sistema, o elétron da esquerda pode ter spin para cima ou para baixo e a mesma coisa vale para o elétron da direita, só que existe uma lenda na natureza chamada de Princípio da exclusão de Pauli que diz que dois elétrons não podem ter o número quântico igual e o spin é um número quântico, isso significa que se o elétron da esquerda estiver com o spin para cima o elétron da direita obrigatoriamente precisa ter o spin para baixo (Porto Editora). Vamos pegar o primeiro elétron e medir o seu spin que até o momento da medição estava em superposição, ou seja, para cima e para baixo, se medirmos o spin e estiver apontado para baixo o spin do segundo tem que está para cima. Isso é o emaranhamento quântico, essa aparente ligação entre dois elétrons que obriga que o spin de um seja diferente do outro, se obtermos informações de metade dos componentes do sistema, saberíamos de toda a informação, ou seja, um emaranhamento quântico é quando você não consegue descrever uma partícula independentemente de outra partícula, uma depende da outra, se o spin de uma é para cima o spin da outra obrigatoriamente deve ser para baixo e vice-versa e por consequência fazer uma medida em uma parte do sistema revela informações sobre o resto do sistema .

Vamos imaginar dois elétrons emaranhados e deixa-los separados por uma distancia extremamente grande, um ficara em Limeira e o outro na lua, ambos os elétrons tem seus spins em superposição, então fazemos uma medida no elétron em Limeira e descobrimos que seu spin aponta para cima, obrigatoriamente o da Lua aponta para baixo no exato instante.

Parece que de alguma forma os elétrons estão se comunicando instantaneamente para decidir que spin vai ter, violando o limite da velocidade da luz, temos experiências que provam que isso de certa forma está correto o problema é que esse efeito de comunicação instantaneamente entre os elétron independente da distância, Einstein acreditava que a física quântica estava correta inclusive ele era um dos defensores da física quântica, mas como a informação em emaranhamento quântico aparentemente viaja mais rápida que a velocidade da luz Einstein achava que a física quântica não estava completa ele inclusive nomeou esse efeito como ação fantasmagórica a distância deveria existir alguma teoria que explicasse o mecanismo pelo qual os elétrons se

comunicam, mais pelo nosso entendimento atual da natureza quântica não existe um mecanismo ou uma forma dos elétrons se comunicarem na verdade esse comportamento esquisito do emaranhamento quântico é simplesmente uma parte fundamental da teoria quântica, mas como nós resolvemos esse problema a informações de dois elétron emaranhados realmente viaja mais rápido do que a luz?

A forma certa de pensar sobre essa questão é tratar como um único sistema uma coisa só, o que acontece e que os estados finais ficam dependendo um do outro e existem duas situações possíveis para esse sistema, ou seja, se nós medimos o spin do primeiro elétron nos automaticamente descobrimos o spin do segundo elétron e nem precisamos olha, a gente já sabe o que é.

Mas não é como se estive uma partícula fantasmagórica voando entre os dois elétrons para o primeiro dizer para o segundo qual tem que ser o spin dele é simplesmente o único que sobrou dos dois possíveis. A informação não se move mais rápido que a luz porque simplesmente não existe informação nova ela já estava ali, em estado de superposição (Ação fantasmagórica à distância é 10.000 vezes mais rápida que a luz., 2013). Concluimos que é impossível termos informação mais rápida que a velocidade da luz, pois precisa se de uma informação previa para isso.

### **3. COMPUTAÇÃO QUÂNTICA**

A ciência da computação foi anunciada pelo grande matemático Alan. Turing que desenvolveu uma noção abstrata do que chamaríamos agora de um computador programável, a ciência da computação tem evoluído de forma surpreendente a cada década com computadores cada vez mais potentes (F. & Son, 1936).

No entanto as abordagens convencionais para a fabricação de tecnologia de computadores estão começando a enfrentar dificuldades



fundamentais de tamanho. Os efeitos quânticos estão começando a interferir no funcionamento dos dispositivos eletrônicos à medida que se tornam cada vez menores. Uma solução possível para o problema é mudar para um paradigma de computação diferente. Um desses paradigmas é fornecido pela teoria da computação quântica, que se baseia na ideia de usar a mecânica quântica para realizar cálculos, em vez da física clássica. Embora um computador comum possa ser usado para simular um computador quântico, parece impossível que as perspectivas globais realizem a simulação de maneira eficiente. Assim, os computadores quânticos oferecem uma vantagem essencial de velocidade em relação aos computadores clássicos. Essa vantagem de velocidade é tão significativa que muitos pesquisadores acreditam que nenhuma quantidade concebível de progresso na computação clássica seria capaz de superar a potência de um computador quântico. A promessa dos computadores quânticos é que certas tarefas computacionais poderão ser executadas exponencialmente mais rapidamente em um processador quântico do que em um processador clássico .

### **3.1. Simulações "eficientes" versus "ineficientes"**

Em particular, a ideia de algoritmos eficientes e ineficientes foi tornada matematicamente precisa pelo campo da complexidade computacional. Grosso modo, um algoritmo eficiente é aquele que roda em tempo polinomial no tamanho do problema resolvido. Por outro lado, um algoritmo ineficiente requer tempo superpolinomial (geralmente exponencial) ( FREEDMAN, 1998). Nos anos desde Turing, muitas equipes de pesquisadores notaram que certos tipos de computadores analógicos podem resolver com eficiência problemas que, acredita-se, não têm solução eficiente em uma máquina de Turing. Infelizmente para o cálculo analógico, verifica-se que, quando são feitas suposições realistas sobre a presença de ruído em computadores analógicos, seu poder desaparece em todos os casos conhecidos; eles não conseguem resolver com eficiência problemas que não podem ser solucionados com eficiência em uma máquina de Turing. Esta lição - que os efeitos do ruído realista devem ser levados em consideração na avaliação da eficiência de um modelo

computacional - foi um dos grandes desafios iniciais da computação quântica e da informação quântica, um desafio enfrentado com sucesso pelo desenvolvimento de uma teoria do erro quântico códigos de correção e computação quântica tolerante a falhas. Assim, diferentemente da computação analógica, a computação quântica pode, em princípio, tolerar uma quantidade finita de ruído e ainda manter suas vantagens computacionais.

### 3.2. Bit Quântico

O bit é o conceito fundamental da computação clássica e da informação clássica. A computação quântica e a informação quântica são construídas sobre um conceito análogo, o bit quântico ou qubit, para abreviar. Assim como um bit clássico tem um estado 0 ou 1, um qubit também tem um estado. Dois estados possíveis para um qubit são os estados:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

A notação como ' $|\rangle$ ' é chamada de notação Dirac, e é a notação padrão para estados em mecânica quântica. A diferença entre bits e qubits é que um qubit pode estar em um estado diferente de  $|0\rangle$  ou  $|1\rangle$ . Também é possível formar combinações lineares de estados, geralmente chamadas de superposições:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Os números  $\alpha$  e  $\beta$  são números complexos, o estado de um qubit é um vetor em um espaço vetorial complexo bidimensional. Os estados especiais  $|0\rangle$  e  $|1\rangle$  são conhecidos como estados de base computacional e formam uma base ortonormal para esse espaço vetorial. Podemos examinar um pouco para

determinar se está no estado 0 ou 1. Por exemplo, os computadores fazem isso o tempo todo quando recuperam o conteúdo de sua memória. Surpreendentemente, não podemos examinar um qubit para determinar seu estado quântico, ou seja, os valores de  $\alpha$  e  $\beta$ . Em vez disso, a mecânica quântica nos diz que só podemos adquirir informações muito mais restritas sobre o estado quântico. Quando medimos um qubit, obtemos o resultado 0, com probabilidade  $|\alpha|^2$ , ou o resultado 1, com probabilidade  $|\beta|^2$ . Naturalmente,  $|\alpha|^2 + |\beta|^2 = 1$ , pois as probabilidades devem ter somatória um.

Geometricamente, podemos interpretar isso como a condição de normalização do estado do qubit para o comprimento um. Assim, em geral, o estado de um qubit é um vetor unitário em um espaço vetorial complexo bidimensional. Na maioria dos nossos modelos abstratos do mundo, há uma correspondência direta entre elementos da abstração e o mundo real assim como os planos de um arquiteto para um edifício está em correspondência com o edifício final.

A falta dessa correspondência direta na mecânica quântica dificulta a intuição do comportamento dos sistemas quânticos; no entanto, existe uma correspondência indireta, pois os estados de qubit podem ser manipulados e transformados de maneiras que levam a resultados de medição que dependem distintamente das diferentes propriedades do estado.

Assim, esses estados quânticos têm consequências reais, experimentalmente verificáveis, que veremos serem essenciais para o poder da computação quântica e da informação quântica. A capacidade de um qubit estar em um estado de superposição contraria nossa compreensão do "senso comum" do mundo físico ao nosso redor. Uma parte clássica é como uma moeda: cara ou coroa. Por outro lado, um qubit pode existir em um continuum de estados entre  $|0\rangle$  e  $|1\rangle$  - até que seja observado. Vamos enfatizar novamente que, quando um qubit é medido, ele apenas fornece '0' ou '1' como resultado da medição - probabilisticamente. Por exemplo, um qubit pode estar no estado

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

Que, quando medido, fornece o resultado 0 cinquenta por cento ( $|1 / \sqrt{2}|^2$ ) do tempo, e o resultado 1 cinquenta por cento do tempo. Voltaremos frequentemente a esse estado, que às vezes é denotado  $|+\rangle$ . Apesar dessa estranheza, os qubits são reais, sua existência e comportamento são amplamente validados por experimentos, e muitos sistemas físicos diferentes podem ser usados para realizar qubits.

Para ter uma idéia concreta de como um qubit pode ser realizado, pode ser útil listar algumas das maneiras pelas quais essa realização pode ocorrer: como as duas polarizações diferentes de um fóton; como o alinhamento de um spin nuclear em um campo magnético uniforme; como dois estados de um elétron orbitando um único átomo. No modelo de átomo, o elétron pode existir nos chamados estados de 'terra' ou 'excitados', que chamaremos de  $|0\rangle$  e  $|1\rangle$ , respectivamente. Ao iluminar o átomo, com energia apropriada e por um período de tempo apropriado, é possível mover o elétron do estado  $|0\rangle$  para o estado  $|1\rangle$  e vice-versa. Mas o mais interessante é que, ao reduzir o tempo em que iluminamos a luz, um elétron inicialmente no estado  $|0\rangle$  pode ser movido 'no meio do caminho' entre  $|0\rangle$  e  $|1\rangle$ , para o estado  $|+\rangle$ .

Quanta informação é representada por um qubit? Paradoxalmente, há um número infinito de pontos na esfera unitária, de modo que, em princípio, é possível armazenar um valor muito grande na infinita expansão binária de  $\theta$ . No entanto, essa conclusão acaba sendo enganosa, devido ao comportamento de um qubit quando observado. Lembre-se de que a medição de um qubit fornecerá apenas 0 ou 1. Além disso, a medição altera o estado de um qubit, reduzindo-o da superposição de  $|0\rangle$  e  $|1\rangle$  para o estado específico consistente com o resultado da medição. Por exemplo, se a medição de  $|+\rangle$  der 0, o estado de pós-medição do qubit será  $|0\rangle$ . Por que esse tipo de colapso ocorre? Ninguém sabe. Como discutido no capítulo 1, esse comportamento é simplesmente um dos postulados fundamentais da mecânica quântica. O que é relevante para nossos propósitos é que, a partir de uma

única medição, obtém-se apenas um único bit de informação sobre o estado do qubit, resolvendo o aparente paradoxo. Acontece que somente se fossem medidos infinitamente muitos qubits preparados de forma idêntica, seria possível determinar  $\alpha$  e  $\beta$  para um qubit no estado dado na Equação.

### 3.3. Portas de um qubit único

Na computação quântica e, especificamente, no modelo de computação quântica, uma porta lógica quântica é um circuito quântico básico que opera em um pequeno número de qubits. Elas são os blocos de construção de circuitos quânticos, como portas lógicas clássicas são para circuitos digitais convencionais. Ao contrário de muitas portas lógicas clássicas, as portas lógicas quânticas são reversíveis.

### 3.4. Porta Hadamard

A porta Hadamard, ou porta H, aparece em toda parte na computação quântica e por boas razões. A Hadamard tem a capacidade quântica caracteristicamente de transformar um estado quântico definido, como spin-up, em um obscuro, como uma superposição de spin-up e spin-down ao mesmo tempo.

Essa porta atua em um único qubit, mapeando o estado inicial  $|0\rangle$  para  $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$  e  $|1\rangle$  para  $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ . Quando medido terá probabilidade igual de se tornar 1 ou 0, criando uma superposição, e pode ser representado pela matriz de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

### 3.5. Porta Pauli-X

É equivalente á porta lógica clássica NOT, e seu papel é simplesmente mapear o estado inicial  $|0\rangle$  para  $|1\rangle$  e vice versa, é representada pela matriz de Pauli:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

### 3.6. Porta Pauli-Z

Mantém o estado inicial  $|0\rangle$  inalterado e mapeia  $|1\rangle$  para  $-|1\rangle$ . É representada pela matriz de Pauli

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

### 3.7. Porta ( $\sqrt{NOT}$ )

É a raiz quadrada da porta NOT. É representada pela matriz

$$\sqrt{NOT} = \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \quad \sqrt{NOT}\sqrt{NOT} = NOT$$

### 3.8. Circuitos quânticos

Os algoritmos quânticos são mais comumente descritos por um circuito quântico. Um circuito quântico é um modelo para computação quântica, onde as etapas para resolver o problema são portas quânticas executadas em um ou mais qubits. Uma porta quântica é uma operação aplicada a um qubit que altera o estado quântico do qubit. As portas quânticas podem ser divididas em portas de um qubit e portas de dois qubit, dependendo do número de qubits nos quais são aplicados ao mesmo tempo. Também podem ser definidas portas de três qubit e outras portas de múltiplos qubit. Um circuito quântico é concluído com uma medição em um ou mais qubits.

Uma diferença com um algoritmo clássico é que um algoritmo quântico é sempre reversível. Isso significa que, se as medições não forem feitas, podemos desfazer as operações desse circuito.

### **3.9. O que da pra fazer com algoritmos quânticos?**

Problemas que são fundamentalmente insolúveis por algoritmos clássicos (chamados problemas indecidíveis) também não podem ser resolvidos por algoritmos quânticos. O valor agregado dos algoritmos quânticos é que eles podem resolver alguns problemas significativamente mais rapidamente que os algoritmos clássicos. Os exemplos mais conhecidos são o algoritmo de Shor e o algoritmo de Grover. O algoritmo de Shor é um algoritmo quântico para fatoração de número inteiro. Simplificando, ao receber um número inteiro  $N$ , ele encontrará seus principais fatores. Ele pode resolver esse problema exponencialmente mais rápido que o algoritmo clássico mais conhecido. O algoritmo de Grover pode pesquisar um banco de dados não estruturado ou lista não ordenada quadraticamente mais rápido que o melhor algoritmo clássico com esse objetivo.

## **4. MODELO DE APRESENTAÇÃO DINAMICA**

A apresentação dinâmica traz uma facilidade no entendimento e tem o objetivo de explicar o complicado de uma forma mais simples e clara.

Construída basicamente com objetos em três dimensões fazendo uma analogia ao mundo real, com a vantagem de possuir animações e efeitos gráficos.

Dessa forma o trabalho de modelagem é eficaz na explicação de qualquer outra área sendo, neste caso utilizado para facilitar o desempenho no processo de aprendizagem da computação quântica. Neste trabalho foi utilizado o software Blender para modelagem dos objetos e cenário, e o software Unity para construir a lógica da animação.

Não entrarei em muitos detalhes sobre as ferramentas pois esse não é o objetivo deste trabalho de conclusão de curso.

### **4.1. Enredo**

O cenário é parecido com um anfiteatro e conta com um projetor, uma representação de um computador quântico e outros.

**Figura 2 Cenário**



**Fonte: Autoria própria – Produzido no Software Blender**

A proposta de apresentação é bem similar ao um jogo eletrônico, mas com outro propósito.

Desta forma é possível ter um controle maior e trabalhar de forma mais abstrata possibilitando criar analogias mais simples que facilitaram o entendimento do público.



## **CONCLUSÃO**

Resumindo todas as pesquisas, eu concluo que a teoria quântica é uma teoria bastante extensa, contra intuitiva, até mesmo para os especialistas e ao longo dos séculos muitos físicos dedicaram suas vidas com o objetivo de torná-la mais transparente e compreensível ao entendimento humano.

A partir do momento em que a toda essa teoria começou a se juntar com a Ciência da Computação e a teoria da informação, a mecânica quântica começou a ganhar outro propósito que até então utilizávamos para descrever fenômenos naturais, passo a poder criar.

Com o fim da lei de Moore e a dificuldade em projetar hardware mais potentes devido ao tamanho microscópico dos componentes, a computação quântica é uma forte aliada para essa questão, com isso deixo aqui a minha contribuição para iniciantes que queiram conhecer a área de uma forma descomplicada para ingresso nesse fantástico mundo quântico

## Referências

- FREEDMAN, M. H. (1998). P/ NP, and the quantum field computer. *Proc. Natl. Acad. Sci. USA*, 98–101.
- Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. New York: CAMBRIDGE UNIVERSITY PRESS.
- Ação fantasmagórica à distância é 10.000 vezes mais rápida que a luz.* (02 de 04 de 2013). Acesso em 05 de 10 de 2019, disponível em INOVAÇÃO TECNOLÓGICA: [www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=acao-fantasmagorica-distancia-mais-rapida-luz](http://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=acao-fantasmagorica-distancia-mais-rapida-luz)
- Blender 2.80 Manual.* (s.d.). Acesso em 12 de 11 de 2019, disponível em Blender: [https://docs.blender.org/manual/pt/2.80/getting\\_started/about/introduction.html](https://docs.blender.org/manual/pt/2.80/getting_started/about/introduction.html)
- Cuffaro, A. H. (2015). Quantum computing. *Stanford Encyclopedia of Philosophy*.
- F., H., & Son. (1936). *Allan Turing, On computable numbers with an application to the entscheidungsproblem.*
- Instituto de Pesquisas Científicas.* (s.d.). Acesso em 14 de 11 de 2019, disponível em Conceitos: Mecânica quântica, emaranhamento e superposição: <https://institutodepesquisascientificas.wordpress.com/2016/04/14/conceitos-mecanica-quantica-emaranhamento-e-superposicao/>
- Junior, O. F., Junior, O. P., & Bromberg, J. L. (2011). *Teoria Quântica: estudos históricos e implicações culturais*. Campina Grande-PB / São Paulo-SP: Eduepd.
- Machado, P. (s.d.). *Experiência da dupla fenda.* Acesso em 17 de 11 de 2019, disponível em CREF: <https://www.if.ufrgs.br/novocref/?contact-pergunta=experiencia-da-dupla-fenda>
- Moreira, M. A., & V. E. (s.d.). *Revista Brasileira de Ensino de Física.* Acesso em 12 de 11 de 2019, disponível em Scielo: [http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1806-11172001000400010](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1806-11172001000400010)
- O SPIN QUE MOVE O MUNDO.* (19 de 11 de 2010). Acesso em 20 de 10 de 2019, disponível em Ciencia Hoje: <http://cienciahoje.org.br/coluna/o-spin-que-move-o-mundo/>
- Porto Editora, 2.-2. (s.d.). *princípio de exclusão de Pauli.* Acesso em 10 de 08 de 2019, disponível em Artigos de apoio Infopédia: [https://www.infopedia.pt/apoio/artigos/\\$princípio-de-exclusao-de-pauli](https://www.infopedia.pt/apoio/artigos/$princípio-de-exclusao-de-pauli)

