UNIVERSIDADE ESTADUAL PAULISTA

"JÚLIO DE MESQUITA FILHO"

Instituto de Geociências e Ciências Exatas – IGCE

Curso de Bacharelado em Ciências da Computação

CAROLINA MIDORI OKAMOTO

TEORIA QUÂNTICA DA COMPUTAÇÃO

Trabalho realizado sob orientação do Prof. Dr. Eraldo Pereira Marinho, DEMAC/IGCE

Período: 07.05.2015 a 25.01.2016

Rio Claro – SP

2015

TEORIA QUÂNTICA DA COMPUTAÇÃO

Trabalho de Conclusão do Curso, modalidade Trabalho de Graduação, apresentado, no 2º semestre de 2015, à disciplina ES/TG do Curso de Bacharelado em Ciências da Computação, período Integral, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", campus de Rio Claro, para apreciação segundo as normas estabelecidas pelo Conselho do Curso, em 27.11.2007.

Aluno: Carolina Midori Okamoto

Orientador: Prof. Dr. Eraldo Pereira Marinho

DEMAC/IGCE

Rio Claro-SP

2015

004 Okamoto, Carolina
O41t Teoria quântica da computação / Carolina Okamoto. - Rio Claro, 2015
54 f. : il., figs., tabs.

Trabalho de conclusão de curso (Bacharelado em Ciências da Computação) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas
Orientador: Eraldo Pereira Marinho

1. Computação 2. Computação quântica. 3. Máquina de Turing Quântica. 4. Teoria da Computação. I. Título.

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

AGRADECIMENTO

É muito difícil expressar em poucas palavras o quão importante foram as pessoas que me ajudaram a concluir mais essa etapa, mas, por mais simbólico que seja este agradecimento, não posso deixar de fazê-lo.

Primeiramente, agradeço e dedico este trabalho aos meus pais e a toda a minha família. Eles não só me deram a base para o que sou hoje, como me suportaram e apoiaram em todas as minhas escolhas.

Em segundo, gostaria de transmitir meu imenso agradecimento ao meu orientador, Prof. Dr. Eraldo Marinho Pereira, por acreditar que as pessoas podem ir além do que elas imaginam, e por me incentivar a ser uma dessas pessoas. Agradeço pelos ensinamentos (e foram muitos), e por estar sempre disponível para quando precisei. Obrigada por me apresentar o tema aqui exposto nesta monografia de forma tão entusiasmada, e por me passar um pouquinho do seu enorme conhecimento.

Agradeço aos amigos e ao meu namorado, que direta ou indiretamente participaram da minha formação. Ainda enfrentarão ao meu lado muitos outros desafios.

Por fim, mas não menos importante, aos meus professores de graduação, por se dedicarem a uma profissão tão nobre como essa, e aos meus colegas de trabalho, que demonstraram paciência e carinho dia após dia neste momento tão significativo.

Muito obrigada!

RESUMO

Esta tese de graduação tem como objetivo principal definir formalmente aspectos de uma Máquina de Turing Quântica utilizando como base autômatos finitos quânticos. Introduziremos os conceitos básicos de mecânica quântica e computação quântica através de princípios como superposição, emaranhamento de estados quânticos, bits quânticos e algoritmos. Demonstraremos o teorema do teletransporte de Bell, enunciado na forma da definição de Deutsch-Jozsa para algoritmos quânticos. A maneira global como o texto foi escrito omite aspectos formais de mecânica quântica, encorajando os cientistas da computação a entender o cenário da computação quântica. Concluiremos nossa tese listando as principais limitações de uma Máquina de Turing Quântica frente à bem conhecida Máquina de Turing Clássica.

Palavras-chave: Computação Quântica. Máquina de Turing Quântica. Teoria da Computação.

ABSTRACT

This undergraduate thesis aims formally define aspects of Quantum Turing Machine using as a basis quantum finite automata. We introduce the basic concepts of quantum mechanics and quantum computing through principles such as superposition, entanglement of quantum states, quantum bits and algorithms. We demonstrate the Bell's teleportation theorem, enunciated in the form of Deutsch-Jozsa definition for quantum algorithms. The way as the overall text were written omits formal aspects of quantum mechanics, encouraging computer scientists to understand the framework of quantum computation. We conclude our thesis by listing the Quantum Turing Machine's main limitations regarding the well-known Classical Turing Machines.

Keywords: Quantum Computing. Quantum Turing Machine. Theory of computation.

LISTA DE FIGURAS

Página

LISTA DE TABELAS

Página

Sumário

Página

1 INTRODUÇÃO

Qual o futuro da computação quântica e o que ela pode oferecer para a ciência, tecnologia e humanidade em geral? Quais benefícios a computação quântica tem em relação aos computadores clássicos? Quais são as limitações de um computador quântico? Exploraremos todas estas questões com o intuito de demonstrar o potencial da computação quântica e instigar o pensamento sobre o que estas máquinas podem mudar no cotidiano de todos no futuro.

A computação quântica teve início provavelmente em 1981, quando o físico Richard Feynman (FEYNMAN, 1981) criou a primeira proposta para utilizar as propriedades quânticas em programas de computador. Quatro anos depois, o também físico David Deutsch (DEUTSCH, 1985) descreveu o primeiro computador quântico universal, que se aplicava às limitações da mecânica quântica. Em 1994, o matemático Peter Shor (SHOR, 1994) desenvolveu o primeiro algoritmo puramente quântico, o Algoritmo de Shor, para resolução da fatoração de números primos. Em 1999, o primeiro protótipo de um computador quântico real foi desenvolvido no Instituto de Tecnologia de Massachusetts (MIT) e, em 2007, a empresa D-Wave afirmou ter construído o primeiro processador quântico, o Orion. Recentemente, a Google e a NASA, através do laboratório Quantum Artificial Inteligence Lab, anunciaram investimentos em um processador quântico, o D-Wave 2X, com mais de mil bits quânticos.

Durante todos esses anos, diversas pesquisas na área foram realizadas até se chegar no atual cenário. Uma grande motivação para isto é o fato de o computador quântico utilizar propriedades da mecânica quântica, tais como sobreposição e emaranhamento quântico. Se bem aplicadas, podem gerar uma redução exponencial no tempo para solucionar problemas que, no caso clássico, seriam impraticáveis. Exemplo disto é a fatoração de números primos (como mencionado anteriormente) ou até mesmo a quebra de criptografias.

Ao mesmo tempo que estas propriedades tornam um computador quântico vantajoso em relação ao modelo clássico, elas também viraram um empecilho para estudiosos da área. A mecânica quântica trabalha no universo atômico que, além de muito sensível a qualquer micro ruído eletromagnético, pode causar superaquecimento nas máquinas.

Para entendermos o estado da arte da computação quântica, devemos voltar no tempo e explorar os principais campos que contribuíram para o desenvolvimento dessa nova ciência,

que são, essencialmente, a mecânica quântica e seu formalismo matemático, baseado em operações e transformações sobre vetores no espaço de Hilbert.

Presumimos que o leitor possui algum conhecimento sobre teoria da computação e, em particular, com a definição formal de algoritmos, usualmente referida como Hipótese de Church e Tese de Turing.

Este trabalho tem como intuito apresentar a teoria quântica da computação, como um novo ramo da teoria da computação e complexidade de algoritmos, buscando uma forma simples, sem maiores aprofundamentos nos detalhes teóricos e experimentais da mecânica quântica, todavia mantendo o formalismo matemático adotado nos textos de linguagens formais e autômatos e análise e projeto de algoritmos.

O presente trabalho é estruturado como segue nos seguintes parágrafos.

No Capítulo 2, apresentamos os postulados da mecânica quântica, na forma conhecida como formalismo de Dirac e von Neumann (1932), onde passamos ao leitor a ideia de que as primitivas de computação quântica se baseiam no princípio de superposição de estados quânticos, mesmo que mutualmente excludentes, no produto tensor entre estados quânticos, o que está intimamente ligado ao conceito de emaranhamento quântico, e os automorfismos no espaço de Hilbert, que estão ligados ao conceito de medida/observação.

No Capítulo 3, apresentamos os conceitos fundamentais da computação quântica, baseados na teoria explicada no capítulo 2. Estas noções são apresentadas em ordem crescente de complexidade, começando da ideia de bit quântico e portas quânticas, até chegarmos no conceito de algoritmo quântico, introduzido por Deutsch (1985) e, posteriormente, numa forma mais elegante, por Deutsch e Jozsa (1992). Assim, situamos o leitor sobre os conceitos de algoritmos quânticos, que dão base para a idealização de autômatos quânticos e sua forma mais generalizada, as máquinas de Turing quânticas, que serão discutidas no Capítulo 4.

No Capítulo 5, concluiremos o trabalho reforçando a importância dos avanços que os cientistas quanto-computacionais têm obtido sobre o assunto até o momento e elencando algumas limitações de não termos um computador operacional totalmente quântico.

2 NOÇÕES DE MECÂNICA QUÂNTICA

Neste capítulo, faremos uma breve introdução a mecânica quântica. Muito do formalismo será omitido, uma vez que nosso trabalho é voltado para alguns aspectos que permitem a construção de um modelo de computação baseado nas propriedades de superposição e emaranhamento quânticos.

A mecânica clássica aborda de forma determinística o conceito de partícula, também chamada ponto material. Sua descrição clássica do movimento requer um conjunto de equações diferenciais de segunda ordem, conhecidas como segunda lei de Newton ou, de forma mais elegante, as equações de Lagrange (ARNOLD, 1987). As soluções das equações da mecânica clássica são curvas (trajetórias), unicamente determinadas pelas condições iniciais de posição e velocidade/ momentum, além da lei de interação entre essas partículas e a ação de um possível campo externo de forças.

Segundo a mecânica clássica, a posição exata de uma partícula pode ser prevista em qualquer ocasião (tempo), posterior às condições iniciais, ou mesmo recuar no tempo antes dessas condições. Pelo menos teoricamente, o espírito da mecânica clássica se estende à solução de um sistema de equações diferenciais para um número qualquer de partículas, sejam essas partículas as moléculas de um gás, os componentes planetários do sistema solar, as estrelas de uma galáxia, etc.

Contudo, tanto as moléculas de um gás quanto as estrelas de uma galáxia possuem uma população extremamente grande, o que torna inviável qualquer tentativa de se obter uma solução exata para um tal número de partículas.

Para sistemas complexos, compostos de um grande número de partículas, a melhor descrição é a estatística, que passa a ser assunto da mecânica estatística e dos processos estocásticos. Assim, o conceito de movimento é substituído pela evolução temporal das densidades de probabilidade, ao invés de se descrever individualmente a evolução de cada partícula. Ainda assim, essa estatística, denominada mecânica estatística clássica, tem como base as leis determinísticas da mecânica clássica.

Já no universo quântico, cuja evidência se dá em escalas atômicas e subatômicas, a forma de se descrever a dinâmica de átomos, elétrons, prótons, nêutrons e as demais partículas fundamentais, incluindo o fóton, não é determinística no sentido de previsão exata da posição e velocidade/momentum de uma partícula.

Diferentemente da mecânica clássica, a descrição do movimento de uma só partícula é inerentemente estocástica. Contudo, a descrição estatística de uma partícula no mundo quântico não é feita diretamente através de probabilidades, ou mesmo de densidades de probabilidade, que são valores reais não negativos. Ao invés, os eventos quânticos ocorrem ponderados por números complexos, denominados "amplitudes de probabilidade", cujos módulos ao quadrado são as probabilidades (ou densidades) de que esses eventos quânticos sejam observados.

Eventos quânticos são denominados "estados quânticos", geralmente associados à grandeza física esperada no processo de medida, e vinculado ao aparato de detecção quântica. Por exemplo, o fenômeno de difração de elétrons é evidenciado pela distribuição do ângulo de deflexão que cada partícula incidente sobre uma amostra cristalina emerge após colidir com os átomos do retículo do cristal. Tal distribuição revela um padrão ondulatório, muito similar ao fenômeno de difração da luz por uma rede de difração (TIPLER, 1995).

Em ambas as situações do exemplo acima, seja com fótons ou seja com elétrons, o feixe incidente é preparado de forma a tornar os participantes do experimento equivalentes (com uma reduzida margem de erros). Este raciocínio é o que dá a ideia de ensemble de sistemas quânticos (HUANG, 1987). Assim, o ideal é que os elétrons estejam colimados ou filtrados, de modo a terem aproximadamente o mesmo momentum linear ao incidir sobre a amostra. Os fótons devem estar associados a um feixe de luz coerente monocromática, como é o caso de um feixe laser.

Ainda no exemplo de difração de elétrons, a obtenção de um estado puro de momento linear, $\boldsymbol{p}$, para os elétrons incidentes, se chama preparação do sistema quântico para um estado puro $|\boldsymbol{p}\rangle$. Desse modo, qualquer elétron do feixe está com estado quântico $|\boldsymbol{p}\rangle$ e, portanto, é equivalente a qualquer outro elétron que esteja neste mesmo feixe.

2.1 Espaços de Hilbert e Estados Quânticos

A notação $|\psi\rangle$, precocemente utilizada na seção anterior, é denominada notação "ket", ou simplesmente vetor ket, introduzida por Paul Maurice Dirac (DIRAC, 1939), e representa um vetor do espaço de Hilbert. Denotamos daqui em diante os espaços de Hilbert com um H caligráfico, $\mathcal{H}$.

O formalismo moderno da mecânica quântica é conhecido como *axiomas de Dirac-von Neumann* (NEUMANN, 1932), publicado por John von Neumann em 1932 na obra intitulada

Mathematische Grundlagen der Quantenmechanik. Aliás, foi o próprio von Neumann quem percebeu que as entidades ket constituíam vetores em $\mathcal{H}$.

Por definição, espaços de Hilbert são espaços vetoriais complexos, que admitem distâncias definidas em termos da sequência de Cauchy (LIMA, 2013). Essa forma de definir distâncias é o que permite ter $\mathcal{H}$ com dimensionalidade infinita, inclusive ser gerado por uma base ortonormal não enumerável, o que é isomorfo ao espaço das funções ortogonais.

É definido em $\mathcal{H}$ um produto interno $\langle .,. \rangle: \mathcal{H} \times \mathcal{H} \mapsto \mathbb{C}$, que leva um par $(\boldsymbol{a}, \boldsymbol{b})$ de $\mathcal{H} \times \mathcal{H}$ em um escalar complexo $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$. Alternativamente, como apresentado nos textos de geometria analítica, o produto interno aparece como o operador "*dot*", $\cdot: \mathcal{H} \times \mathcal{H} \mapsto \mathbb{C}$, que leva um par $(\boldsymbol{a}, \boldsymbol{b})$ de $\mathcal{H} \times \mathcal{H}$ em um escalar complexo, $\boldsymbol{a} \cdot \boldsymbol{b}$.

É conhecido da álgebra linear que o produto interno nasce da forma linear, que é um vetor dual ou, equivalentemente, um vetor do espaço dual $\mathcal{H}^*$. Assim, na notação $\boldsymbol{a} \cdot \boldsymbol{b}$, o vetor $\boldsymbol{b}$ pertence a $\mathcal{H}$, enquanto $\boldsymbol{a} \cdot$, ou $\langle \boldsymbol{a}, . \rangle$, de $\mathcal{H}^*$, é o vetor dual de $\boldsymbol{a} \in \mathcal{H}$.

Segue imediatamente as seguintes propriedades do produto interno:

a) $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \langle \boldsymbol{a}, \boldsymbol{b} \rangle^*$;
b) $\langle \boldsymbol{a}, \alpha \boldsymbol{b} \rangle = \alpha \langle \boldsymbol{a}, \boldsymbol{b} \rangle$, enquanto $\langle \alpha \boldsymbol{a}, \boldsymbol{b} \rangle = \alpha^* \langle \boldsymbol{a}, \boldsymbol{b} \rangle$, com $\alpha \in \mathbb{C}$;
c) $\langle \boldsymbol{a} + \boldsymbol{b}, \boldsymbol{c} \rangle = \langle \boldsymbol{a}, \boldsymbol{c} \rangle + \langle \boldsymbol{b}, \boldsymbol{c} \rangle$ e $\langle \boldsymbol{a}, \boldsymbol{b} + \boldsymbol{c} \rangle = \langle \boldsymbol{a}, \boldsymbol{b} \rangle + \langle \boldsymbol{a}, \boldsymbol{c} \rangle$.

Na notação de Dirac, $\langle \boldsymbol{a}|$ é denominado "bra", que é a forma dual do ket $|\boldsymbol{a}\rangle$. Ainda nesta notação, o produto interno entre os estados quânticos $|\boldsymbol{a}\rangle$ e $|\boldsymbol{b}\rangle$ é denotado como $\langle \boldsymbol{a}|\boldsymbol{b} \rangle$, denominado "bracket", que é obtido através da concatenação entre os vetores $\langle \boldsymbol{a}|$ e $|\boldsymbol{b}\rangle$.

Sendo $|\psi\rangle$ o estado de um sistema quântico ψ, a amplitude de probabilidade de se observar ψ em um estado particular $|a\rangle$ é dada pelo bracket $\langle a|\psi \rangle$. A probabilidade de se encontrar o estado quântico $|\psi\rangle$ no estado $|a\rangle$ é igual ao quadrado do módulo da amplitude: $|\langle a|\psi \rangle|^2 = \langle \psi|a \rangle \langle a|\psi \rangle$.

A norma, $||\psi||$, de um estado quântico $|\psi\rangle$, é dada pelo bracket de ψ com o próprio ψ, $\big||\psi|\big| = \langle \psi|\psi \rangle$, que, segundo a interpretação do parágrafo anterior, é a probabilidade de que o sistema quântico ψ, conhecido a priori, seja ele mesmo quando observado. Portanto, se não há alteração desde a preparação do estado $|\psi\rangle$ até a sua constatação, tem-se $\langle \psi|\psi \rangle = 1$, que é conhecida como condição de normalização de um sistema quântico ψ.

2.1.1 Formulação contínua

O conjunto de estados puros associados a uma grandeza física, como o estado puro de posição, $|\boldsymbol{x}\rangle$, forma uma base do espaço de Hilbert. Assim, qualquer vetor de estado $|\psi\rangle$ pode ser continuamente decomposto na base dos estados quânticos, $|\boldsymbol{x}\rangle$, associados às medidas de posição, $\boldsymbol{x}$, sendo conhecida sua função de onda $\psi(\boldsymbol{x})$:

$$|\psi\rangle = \int dx^3\, \psi(\boldsymbol{x})|\boldsymbol{x}\rangle, \tag{1}$$

onde essa integral, de volume, se estende por todo o espaço euclidiano tridimensional. Observe que a dimensionalidade do espaço de Hilbert onde a combinação linear se aplica, é infinitamente não-enumerável.

Enfatizamos que a base de estados quânticos na formulação contínua, via Equação (1), é não enumerável. De fato, para todo estado quântico $|\boldsymbol{x}\rangle \in \mathcal{H}$, existe um número real positivo ε, arbitrariamente pequeno, e existe uma sequência infinita S_m ($m \in \mathbb{N}$) de estados quânticos, $S_m = \{|\boldsymbol{x}_{mn}\rangle, \forall n \in \mathbb{N}\}$, arbitrariamente escolhida, tal que $0 < ||\boldsymbol{x}\rangle - |\boldsymbol{x}_{mn}\rangle|^2 < \varepsilon$, sempre que n for arbitrariamente grande.

Como existem infinitas sequências de escalares reais positivos satisfazendo relações do tipo $\{||\boldsymbol{x}\rangle - |\boldsymbol{x}_{mn}\rangle|^2 < \varepsilon, \forall n \in \mathbb{N}\}$, e como não há racionalidade entre os possíveis ε e m, então não há como estabelecer uma bijeção entre as possíveis sequências infinitas, $\{S_m, \forall m \in \mathbb{N}\}$, de elementos da base e o conjunto dos números naturais $\mathbb{N}$. Portanto, tal sequência é não enumerável.

2.1.2 Formulação discreta

No caso da computação quântica, os sistemas são representações num espaço de Hilbert definidos com bases discretas, que podem ser conjuntos de estados quânticos ortonormais infinitamente enumeráveis.

Assim, o estado quântico do sistema pode ser escrito como:

$$|\psi\rangle = \sum_{j=-\infty}^{+\infty} \psi_j |j\rangle. \tag{2}$$

Se o espaço de Hilbert é finitamente gerado, por exemplo gerado pela base $\Gamma = \{|j\rangle, j = 0,1,\dots,N-1\}$, portanto $\dim \mathcal{H} = N$, então um sistema quântico tem seu estado $|\psi\rangle$ decomposto em:

$$|\psi\rangle = \sum_{j=0}^{N-1} \psi_j |j\rangle. \tag{3}$$

Uma escolha particularmente interessante, que será estudada com muito mais detalhe no Capítulo 3, é uma base ortonormal cujo número de componentes é potência inteira de 2: $N = 2^n$, com $n \in \mathbb{N}$.

2.2 Princípio de superposição de estados quânticos

Tanto na formulação contínua, Equação (1), quanto na formulação discreta, Equações (2) e (3), o sistema é decomposto em estados puros, que formam a base. Equivalentemente, o estado quântico, $|\psi\rangle$, é interpretado como uma superposição de estados mutuamente exclusivos, uma vez que o produto interno entre estados distintos da base é nulo.

Surge aqui um aparente paradoxo. Como um sistema pode estar simultaneamente em estados antagônicos? A resposta é: "enquanto não observado, o sistema ψ existe virtualmente em todas as suas possíveis situações, conforme suas respectivas amplitudes de probabilidade". Contudo, apenas um, e somente um, desses estados puros será detectado.

O princípio discutido no parágrafo acima é conhecido como *princípio de superposição de estados quânticos*, que é o primeiro postulado da mecânica quântica. É este princípio que garante a ocorrência de fenômenos de interferência, uma vez que certas combinações lineares podem atenuar, ou reforçar, a amplitude de probabilidade de se obter um dado estado.

O princípio de superposição vale para qualquer situação em que um estado quântico $|\psi\rangle$ pode ser decomposto em estados parciais, $|\psi\rangle = |\psi_A\rangle + |\psi_B\rangle$, como ocorre, por exemplo, com a superposição de situações tais como no experimento de interferência de dupla fenda, onde $|\psi_A\rangle$ é o estado quântico da partícula que trafega pela fenda A e $|\psi_B\rangle$ é o estado dessa mesma partícula passando pela fenda B.

A partícula do referido experimento de interferência, se fosse interpretada classicamente, passaria por uma das fendas, exclusivamente A ou exclusivamente B, conforme

o determinismo da mecânica clássica. Contudo, se considerarmos a situação real, o padrão de ocorrências de detecção da partícula ao longo de um anteparo, uma placa fotossensível por exemplo, se dá de forma ondulatória, com regiões mais prováveis intercaladas com regiões de sombra, como na **Figura 1.**

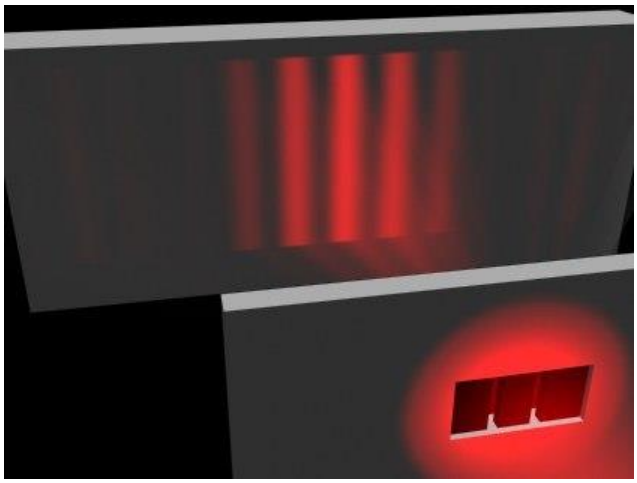

Figura 1 - Interferência de dupla fenda.
Fonte: https://antunesift.wordpress.com/2015/06/30/a-dupla-fenda/ Publicado em 30 de junho de 2015 por **Sérgio Antunes**, no Blog "**MultiFísica: Física sem Mistérios**"

Tal padrão torna-se evidente após um grande número de repetições do experimento, revelando assim uma distribuição de pontos de colisão mais densa nos modos normais, onde as amplitudes estão em fase, igualmente distanciados e intercalados por regiões de baixa densidade de colisões, onde as amplitudes estão em contra fase.

A explicação atual para tal fenômeno é que, enquanto a partícula não for observada, a sua distribuição de probabilidade de detecção sofre interferência de duas realidades potenciais superpostas, a da partícula que passa pela fenda A (a da esquerda na ilustração) e a da mesma partícula passando pela fenda B (à direita).

Essa potencial simetria é quebrada quando a partícula é observada. Por exemplo, se houvesse um detector na fenda A, todas as possíveis detecções ocorreriam no detector A ou chegariam livremente no anteparo, que obviamente só seria possível passando por B. Neste caso, não haveria o padrão ondulatório na distribuição de colisões da partícula com o anteparo, visto que, após atingir uma das fendas, a realidade (potencial) $|\psi_A\rangle$ é destruída no processo de detecção em A, enquanto $|\psi_B\rangle$ não sofrerá interferência de $|\psi_A\rangle$, uma vez que esse não pode existir após a passagem pela fenda.

Outro exemplo é o do gato de Schrödinger. Um hipotético gato, inicialmente vivo, encontra-se no estado inicial $|\psi_A\rangle$. Após essa constatação/preparação, o gato é trancafiado num cofre hermeticamente fechado cujo interior existe um dispositivo que tem 50% de chance de liberar um gás letal, matando o gato no interior do cofre, estado quântico $|\psi_B\rangle$, e 50% de chance de falhar, deixando o gato permanecer vivo, estado $|\psi_A\rangle$.

O cofre funciona como um dispositivo quântico, ou operador, que transforma o estado inicial $|\psi_0\rangle = |\psi_A\rangle$ no estado misto $|\psi\rangle = (|\psi_A\rangle + |\psi_B\rangle)/\sqrt{2}$. Como $|\psi_A\rangle$ e $|\psi_B\rangle$ são ortogonais, a probabilidade de encontrar o gato no estado $|\psi_A\rangle$, vivo, é obtida como veremos na Seção 2.3, tomando o quadrado do módulo do produto interno entre $|\psi_A\rangle$ e $|\psi\rangle$, resultando em ½, que é a probabilidade de o gato permanecer vivo após a abertura do cofre, sendo equivalente à detecção da partícula que passou pelas fendas do exemplo anterior.

O exemplo parece inócuo, uma vez que isso ocorreria mesmo no cenário clássico. Contudo, enquanto uma das situações antagônicas não é observada, alguma computação quântica poderia ocorrer de modo a interferir nos resultados ou na distribuição de amplitudes de probabilidade de o gato estar vivo ou morto. Essa manipulação sobre os destinos quânticos ocorre no que chamamos de computador quântico.

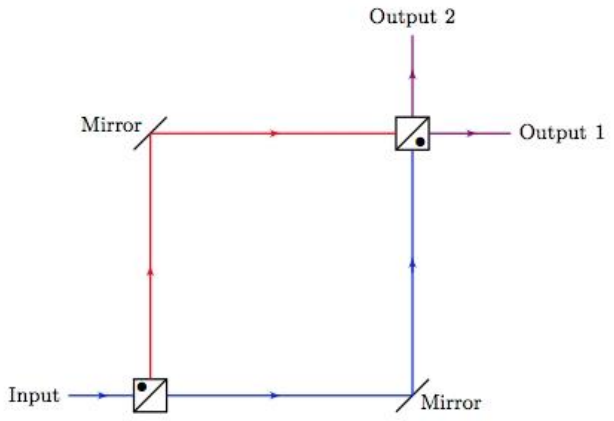

Figura 2- Esboço simplificado do interferômetro de Mach-Zehnder.
Fonte: https://quantummoxie.files.wordpress.com/2013/05/mzi.jpg

Um exemplo mais convincente é o do interferômetro de Mach-Zehnder, vide **Figura 2**. Considere o gato de Schrödinger, vivo, $|\psi_A\rangle$, o fóton que incide pela direção horizontal no espelho semitransparente, conhecido como divisor de feixe. Este será dividido em duas componentes, cada uma com um fator de normalização $1/\sqrt{2}$. O fóton refratado, $|\psi_A\rangle/\sqrt{2}$, que persiste no Caminho Azul, corresponde ao gato vivo até encontrar o espelho na metade do

caminho. Este fóton não sofre retardo de fase, mas sofre uma reflexão total no segundo espelho, mudando seu estado para vertical, $|\psi_B\rangle/\sqrt{2}$, e passando à realidade antagônica à do gato vivo.

Voltando ao início, a segunda possibilidade (Caminho Vermelho) é a de que o fóton esteja no estado $|\psi_B\rangle e^{i\pi}/\sqrt{2}$, onde agora encontra-se com um atraso de meia fase devido ao material (anisotrópico) com que o divisor foi construído. Esta possibilidade conduz o fóton ao estado $|\psi_A\rangle e^{i\pi}/\sqrt{2}$ ao emergir do segundo espelho. Agora o gato do Caminho Vermelho está vivo, mas em contra fase com seu estado inicial.

Continuando, o fóton (gato) do Caminho Vermelho, encontra-se com o segundo divisor, mas a face reflexiva, com retardo de meia fase, está voltada para o fóton do Caminho Azul. Portanto, o $|\psi_A\rangle e^{i\pi}/\sqrt{2}$ divide-se em duas situações antagônicas: $|\psi_A\rangle e^{i\pi}/\sqrt{2}$ e $|\psi_B\rangle e^{i\pi}/\sqrt{2}$. Simbolicamente: $|\psi_A\rangle e^{i\pi}/\sqrt{2} \rightarrow (|\psi_A\rangle e^{i\pi} + |\psi_B\rangle e^{i\pi})/2$.

Por outro lado, o fóton (gato) do Caminho Azul encontra-se no estado $|\psi_B\rangle$ e vai sofrer uma separação no divisor, mas a componente horizontal é quem sofrerá o atraso de meia fase: $|\psi_B\rangle/\sqrt{2} \rightarrow (|\psi_A\rangle e^{i\pi} + |\psi_B\rangle)/2$.

O resultado é que, tomando apenas a componente vertical, emergente do segundo divisor, o estado quântico vertical (gato morto) final é $(|\psi_B\rangle + |\psi_B\rangle e^{i\pi})/2$. Considerando que as cores vermelho e azul nos estados quânticos ilustram o caminho seguido por cada idealização do fóton, podemos reescrever este último resultado sem cores: $(|\psi_B\rangle + |\psi_B\rangle e^{i\pi})/2 = (|\psi_B\rangle - |\psi_B\rangle)/2 = 0$. Portanto, não haverá mais gato morto nesta idealização, já que a amplitude de probabilidade dessa ocorrência é nula.

Analogamente, o resultado do estado emergente horizontal (gato vivo) será $(|\psi_A\rangle + |\psi_A\rangle)e^{i\pi}/2 = |\psi_A\rangle e^{i\pi}$. Portanto, o gato sempre sairá vivo do interferômetro de Mach-Zehnder, mas com um atraso de meia onda. O que interessa é que o gato entra vivo e sai vivo, uma vez que seu destino sofreu uma interferência destrutiva para o caso de sair morto e sofreu uma interferência construtiva para o caso vivo.

Desconsiderando o lado lúdico do exemplo recente, o que esse experimento, dificílimo de pôr em prática devido a questões instrumentais, quer dizer, é que o fóton incidente em uma das duas possíveis direções de entrada do interferômetro emergirá sempre na mesma direção. Isso ilustra a ideia de que a interferência está acontecendo, independentemente de termos ou não um fóton passando através dos caminhos ópticos do interferômetro sobre a distribuição de probabilidades de detecção dos fótons incidentes.

Retornando à Equação (3), a distribuição de amplitudes ψ_j, com $j = 0, \dots, N-1$, forma o espectro de detectabilidade do estado quântico, $|\psi\rangle$, em algum estado puro $|j\rangle$. Tal amplitude é uma consequência seja da repetição de um experimento um grande número de vezes, ou pela realização do mesmo com uma amostra bastante populosa de partículas dinamicamente equivalentes.

Na prática, tal espectro é representado na forma de distribuição de probabilidades, $|\psi_j|^2 \mid j = 0, \dots, N-1$, como é o caso do espectro visível da luz do Sol, onde os quadrados $|\psi_j|^2$ são proporcionais às medidas de intensidade de linhas de emissão e absorção atômicas da atmosfera solar (CHESMAN, ANDRÉ, & MACÊDO, 2004), como ilustrado na **Figura 3**.

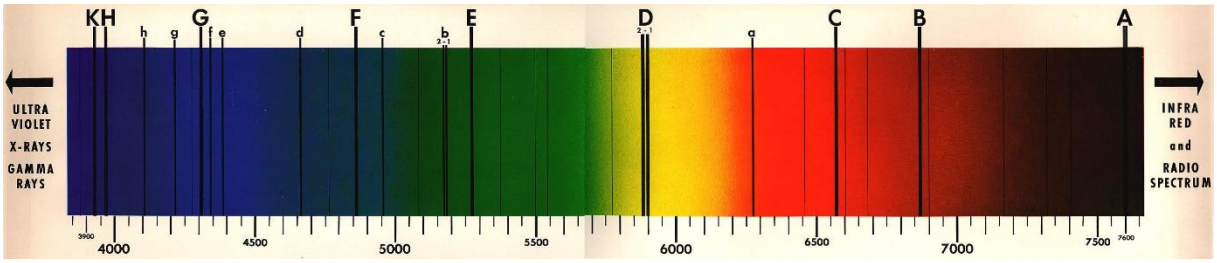

Figura 3 - Espectro solar exibindo linhas de absorção atômica da atmosfera solar.
Fonte: http://www.coseti.org/images/ospect_1.jpg

2.3 Operadores e medida quântica

Operadores no espaço de Hilbert são definidos do mesmo modo que os operadores de espaços vetoriais reais, com a diferença de que a forma dual de um operador, definida como operador adjunto, tem sua representação matricial na forma de transposto Hermitiano do operador original.

O operador adjunto $\hat{A}^\dagger$, associado a um operador $\hat{A}$ do espaço de Hilbert, é o operador definido no espaço dual com a seguinte propriedade: se $|y\rangle = \hat{A}|x\rangle$, então $\langle y| = \langle x|\hat{A}^\dagger$. Neste caso, dizemos que a representação bra $\langle x|$ do ket $|x\rangle$ são adjuntos entre si. De fato, se definirmos $()^\dagger$ a transformação que leva o argumento entre parênteses na sua forma dual, temos por consistência: $(\hat{A}|x\rangle)^\dagger = |x\rangle^\dagger \hat{A}^\dagger = \langle x|\hat{A}^\dagger$.

Se, em particular, $\hat{A} = \hat{A}^\dagger$, o operador $\hat{A}$ é dito auto adjunto ou, como é mais conhecido, *operador hermitiano*. Operadores hermitianos são de extrema relevância na formulação da mecânica quântica, pois estão associados ao processo de medida quântica das grandezas

observáveis, como por exemplo, energia, momento, posição, campo eletromagnético e spin, que são grandezas reais.

Vale observar que a soma $\hat{S} = (\hat{A} + \hat{A}^{\dagger})$ é Hermitiana, já a diferença $\hat{S} = (\hat{A} - \hat{A}^{\dagger})$ é anti-hermitiana, visto que $\hat{S} = -\hat{S}^{\dagger}$.

Se $\hat{A} = \hat{B}^{\dagger}\hat{B}$, então $\hat{A}$ é um operador positivamente semidefinitivo, visto que $\langle\psi|\hat{A}|\psi\rangle \geq 0$, o que pode ser diretamente verificado do fato de que $\langle\psi|\hat{B}^{\dagger}\hat{B}|\psi\rangle = \hat{B}|\psi\rangle \cdot \hat{B}|\psi\rangle = |\hat{B}|\psi\rangle|^2 \geq 0$. Por outro lado, se $\hat{B}$ tem sua representação matricial $\boldsymbol{B}$ tal que $\det(\boldsymbol{B}) \neq 0$, $\hat{A}$ é positivamente definitivo, uma vez que $\langle\psi|\hat{A}|\psi\rangle > 0$. Outra definição que será essencial na definição de portas quânticas no próximo capítulo é a de operador unitário.

Define-se operador unitário $\widehat{\boldsymbol{U}}$ sobre o espaço de Hilbert, o operador quântico com a seguinte propriedade $\widehat{\boldsymbol{U}}^{\dagger}\widehat{\boldsymbol{U}} = \hat{\boldsymbol{I}}$, onde $\hat{\boldsymbol{I}}$ é o operador unitário, cuja representação matricial é a matriz identidade $\boldsymbol{I}$.

Apesar de, na maioria das vezes, os operadores transformarem uma função em outra, em alguns casos um operador pode transformar uma função nela mesma. Esta função é chamada autovetor, e a constante multiplicativa introduzida pelo operador é chamada autovalor.

O autovalor é o único valor que pode efetivamente ser observado ao se fazer uma medida. Um exemplo disto pode ser descrito pelos níveis de energia de um átomo, os quais são os autovalores do operador energia.

2.4 Representação matricial

O teorema espectral nos diz que, se $\widehat{\boldsymbol{A}}$ é um operador, e $\{|e_l\rangle, l = 0,1, \dots, N-1\}$ é uma base ortonormal, isto é $\langle e_k|e_l\rangle = \delta_{kl}$, então $\widehat{\boldsymbol{A}}$ pode ser decomposto nesta base como:

$$\widehat{\boldsymbol{A}} = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} |e_k\rangle\langle e_k|\widehat{\boldsymbol{A}}|e_l\rangle\langle e_l| = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} |e_k\rangle A_{kl}\langle e_l|. \tag{4}$$

Os coeficientes $A_{kl} = \langle e_k|\widehat{\boldsymbol{A}}|e_l\rangle$ são os elementos da matriz $\boldsymbol{A}$ associada ao operador $\widehat{\boldsymbol{A}}$ na base especificada. Os termos na forma $|a\rangle\langle b|$ são a versão ket-bra do produto externo entre os estados quânticos $|a\rangle$ e $|b\rangle$: $|a\rangle\langle b| \equiv |a\rangle \wedge |b\rangle$.

Se, em particular, o operador é definido de modo a ter seus termos matriciais na forma diagonal:

$$\widehat{\boldsymbol{A}} = \sum_{k=0}^{N-1} |e_k\rangle A_k \langle e_k|, \tag{5}$$

então, diz-se que $\widehat{\boldsymbol{A}}$ é diagonalizável com respeito a esta base e seus coeficientes A_k são seus autovalores, e os vetores da base, $|e_k\rangle$, são seus correspondentes autovetores, ou autoestados.

Define-se projetor $\widehat{\boldsymbol{P}}$, sobre a base $\{|e_l\rangle, l = 0,1, \dots, N-1\}$, o seguinte operador unitário:

$$\widehat{\boldsymbol{P}} = \sum_{k=0}^{N-1} |e_k\rangle\langle e_k|, \tag{6}$$

que é o caso particular de se ter $A_{kl} = \delta_{kl}$.

O projetor é, portanto, o operador que revela as coordenadas de um vetor, ou de um outro operador, em relação à base adotada. Por exemplo, um estado quântico $|\psi\rangle$ tem sua representação sobre a base adotada através de:

$$|\psi\rangle = \widehat{\boldsymbol{P}}|\psi\rangle = \sum_{k=0}^{N-1} |e_k\rangle\langle e_k|\psi\rangle = \sum_{k=0}^{N-1} |e_k\rangle\psi_k, \tag{7}$$

onde $\psi_k = \langle e_k|\psi\rangle$. Por este motivo, o projetor na base é isomorfo ao operador identidade: $\widehat{\boldsymbol{P}} = \widehat{\boldsymbol{I}}$.

Com base neste último raciocínio, qualquer operador pode ser decomposto sobre uma base através da aplicação bilateral do projetor da base:

$$\widehat{\boldsymbol{A}} = \widehat{\boldsymbol{P}}\widehat{\boldsymbol{A}}\widehat{\boldsymbol{P}} = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} |e_k\rangle\langle e_k|\widehat{\boldsymbol{A}}|e_l\rangle\langle e_l| = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} |e_k\rangle A_{kl}\langle e_l|. \tag{8}$$

Uma vez especificada a base, é conveniente construir a representação matricial dos operadores. Considere um espaço vetorial complexo V, de dimensão finita n. Dada uma base V, existe uma representação matricial que os associa. Podemos representar as componentes de um vetor de V numa base através de matrizes:

$$|\boldsymbol{a}\rangle \equiv \begin{pmatrix} \boldsymbol{a_1} \\ \boldsymbol{a_2} \\ \vdots \\ \boldsymbol{a_n} \end{pmatrix}, |\boldsymbol{b}\rangle \equiv \begin{pmatrix} \boldsymbol{b_1} \\ \boldsymbol{b_2} \\ \vdots \\ \boldsymbol{b_n} \end{pmatrix}. \tag{9}$$

Os vetores do espaço dual, por sua vez, serão representados da seguinte forma:

$$\begin{aligned} \langle \boldsymbol{a}| &= (\boldsymbol{a_1^*}\ \boldsymbol{a_2^*} \ldots\ \boldsymbol{a_n^*}), \\ \langle \boldsymbol{b}| &= (\boldsymbol{b_1^*}\ \boldsymbol{b_2^*} \ldots\ \boldsymbol{b_n^*}). \end{aligned} \tag{10}$$

E o produto interno:

$$\langle a|b\rangle \equiv (\boldsymbol{a_1^*}\ \boldsymbol{a_2^*} \ldots\ \boldsymbol{a_n^*}) \begin{pmatrix} \boldsymbol{b_1} \\ \boldsymbol{b_2} \\ \vdots \\ \boldsymbol{b_n} \end{pmatrix} = (\boldsymbol{a_1^* b_1} + \ \boldsymbol{a_2^* b_2} + \cdots\ \boldsymbol{a_n^* b_n}), \tag{11}$$

Esta representação será bastante útil na seção 3.2, quando abordaremos sobre bits quânticos.

2.5 Sistemas quânticos acoplados, produtos tensor e emaranhamento quântico

O produto tensor, $|a\rangle \otimes |b\rangle$, entre dois estados puros, $|a\rangle$ e $|b\rangle$, é a abstração matemática da possibilidade de detecção de dois sistemas quânticos em seus estados puros individuais como se formassem um único estado quântico combinado, $|a\rangle \otimes |b\rangle \equiv |a, b\rangle$, denominado estado tensor.

Em particular, se escrevermos o estado quântico de um sistema em coordenadas cartesianas, (x, y, z), temos a função de onda escrita como $\psi(\boldsymbol{x}) = \psi(x, y, z)$. Assim, a componente $\psi(\boldsymbol{x})|\boldsymbol{x}\rangle = \psi(x, y, z)|x, y, z\rangle$. Este último pode ser reescrito segundo a convenção feita no fim do parágrafo anterior:

$$\psi(\boldsymbol{x})|\boldsymbol{x}\rangle = \psi(x, y, z)|x\rangle \otimes |y\rangle \otimes |z\rangle. \tag{12}$$

Se a função de onda pode ser fatorada em três componentes: $\psi(x, y, z) = X(x)Y(y)Z(z)$, então o sistema quântico que é representado por uma partícula na posição (x, y, z) do espaço euclidiano equivale a três sistemas quânticos independentes: $X(x)|x\rangle$, $Y(y)|y\rangle$ e $Z(z)|z\rangle$. Um sistema quântico com essa propriedade de separação de suas variáveis

é dito sistema desacoplado, ou sistema livre em relação às suas componentes quânticas $|x\rangle$, $|y\rangle$ e $|z\rangle$.

Caso contrário ao raciocínio do parágrafo anterior, se não é possível escrever $\psi(x, y, z)$ em termos de funções independentes, $\psi(x, y, z) \neq X(x)Y(y)Z(z)$, então o sistema quântico é dito inseparável em relação aos seus componentes, ou simplesmente dizemos que o sistema tem seus estados puros $|x\rangle$, $|y\rangle$ e $|z\rangle$ emaranhados (no inglês: *entangled*).

Os estados quânticos emaranhados, além de muito úteis no entendimento da mecânica quântica, se sabiamente manipulados, podem resolver diversas tarefas que com apoio de artifícios clássicos não seria viável.

Embora existam modelos computacionais que não utilizam ou utilizam pouco o emaranhamento, como no caso dos modelos de um bit quântico, apenas os que o utilizam constituem computadores ditos universais. Um exemplo prático será demonstrado na seção 3.5.2, através do Problema do Teletransporte.

2.6 Equações de movimento da mecânica quântica

Estados quânticos, associados a medidas de posição e de momento, são determinantes na evolução de uma partícula quântica por serem canonicamente conjugados a partir da transformada quântica de Fourier (adotaremos a sigla inglesa QFT).

2.6.1 Formulação contínua

No contínuo, a QFT dos estados quânticos de posições revela os estados quânticos de momento:

$$|\boldsymbol{p}\rangle = \int dx^3 \, |\boldsymbol{x}\rangle \frac{e^{i\boldsymbol{p}\cdot\boldsymbol{x}/\hbar}}{(2\pi\hbar)^{3/2}}. \tag{13}$$

Já os estados de posição são revelados pela transformada inversa dos momentos:

$$|\boldsymbol{x}\rangle = \int dp^3 \, |\boldsymbol{p}\rangle \frac{e^{-i\boldsymbol{p}\cdot\boldsymbol{x}/\hbar}}{(2\pi\hbar)^{3/2}}. \tag{14}$$

Os operadores que revelam as medidas de posição e de momento são, respectivamente, $\widehat{\boldsymbol{x}}$ e $\widehat{\boldsymbol{p}}$, tais que:

$$\hat{\boldsymbol{x}}|\boldsymbol{x}\rangle = \boldsymbol{x}|\boldsymbol{x}\rangle, \tag{15}$$
$$\hat{\boldsymbol{p}}|\boldsymbol{p}\rangle = \boldsymbol{p}|\boldsymbol{p}\rangle.$$

A partir das equações (13) a (15), chega-se à seguinte decomposição do operador de momento na base dos estados quânticos de posição (MESSIAH, 1961):

$$|\boldsymbol{p}\rangle \equiv \int dx'^{3}\, |\boldsymbol{x}'\rangle\langle\boldsymbol{x}'|\nabla'. \tag{16}$$

Deste último resultado, chega-se à conhecida relação de comutação entre os operadores de posição e momento:

$$[\hat{\boldsymbol{x}}, \hat{\boldsymbol{p}}] = \hat{\boldsymbol{x}}\hat{\boldsymbol{p}} - \hat{\boldsymbol{p}}\hat{\boldsymbol{x}} = i\hbar\mathbf{1}. \tag{17}$$

onde $[\hat{\boldsymbol{x}}, \hat{\boldsymbol{p}}]$ é conhecido como o comutador entre os operadores $\hat{\boldsymbol{x}}$ e $\hat{\boldsymbol{p}}$. O operador $\mathbf{1}$ representa a matriz identidade no espaço euclidiano, que é o espaço dos autovalores observados $\boldsymbol{x}$ e $\boldsymbol{p}$.

O resultado na Equação (16) representa um princípio negativo, conhecido como o *princípio de incerteza de Heisenberg* (HEISENBERG, 1927), que está vinculado ao fato de que grandezas canonicamente conjugadas são perturbadas pelo processo de medida de uma grandeza, por exemplo $\boldsymbol{p}$, seguida da medida da outra $\boldsymbol{x}$.

Além dos operadores de momento e posição, existem os operadores canonicamente conjugados de energia total de um sistema quântico e do tempo do mesmo.

O operador que revela a energia total do sistema quântico é o operador hamiltoniano $\hat{H}$, cujo autovalor é a medida da energia total E na sua forma clássica envolvendo o valor do momento e a energia potencial, independente do tempo:

$$E = \frac{p^2}{2m} + V(\boldsymbol{x}) \tag{18}$$

Portanto, existe a seguinte relação entre os operadores associados aos autovalores envolvidos na Equação (18):

$$\hat{H} = \frac{\hat{\boldsymbol{p}} \cdot \hat{\boldsymbol{p}}}{2m} + V(\boldsymbol{x}) \tag{19}$$

A energia potencial é sempre diagonal na representação das posições $\boldsymbol{x}$ e por este motivo aparece como uma função sem a notação chapéu (^). O produto escalar entre o operador $\hat{\boldsymbol{p}}$ e ele mesmo se deve ao fato de ser um operador quântico com autovalores vetoriais no espaço euclidiano. Contudo, alguns autores representam simplesmente como $\hat{p}^2$.

A equação fundamental do movimento de uma partícula na mecânica quântica é conhecida como Equação de Schrödinger e é escrita operacionalmente como:

$$\widehat{H}|\psi\rangle = \left[\frac{\widehat{\boldsymbol{p}}\cdot\widehat{\boldsymbol{p}}}{2m} + V(\boldsymbol{x})\right]|\psi\rangle = E|\psi\rangle = i\hbar\frac{\partial}{\partial t}|\psi\rangle. \tag{20}$$

A solução geral, no regime estacionário, é obtida do seguinte operador unitário:

$$|\psi(t)\rangle = e^{i\widehat{H}t/\hbar}|\psi_0\rangle, \tag{21}$$

onde $|\psi_0\rangle$ é o estado inicial do sistema quântico.

Este último resultado está diretamente ligado à forma com que as máquinas quânticas sofrem transições conservando a probabilidade de detecção do resultado computado após um número de transformações unitárias, que serão denominadas no Capítulo 3 como portas quânticas (quantum gates).

2.6.2 Formulação discreta

A forma discreta da QFT dos estados quânticos de posições revela os estados quânticos de momento. Contudo, abolimos a representação tridimensional e passamos a representar as coordenadas como sendo parte de cada elemento de uma grade quântica com $N = n^3$.

Com base no raciocínio acima, redefinindo as coordenadas de posição x e momento p, numa grade de N elementos, como inteiros não negativos, $0 \leq x, p \leq N-1$.

$$|p\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle e^{\frac{i2\pi px}{N}}. \tag{22}$$

Já os estados de posição são revelados pela transformada inversa dos momentos:

$$|x\rangle = \frac{1}{\sqrt{N}}\sum_{p=0}^{N-1}|p\rangle e^{\frac{-i2\pi px}{N}}. \tag{23}$$

Apesar dos símbolos x e y representarem os valores discretos de posição e momentum, respectivamente, existe um fator de escala que está sendo omitido que é a multiplicação de px por $\left(\frac{2\pi\hbar}{N}\right)$.

O mesmo raciocínio feito com operadores de posição, momento e energia continuam valendo para o caso discreto. Em particular, se $\widehat{H}$ é o operador hamiltoniano, vale a solução da

equação de Schrödinger, no regime permanente, sendo escrita como a atuação de um operador unitário $\widehat{U}_t = e^{i\hat{H}t/\hbar}$:

$$|q_t\rangle = \widehat{U}_t|q_0\rangle. \tag{24}$$

O resultado na Equação (24) é a chave do elemento de complexidade temporal quântica, que é expressa na forma de transformações quânticas unitárias, representadas tanto nos circuitos quânticos quanto nas transições de autômatos quânticos e máquinas de Turing quânticas, no Capítulo 3.

2.7 Resumo dos postulados da mecânica quântica

Em resumo do que foi visto nas seções anteriores deste capítulo, mecânica quântica é postulada por quatro princípios:

a) Todo sistema físico se associa a um espaço vetorial complexo denominado espaço de Hilbert, $\mathcal{H}$. Os elementos deste espaço são vetores complexos, $|\psi\rangle$, denominados *ket*, e os elementos do espaço dual $\mathcal{H}^*$, correspondem ao transposto hermitiano $\langle\psi|$, denominados *bra*, de cada vetor $|\psi\rangle$ de $\mathcal{H}$;
b) A evolução temporal de um sistema quântico se dá através de transformações unitárias;
c) As medições são representadas por um conjunto de operadores de medidas. A probabilidade de que o resultado seja encontrado em um desses operadores é que nos dá a resposta;
d) Os elementos de um sistema quântico composto são formados pelo produto tensor dos vetores complexos dos espaços de Hilbert desses sistemas individuais.

3 ELEMENTOS DE COMPUTAÇÃO QUÂNTICA

A ciência da computação moderna teve início em 1936, quando o britânico Alan Turing (TURING, 1936) desenvolveu um dispositivo universal denominado Máquina de Turing em seu artigo “On Computable Numbers, with an application to the Entscheidungsproblem”.

No mesmo ano de 1936, o matemático estadunidense Alonzo Church e Alan Turing alegaram que o modelo computacional da Máquina de Turing era tão poderoso quanto qualquer outra máquina, não havendo possibilidade de existir outra mais potente. Essa observação pode ser definida na teste de Church-Turing como:

“Toda função que é considerada naturalmente computável pode ser computada por uma Máquina de Turing.”

Tal princípio é tão forte que induz a **Máquina de Turing Universal**, que é a máquina que tem capacidade de exercitar (simular) uma Máquina de Turing teste, cuja descrição matemática é codificada, juntamente com seus dados de teste, e posta na entrada da máquina universal. Esta é a ideia do processador que recebe uma codificação da memória e executa as instruções codificadas nela.

Após Turing, os primeiros computadores foram desenvolvidos. John von Neumann criou uma forma de tornar uma Máquina de Turing Universal utilizável de forma prática, juntando todos os componentes e criando uma estrutura capaz de armazenar programas na própria memória, a arquitetura de Von Neumann.

A evolução e o poder dos computadores chegou a um ponto que, em 1965, Gordon Moore, cofundador e chefe aposentado da Intel, realizou uma observação denominada Lei de Moore, indicando que o poder de processamento dos computadores iria dobrar a cada dois anos. De fato, ele estava certo e eis que surge um problema: para enfrentar esta enorme demanda, os componentes foram reduzindo de forma espantosa. Efeitos quânticos começaram a ser necessários.

Uma possível solução para tal problema seria a criação de um computador quântico que ofereceria uma vantagem exponencial em relação aos computadores clássicos. Motivado por esta premissa, o físico David Deutsch (DEUTSCH, 1985) tentou definir um dispositivo computacional capaz de simular um sistema físico arbitrário. Ele descreveu um simples exemplo demonstrando o poder computacional que teria um computador quântico. Este primeiro passo foi essencial para que, anos depois, diversos outros estudiosos explorassem

problemas que poderiam ser solucionados através de computadores quânticos (NIELSEN & CHUANG, 2000).

3.1 Teorema de Bell e o efeito EPR

No início do século XX, Albert Einstein mostrou-se infeliz com a mecânica quântica. Tal era esta inquietação que, em 1935, A. Einstein, B. Podolsky e N. Rosen (EINSTEIN, PODOLSKY, & ROSEN, 1935) deram origem ao chamado paradoxo de EPR, argumentando que a mecânica quântica estava incompleta. Segundo eles, havia uma condição de completude que devia ser seguida:

"Cada elemento de realidade física deve possuir uma contraparte na teoria física."

Esta afirmação foi demonstrada através de um experimento. Se duas partículas são postas a uma certa distância, então para que o teorema da superposição (amplamente discutido na seção 2.2) esteja correto, se estas partículas estão entrelaçadas, o que ocorrer em uma interfere na outra. O paradoxo EPR conclui que, se esta interação entre elas percorre um caminho mais rápido que a da luz, e se as leis da física estavam corretas, isto era impossível de ocorrer.

Foi essa publicação que incentivou o físico John Stewart Bell (BELL, 1964) a provar, através da derivação de uma desigualdade, conhecida como desigualdade de Bell, que o que Einstein argumentou era incompatível com as previsões probabilísticas da mecânica quântica. Ele demonstrou que o emprego das proposições de localidade, realidade e completeza teórica não se aplicam para o caso quântico.

3.2 Bits quânticos (qubits)

Um bit quântico, ou como é chamado nos textos internacionais, *qubit*, é um sistema quântico que tem como observável um bit clássico: 0 ou 1.

Diferentemente dos bits clássicos, um bit quântico $|\psi\rangle$, enquanto não observado, é a superposição dos estados puros antagônicos $|0\rangle$ e $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{25}$$

onde α e β são números complexos e $|\alpha^2|$ e $|\beta^2|$ são as probabilidades de o sistema encontrar-se nos estados $|0\rangle$ e $|1\rangle$, respectivamente, valendo a regra de normalização $|\alpha^2| + |\beta^2| = 1$.

A Equação (25) abstrai um vetor no espaço de Hilbert em duas dimensões, gerado pela base ortonormal $\{|0\rangle, |1\rangle\}$ dos estados computacionais puros $|0\rangle$ e $|1\rangle$.

Em algumas situações, como mencionado na seção 2.4, é conveniente representar os estados quânticos computacionais puros na forma matricial: $|0\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix}$ e $|1\rangle \equiv \begin{bmatrix}0\\1\end{bmatrix}$.

Um bit clássico pode ser comparado a uma moeda, onde pode-se ter cara ou coroa, mas nunca os dois virados para o mesmo lado ao mesmo tempo. No caso quântico, por sua vez, estes dois estados, mutualmente exclusivos, podem coexistir até que os mesmos sejam observados (NIELSEN & CHUANG, 2000).

Como estamos tratando de números complexos, a equação (25) pode ser reescrita da seguinte forma:

$$|\psi\rangle = e^{i\varphi}\left[\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right]. \tag{26}$$

O escalar $e^{i\varphi}$, denominado fator de fase global, pode ser desprezado por não produzir efeitos relativos entre os estados puros $|0\rangle$ e $|1\rangle$. Isso equivale a dizer que esse fator de fase não sofre mudança frente a transformações unitárias (MOTTA, CARVALHO, & MACULAN, 2005):

$$\widehat{U}|\psi\rangle = e^{i\varphi}\widehat{U}\left[\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right]. \tag{27}$$

Resultando, portanto, no seguinte:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{28}$$

Os números θ e φ definem um ponto na esfera tridimensional, denominada esfera de Bloch, como ilustrado na **Figura 4**.

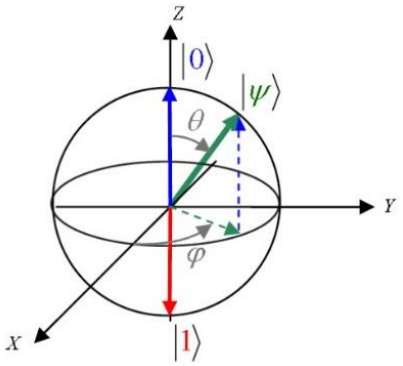

Figura 4 - Esfera de Bloch.
Fonte: https://upload.wikimedia.org/wikipedia/commons/e/e9/Sphere_bloch.jpg

Assim como na computação clássica, os bits quânticos podem ser manipulados através de portas quânticas, onde o circuito contém barramentos e portas que manipulam a informação. Como exemplo, descreveremos um pouco sobre as principais portas utilizadas, que darão base para as demais. Três delas ($\hat{X}$, $\hat{Y}$ e $\hat{Z}$) foram introduzidas pelo físico austríaco Wolfgang Ernst Pauli como operadores de spin de um elétron na teoria não-relativista de Schrödinger, sendo elas matrizes complexas 2x2, hermitianas e unitárias (VIANA, 2010).

3.3 Portas quânticas de 1 qubit

Os circuitos computacionais clássicos são basicamente compostos por fios e portas lógicas, responsáveis pela manipulação de informações. Na computação quântica, as portas lógicas não são mais do que operadores unitários. Ou seja, qualquer operação pode ser realizada a partir de um conjunto de portas.

Como visto na Seção 2.3, operadores quânticos têm representação matricial na forma de transposto Hermitiano do operador original. Este artifício será útil quando necessário fazer um paralelo entre portas quânticas e portas clássicas.

Descreveremos algumas das mais importantes portas lógicas, as quais serão base para entendermos a idealização de algoritmo quântico.

3.3.1 Porta $\hat{X}$ (NOT)

Esta porta quântica tem como função comutar os estados puros, $|0\rangle$ e $|1\rangle$, cujo comportamento clássico, em termos dos rótulos observáveis, '0' e '1', é o mesmo da porta clássica NOT: $\mathrm{NOT}(0) = 1$ e $\mathrm{NOT}(1) = 0$.

Lembremos que toda porta quântica é um operador unitário, que pode atuar sobre um estado misto $|\psi\rangle$, dado na Equação (25). Deste modo, $\hat{X}|\psi\rangle$ tem como efeito:

$$\hat{X}|\psi\rangle = \beta|0\rangle + \alpha|1\rangle. \tag{29}$$

Esta porta é representada matricialmente por:

$$\hat{X} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{30}$$

Se estivermos tratando de um sistema $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, sua representação matricial é escrita simplesmente como:

$$|\psi\rangle \equiv \begin{bmatrix} \alpha \\ \beta \end{bmatrix}. \tag{31}$$

Após passar pela porta $\hat{X}$, obteremos a seguinte saída:

$$\hat{X}|\psi\rangle \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}, \tag{32}$$

que resulta na permuta entre as linhas do vetor original.

3.3.2 Porta $\hat{Y}$

A porta $\hat{Y}$ tem a seguinte representação matricial:

$$\hat{Y} \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \tag{33}$$

onde, ao ser aplicada em um bit quântico genérico, resulta no seguinte:

$$\hat{Y}|\psi\rangle \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -i\beta \\ i\alpha \end{bmatrix} \equiv i(|1\rangle - |0\rangle). \tag{34}$$

3.3.3 Porta $\widehat{Z}$

Conhecida como porta mudança de fase, esta porta mantém o estado $|0\rangle$ inalterado e troca o sinal do estado $|1\rangle$ para $-|1\rangle$. Sua matriz tem a forma:

$$\hat{Z} \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{35}$$

3.3.4 Porta de Hadamard

Uma das portas mais utilizadas, a porta de Hadamard, $\widehat{H}$, criada pelo matemático francês Jacques Salomon Hadamard (Hadamard, 1893), realiza uma operação de rotação de 90º no eixo y da esfera de Bloch, seguido de uma reflexão no plano $x - y$. A matriz pode ser descrita como:

$$\widehat{H} \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{36}$$

Seu papel é transformar o estado $|0\rangle$ em $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e o estado $|1\rangle$ em $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, da seguinte forma:

$$\begin{aligned} \widehat{H}|0\rangle &\equiv \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \\ \widehat{H}|1\rangle &\equiv \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}. \end{aligned} \tag{37}$$

Observe que os estados resultantes são ortogonais.

Veremos mais à frente o poder desta porta para a construção de diversos circuitos quânticos.

3.4 Múltiplos qubits e suas portas quânticas – portas controladas

Agora que entendemos um pouco sobre o qubit, exploraremos a utilização simultânea de dois ou mais deles.

Suponha, primeiramente, um caso mais simples com dois bits quânticos. Assim como no caso clássico, podemos ter quatro possibilidades de estados produto, $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, da base original de qubits.

Esses estados mútuos resultam na superposição de estados que compõem um estado misto $|\psi\rangle$:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \tag{38}$$

Vale para a equação acima o mesmo raciocínio sobre emaranhamento quântico da Seção 2.5.

Da mesma forma como trabalhamos com portas quânticas de um só qubit, é possível obtermos portas de múltiplos qubits. Demonstraremos as mais relevantes a seguir.

3.4.1 Porta de Hadamard generalizada – $\widehat{H}_n$

Uma generalização da porta quântica de Hadamard, $\widehat{H}_n$, para n qubits, é construída, sem quebra de consistência com a ideia de operadores quânticos, a partir da definição recursiva de matrizes de Hadamard:

$$\widehat{H}_n = \frac{1}{\sqrt{2}}\begin{bmatrix} \widehat{H}_{n-1} & \widehat{H}_{n-1} \\ \widehat{H}_{n-1} & -\widehat{H}_{n-1} \end{bmatrix}. \tag{39}$$

É fácil verificar por indução que a matriz associada ao operador de Hadamard para n qubits tem 2^n linhas por 2^n colunas.

Alguns autores utilizam a notação de potência de produto tensor para a porta generalizada de Hadamard. Por exemplo, Nielsen e Chuang (2000), utilizam a notação $\widehat{H}^{\otimes 2^n}$. Contudo, consideramos esta última notação desnecessária uma vez que o próprio Hadamard convencionou a notação adotada neste trabalho.

Por questão de consistência, convencionamos a porta de Hadamard de 1 só qubit satisfazendo a identidade: $\widehat{H}_1 \equiv \widehat{H}$.

3.4.2 Porta Not Controlada ($\widehat{U}_{CN}$)

Esta porta lógica é formada por dois qubits de entrada, onde um deles controla a saída do outro. A representação desse circuito é mostrada na **Figura 5**.

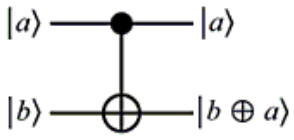

Figura 5 - Representação da porta quântica $\widehat{U}_{CN}$.

A **Tabela 1** descreve o comportamento da porta quântica $\widehat{U}_{\mathrm{CN}}$ em função dos estados puros de entrada $|a\rangle \otimes |b\rangle$. Se o qubit $|a\rangle$ for $|0\rangle$, então ele não controla a saída de $|b\rangle$, que será o mesmo da entrada. Em contrapartida, se $|a\rangle$ for $|1\rangle$, o bit quântico $|b\rangle$ tem seu resultado invertido. Assim, a porta $\widehat{U}_{\mathrm{CN}}$ é multifuncional, visto que pode se comportar como um NOT, se a entrada $|a\rangle = |1\rangle$, ou pode assumir o comportamento de um XOR (ou-exclusivo), se a entrada é genérica $|a\rangle \otimes |b\rangle = |a \oplus b\rangle$, onde $\oplus$ é o operador XOR, atuando sobre os bits clássicos a e b.

Tabela 1 - Possibilidades de entradas da porta quântica $\widehat{U}_{CN}$ e suas saídas.

Entrada $\|a\rangle$	Entrada $\|b\rangle$	Saída $\|a\rangle$	Saída $\|b\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

A matriz desta porta é expressa da seguinte forma:

$$\widehat{U}_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{40}$$

pois $|00\rangle \equiv \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$; $|01\rangle \equiv \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$; $|10\rangle \equiv \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$ e $|11\rangle \equiv \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$.

3.4.3 Porta de Toffoli

Uma das grandes dificuldades da computação quântica ao utilizar portas como as demonstradas anteriormente para fins de simulações, deve-se ao fato de que a mecânica quântica trabalha com portas reversíveis.

Para solucionar esta questão, existe um artifício denominado porta de Toffoli. Ela é composta por 3 bits quânticos de entrada, com os dois primeiros controlando a saída do último.

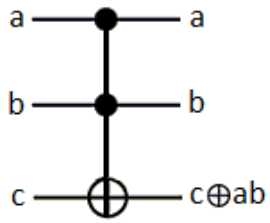

Figura 6 - Representação da porta quântica de Toffoli.

Assim como a porta $\widehat{U}_{CN}$, apenas no caso de os dois bits de controle serem $|1\rangle$, a saída do terceiro bit é invertida (vide **Tabela 2**).

Tabela 2 - Possibilidades de entradas e saídas da porta de Toffoli.

Entrada **a**	Entrada **b**	Entrada **c**	Saída **a**	Saída **b**	Saída **c**
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Esta porta é útil para simular, por exemplo, a porta NAND e o FANOUT.

3.5 Algoritmos quânticos

Um algoritmo nada mais é do que um conjunto de procedimentos para se realizar uma tarefa. Atualmente, os computadores possuem diversos programas que nos ajudam a realizar as atividades do dia a dia, desde programas mais simples como uma calculadora ou até mais complexos. Com o advento da computação quântica, porém, tais algoritmos tornaram-se obsoletos. Um exemplo de um algoritmo quântico proposto foi desenvolvido pelo matemático Peter Shor (SHOR, 1994), onde formulou uma solução para decompor um número relativamente grande em fatores primos. Esta proposta mostrou o poderio de um computador quântico comparado ao modelo clássico. Um exemplo disto pode ser verificado na **Figura 7**, onde é comparado o tempo para calcular a fatoração pelo método de Shor e o tempo por um algoritmo clássico. A rapidez do mesmo deve-se, principalmente, ao fato de ser baseado na transformada quântica de Fourier.

COMPRIMENTO DO NÚMERO A SER FATORADO (EM *BITS*)	TEMPO DE FATORAÇÃO POR ALGORITMO CLÁSSICO	TEMPO DE FATORAÇÃO COM O 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

Figura 7 - Comparação entre o algoritmo de Shor e o modelo clássico.
Fonte: Revista Ciência Hoje, Vol. 33, n. 193, Maio de 2003.

Cerca de dois anos depois, o cientista computacional Lov Kumar Grover (GROVER, 1996) desenvolveu um algoritmo de busca em bancos de dados. A vantagem computacional por ele apresentada foi a nível potencial. Em outras palavras, enquanto um algoritmo clássico realiza um processo de busca com n tentativas, o de Grover necessita de $\sqrt{n}$ (OLIVEIRA, 2004).

Atualmente, existem apenas três algoritmos quânticos: o de Shor e o de Grover que já foram citados anteriormente, e um terceiro do físico israelense David Deutsch (DEUTSCH, 1985) .

3.5.1 O oráculo de Deutsch – paralelismo quântico

É conhecido da teoria de algoritmos o problema da busca por funções binárias balanceadas, sobre o domínio $\{0,1\}^n$ de cadeias de bits de comprimento n. Mais especificamente, o algoritmo verifica se as partições, D_0 e D_1, tais que $f(x) = 0 \Rightarrow x \in D_0$ e $f(x) = 1 \Rightarrow x \in D_1$, têm o mesmo número de pontos.

Um caso particular em que f é não balanceada ocorre quando f é constante sobre o domínio $\{0,1\}^n$, por exemplo, $f(x) = 1, \forall x \in \{0,1\}^n$.

Em qualquer um dos casos, seja na busca por funções balanceadas ou na busca por funções constantes, a complexidade temporal é $O(2^n)$, visto que todos os valores do domínio devem ser verificados, não importando a ordem de varredura do domínio.

O algoritmo de Deutsch é uma forma de verificar se uma função é balanceada, ou constante no domínio, utilizando o potencial do paralelismo quântico.

Tal algoritmo baseia-se na idealização de uma máquina de Turing quântica (**Figura 8**), representada como uma caixa preta, abstraindo a porta quântica U_f, que simula uma função binária clássica, $f: \{0,1\}^n \mapsto \{0,1\}$.

Conforme a **Figura 8**, a caixa preta transforma o estado puro $|x\rangle \otimes |y\rangle$ no estado misto $|y \oplus f(x)\rangle$. O primeiro registrador, que recebe o estado puro $|x\rangle$, corresponde ao estado tensor de n qubits. Já o segundo registrador, recebe o estado puro $|y\rangle$, que é um dos estados $|0\rangle$ e $|1\rangle$.

Todo o potencial de paralelismo da máquina quântica da **Figura 8** é subutilizado se apenas um estado puro de cada vez for posto na entrada da máquina. O mesmo ocorre com o segundo registrador, que transforma a saída, de 1 qubit, em $|f(x)\rangle$, se este for $|y\rangle = |0\rangle$, ou transforma a saída no complementar $|\bar{f}(x)\rangle$, se $|y\rangle = |1\rangle$.

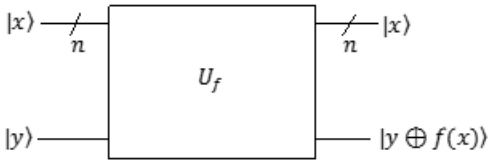

Figura 8 – Ilustração de uma função binária quântica de uma cadeia de n bits

A melhor forma de explorar o paralelismo quântico da máquina hipotética da **Figura 8** é pôr na entrada de n qubits o estado misto da superposição de todos os valores do domínio, substituindo $|x\rangle$ por $|\psi\rangle$:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle = \hat{H}_n|0\rangle. \tag{41}$$

Raciocínio semelhante pode ser feito sobre o qubit do segundo registrador de entrada, mas utilizando na entrada a forma combinada $(|0\rangle - |1\rangle)/\sqrt{2}$ para que haja distinção de fase entre os estados que tornam a saída $|f(x)\rangle$ e $|\bar{f}(x)\rangle$. Assim, omitindo detalhes do desenvolvimento feito por Deutsch (1985), seu algoritmo quântico, ou oráculo quântico, é ilustrado na **Figura 9**.

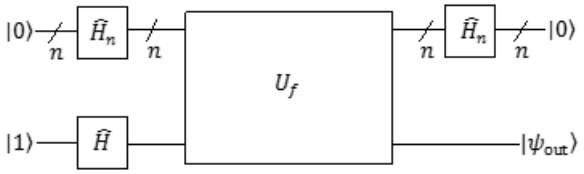

Figura 9 - Oráculo de Deutsch (1985)

Uma generalização deste algoritmo para funções de vários bits foi proposta por David Deutsch e Richard Jozsa (DEUTSCH & JOZSA, 1992) no artigo intitulado *"Rapid solution of problems by quantum computation"*. Enquanto o algoritmo de Deutsch trabalha de forma probabilística, o de Deutsch-Josza funciona de modo determinístico. Esta generalização que tornou possível a demonstração da economia de tempo de algoritmos quânticos para sistemas maiores.

3.5.2 O problema do teletransporte

Um exemplo muito interessante para entender tudo o que foi visto até o momento é o famoso problema do teletransporte. Ao contrário do que muitos pensam, teletransportar não é mover uma matéria de um lugar para outro. O objetivo, na verdade, é transmitir uma informação de um objeto e enviar para outro objeto sem tê-lo observado. Voltando ao exemplo, ele consiste em mover estados quânticos mesmo sem nenhum canal de comunicação entre o remetente e o destinatário da mensagem. Consideremos, por exemplo, dois indivíduos quaisquer Alice e Bob. Eles geram um par emaranhado de bits quânticos, e cada um leva consigo uma unidade desse par. Por algum motivo, anos depois, eles precisam se comunicar de forma que ninguém os intercepte. A missão de Alice é enviar uma informação $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ quaisquer para Bob, sendo que a única forma de fazer isso é enviando uma mensagem clássica, que, a princípio, não tem sentido ou ligação alguma.

Como funciona? Alice deve interagir a informação $|\psi\rangle$ com a metade do par emaranhado que ela possui, e depois realizar a medição clássica deste resultado. Após enviar esta medição clássica para Bob, dependendo de qual ela for, Bob realizará determinada operação em sua metade do par. O resultado que ele obterá é a própria informação $|\psi\rangle$ que Alice desejava a princípio enviar.

Para entendermos melhor, é preciso explorar passo a passo deste exemplo. A **Figura 10** ilustra o sistema como um todo. Cada etapa é observada como se ocorressem em paralelo, em apenas um passo de tempo.

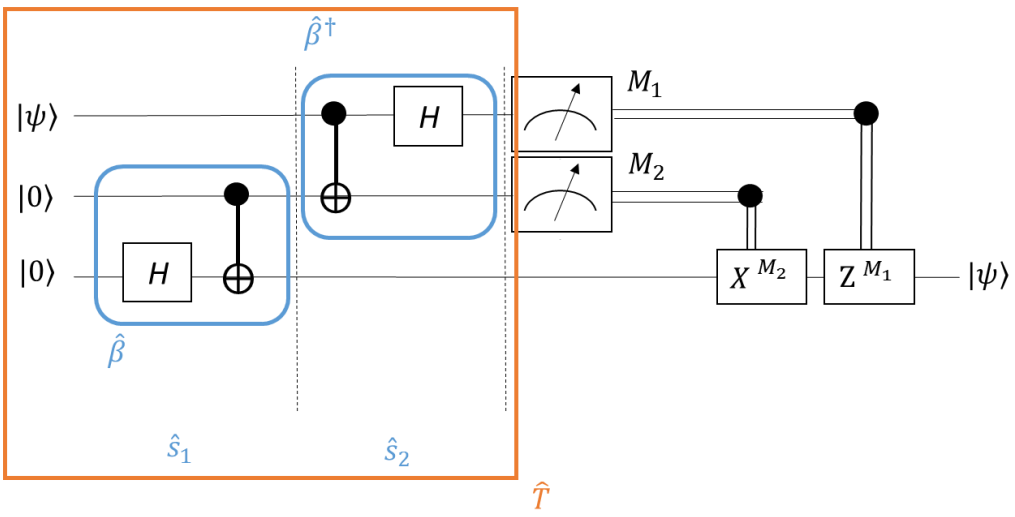

Figura 10 - Circuito quântico para teletransportar um bit quântico.

Primeiramente, Alice e Bob emaranham o par de qubits. Uma forma de fazer isso é passar um dos bits por uma porta de Hadamard, seguido da porta $\widehat{U}_{CN}$. Veja a ilustração em detalhes na **Figura 11**.

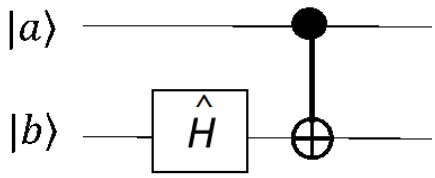

Figura 11 - Emaranhador quântico de Bell.

Esta porta é importantíssima para a computação quântica, e tem a função de emaranhar bits quânticos. A chamaremos de $\hat{\beta}$:

$$\hat{\beta} = \widehat{U}_{CN}(\widehat{H}\otimes\hat{I}), \tag{42}$$

cuja representação matricial é

$$\hat{\beta} \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} I_2 & 0_2 \\ 0_2 & X \end{bmatrix}\begin{bmatrix} I_2 & I_2 \\ I_2 & -I_2 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} I_2 & I_2 \\ X & -X \end{bmatrix}. \tag{43}$$

Se não houvesse a primeira linha da **Figura 10** representando a informação, estes passos bastariam. Porém, como trabalhamos com as três linhas ocorrendo em paralelo, devemos realizar a seguinte operação:

$$\hat{S}_1 = \hat{I}\otimes\hat{\beta}. \tag{44}$$

Cuja representação matricial é

$$\hat{S}_1 \equiv \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\otimes\begin{bmatrix} I_2 & I_2 \\ X & -X \end{bmatrix} = \tfrac{1}{\sqrt{2}}\begin{bmatrix} I_2 & I_2 & & \\ X & -X & & \\ & & I_2 & I_2 \\ & 0_4 & X & -X \end{bmatrix}. \tag{45}$$

Olhando um pouco mais à frente do circuito, é possível verificar uma outra porta, que, ao contrário da porta anterior, tem a função de desemaranhar qubits.

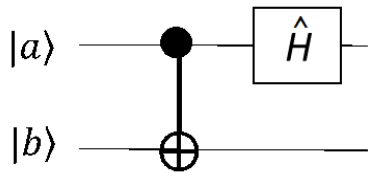

Figura 12 - Desemaranhador quântico.

Para obtê-la, é só seguir o padrão da operação anterior:

$$\hat{\beta}^{\dagger} = (\hat{H}\otimes\hat{I})\hat{U}_{CN}. \tag{46}$$

Representando matricialmente:

$$\hat{\beta}^{\dagger} \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} I_2 & I_2 \\ I_2 & -I_2 \end{bmatrix}\begin{bmatrix} I_2 & 0_2 \\ 0_2 & X \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} I_2 & X \\ I_2 & -X \end{bmatrix}. \tag{47}$$

E, dessa forma, encontrar o $\hat{S}_2$ aplicando novamente o produto tensor. Desta vez, porém, a porta $\hat{\beta}^{\dagger}$ está nas duas linhas de cima da **Figura 10**, resultando em:

$$\hat{S}_2 = \hat{\beta}^{\dagger}\otimes\hat{I}, \tag{48}$$

onde, matricialmente:

$$\hat{S}_2 \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} I_2 & X \\ I_2 & -X \end{bmatrix}\otimes I_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} I_2\otimes I_2 & X\otimes I_2 \\ I_2\otimes I_2 & -X\otimes I_2 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} I_4 & 0_2 & I_2 \\ & I_2 & 0_2 \\ I_4 & 0_2 & -I_2 \\ & -I_2 & 0_2 \end{bmatrix} \tag{49}$$

Por fim, chegamos na matriz resultante do teletransporte, sem medição:

$$\hat{T} \equiv \frac{1}{2}\begin{bmatrix} I_4 & 0_2 & I_2 \\ & I_2 & 0_2 \\ I_4 & 0_2 & -I_2 \\ & -I_2 & 0_2 \end{bmatrix}\begin{bmatrix} I_2 & I_2 & 0_4 \\ X & -X & \\ 0_4 & & I_2 \quad I_2 \\ & & X \quad -X \end{bmatrix} = \begin{bmatrix} I & -X & X & -X \\ X & -X & I & I \\ I & I & -X & X \\ X & -X & -I & -I \end{bmatrix} \tag{50}$$

Vamos analisar agora a entrada desse circuito. Observe que na primeira linha, temos a informação $|\psi\rangle$ que Alice deseja transmitir a Bob. Na segunda linha, temos o bit quântico emaranhado que Alice levou consigo, e na terceira linha o par deste bit quântico que ficou com Bob. Neste caso, como já sabemos a priori que os dois últimos bits quânticos são $|0\rangle$ e $|0\rangle$, a informação só pode ter duas opções: $|000\rangle$ ou $|100\rangle$. Em outras palavras, ela tem uma

probabilidade α de encontrar-se no estado $|000\rangle$ e uma probabilidade β de encontrar-se no estado $|100\rangle$, conforme a matriz abaixo.

$$|\psi\rangle \equiv \begin{bmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ \beta \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{51}$$

Ao multiplicarmos a matriz resultante com a entrada, chegaremos finalmente em quatro possibilidades ilustradas da **Figura 13**.

$$\hat{T}|\psi\rangle \equiv \frac{1}{2}\begin{bmatrix} \alpha \\ \beta \\ \beta \\ \alpha \\ \alpha \\ -\beta \\ -\beta \\ \alpha \end{bmatrix} \begin{matrix} \} \; |00\rangle(\alpha|0\rangle + \beta|1\rangle) = |00\rangle|\psi\rangle \\ \} \; |01\rangle(\beta|0\rangle + \alpha|1\rangle) = |01\rangle\hat{X}|\psi\rangle \\ \} \; |10\rangle(\alpha|0\rangle - \beta|1\rangle) = |10\rangle\hat{Z}|\psi\rangle \\ \} \; |11\rangle(-\beta|0\rangle + \alpha|1\rangle) = |11\rangle\hat{Z}\hat{X}|\psi\rangle \end{matrix}$$

Figura 13 - Possíveis resultados do problema do teletransporte.

Note que, para que Bob recupere o valor de $|\psi\rangle$, basta ele saber qual resultado Alice mediu. Se for $|00\rangle$, ele não precisa fazer nada. Se for $|01\rangle$, ele deve aplicar a porta $\hat{X}$, e assim por diante.

Esta é apenas uma demonstração simples. Através deste exemplo, é possível explorar diversas outras maneiras de intercambiar recursos, e até mesmo desenvolver códigos de correção de erros quânticos.

4 TEORIA QUÂNTICA DA COMPUTAÇÃO

A tese de Church-Turing visto no Capítulo 3 teve larga aceitação na época, levando ao desenvolvimento de uma rica teoria da computação. Acreditava-se que a Máquina de Turing era tão poderosa que qualquer problema poderia ser eficientemente resolvido por ela.

Com o advento da mecânica quântica, surgiu a necessidade de testar problemas que um computador clássico não é capaz de reproduzir, devido às propriedades que a física clássica não obedece. Em 1982, Paul Benioff (BENIOFF, 1982) propôs o primeiro modelo teórico para um computador quântico. Apesar de seu pioneirismo, o que de fato Benioff construiu era perfeitamente capaz de ser simulado através de uma Máquina de Turing, sendo, portanto, considerado clássico.

Ainda em 1982, o físico Richard Feynman (FEYNMAN, 1982), pioneiro no desenvolvimento da eletrodinâmica quântica, criou um simulador quântico universal, do qual podia simular qualquer sistema de espaço de estados de dimensão finita.

Em 1983, David Albert (ALBERT, 1983) publicou o artigo "A Quantum-Mechanical Automation", em que descreve um autômato capaz de medir certas propriedades físicas, não tendo nenhum autômato clássico análogo a ele.

Dois anos depois, David Deutsch (DEUTSCH, 1985) formulou a ideia de um computador quântico universal generalizado capaz de simular qualquer sistema físico finito clássico com perfeição. Ele pode, também, simular sistemas ideais, incluindo todas as outras instâncias de um computador quântico com alta precisão (mas não perfeita). Veremos com detalhes na seção 4.4 as principais características desta máquina.

4.1 Autômatos finitos

Um autômato é um dispositivo que reconhece linguagens formais utilizando o conceito de máquinas. Ele reconhece se uma dada cadeia de símbolos pertence ou não àquela linguagem, sendo usado, por exemplo, em editores de texto para reconhecer padrões. Um autômato finito é a forma mais simples de uma Máquina de Turing.

4.1.1 Autômatos finitos determinísticos

Um autômato finito determinístico, também chamado de máquina de estados finita determinística (AFD), é definido como uma quíntupla, $M = (Q, \Sigma, s, \delta, F)$, com as seguintes especificações (MARINHO, 2013):

a) Q é o conjunto finito de estados da máquina M;
b) Σ é o alfabeto de entrada de M, onde um dispositivo de leitura de símbolos deste alfabeto possui uma cabeça que desloca-se para a próxima posição, após ler um símbolo σ;
c) s é o estado inicial de M;
d) $\delta: Q\ x\ \Sigma\ \mapsto Q$ é a função de transição de M, que leva o par (q, σ) no estado $p\ =\ \delta(q, \sigma)$;
e) $F \subseteq Q$ é o conjunto de estados de aceitação de M, de modo que, se a cadeia em análise finalizar no estado $q_F\ \in F$, então essa cadeia pertence à linguagem aceita pela máquina M. A coleção de todas as cadeias aceitas constitui a linguagem aceita pela máquina.

A partir do estado inicial, têm-se uma sequência de $n - 1$ transições até o estado final pertencente ou não à linguagem. No caso ilustrado pela **Figura 14**, temos três estados S_0, S_1e S_2, com $\Sigma = \{0,1\}$. Para cada estado de M, há uma transição onde, após a leitura de um símbolo, a máquina leva a um outro estado dependendo deste símbolo. Neste exemplo, o estado de aceitação é o mesmo que o estado inicial, onde foi representado por dois círculos.

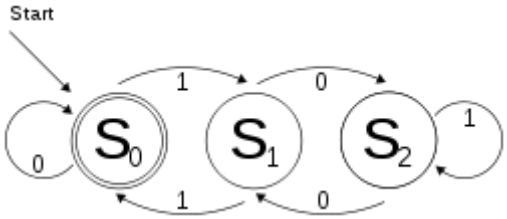

Figura 14 - Exemplo de um autômato finito determinístico.
Fonte: https://upload.wikimedia.org/wikipedia/commons/thumb/9/94/DFA_example_multiplies_of_3.svg/250px-DFA_example_multiplies_of_3.svg.png

4.1.2 Autômatos finitos não determinísticos

Diferentemente dos AFDs, autômatos finitos não determinísticos (AFN) não possuem a obrigatoriedade de se ter transições para todos os pares (q, σ), ou seja, a condição de parada agora ocorre também se não houver transição de determinado estado para a leitura de dado símbolo. Define-se um AFN como sendo a máquina $M = (Q, \Sigma, s, \Delta, F)$ com as seguintes especificações (MARINHO, 2013):

a) Q é o conjunto finito de estados da máquina M;
b) Σ é o alfabeto de entrada de M;
c) s é o estado inicial de M;
d) $\Delta \subseteq Q\ x\ \Sigma\ x\ Q\ \cup Q\ x\ \{\varepsilon\}\ x\ Q$ é a relação de transição de M, que leva o par (q, σ) na coleção de estados de saída, $p\ =\ \Delta(q, \varepsilon)$, onde ε é a palavra vazia;
e) $F \subseteq Q$ é o conjunto de estados de aceitação de M, de modo que se a cadeia em análise finalizar no estado $q_F\ \in F$, então essa cadeia pertence à linguagem aceita pela máquina M.

4.1.3 Autômatos finitos de pilha

Um autômato de pilha é um autômato finito com uma memória auxiliar na forma de pilha, com operações de empilhamento e desempilhamento nas transições da máquina. Há linguagens que requerem um mecanismo de controle para que, por exemplo, o número de a's seja o mesmo do número de b's, ou seja, é necessário que haja uma memorização de quantos a's foram consumidos para que, posteriormente, a máquina reconheça a mesma quantidade de b's. Como este processo deve ser feito de forma automática, o conceito de pilha foi necessário para reconhecer tais linguagens. Define-se, portanto, um autômato de pilha como sendo uma máquina, $M = (Q, \Sigma, \Gamma, s, z, \partial, F)$, com as seguintes especificações (MARINHO, 2013):

a) Q é o conjunto finito de estados da máquina M;
b) Σ é o alfabeto de entrada de M;
c) Γ é o alfabeto da pilha;
d) s é o estado inicial de M;
e) $z \in \Gamma$ é o símbolo inicial da pilha;
f) $\partial \subseteq Q\ x\ \Sigma\ x\ \Gamma\ x\ Q\ x\ \Gamma^*$ é a relação de transição de M, que leva o terno $(q, \sigma, \gamma) \in Q\ x\ \Sigma\ x\ \Gamma$ a um ou mais pares $(p, u) \in Q\ x\ \Gamma^*$, com $u \in \Gamma^*$ sendo a cadeia de símbolos escritos pela máquina no topo da pilha;
g) $F \subseteq Q$ é o conjunto de estados de aceitação de M.

4.2 Máquina de Turing

Como dito na seção 3, a Máquina de Turing desenvolvida em 1936 deu início à ciência da computação moderna. Uma Máquina de Turing nada mais é do que uma generalização dos autômatos finitos, onde possui uma fita de entrada cuja cabeça de leitura e escrita pode avançar tanto para a direita quanto para a esquerda. A cada transição, a cabeça lê um símbolo e sobrescreve outro, conforme a função de transição.

Podemos definir uma máquina de Turing como sendo a máquina $M = (Q, \Sigma, \Gamma, s, \text{b}, \delta, F)$, com as seguintes especificações:

a) Q é o conjunto finito de estados da máquina M;
b) Σ é o alfabeto de símbolos de entrada da máquina;
c) Γ é o alfabeto de fita;
d) s é o estado inicial de M;
e) $\text{b} \in \Gamma$ é o símbolo branco, ou apagamento da fita;
f) $\delta \subseteq Q \times \Gamma \times Q \times \Gamma \times \{L, R\}$ é uma função parcial de transição de M, onde a cabeça pode ir para a esquerda (L) ou para a direita (R);
g) $F \subseteq Q$ é o conjunto de estados de aceitação de M.

Para a máquina de Turing, δ é dita função parcial de transição pelo fato de nem todas as entradas dela terem necessariamente uma transição (MARINHO, 2013).

4.3 Autômatos finitos quânticos

Para estudarmos a computabilidade quântica, é de grande valia iniciarmos com a generalização de linguagens regulares e seus reconhecedores (autômatos finitos) para o caso quântico.

Segundo Cristopher Moore e James P. Crutchfield (C. & P., 1997) (protocolo MC97, daqui em diante), afim de manter a forma probabilística dos observáveis (Capítulo 2), podemos generalizar uma linguagem regular quântica L como sendo uma função probabilística, $\chi_L: \Sigma^* \mapsto [0,1]$, onde:

$$0 \leq \chi_L(w) \leq 1, \tag{52}$$

sendo $w \in \Sigma^*$ a cadeia de entrada, cujo grau de pertinência $\chi_L(w)$ à linguagem regular L é a probabilidade de se encontrar esta palavra em L. Se esta probabilidade é zero, então essa cadeia de caracteres não pertence à linguagem. Por outro lado, se esta probabilidade é 1, então é 100% certo de esta cadeia de entrada pertencer à linguagem quântica. Portanto, o conceito de linguagem quântica definido por MC97 é nebuloso (fuzzy).

Conforme o modelo MC97 de reconhecimento quântico de uma cadeia regular de caracteres, um autômato finito quântico M, é uma quíntupla da forma:

$$M = \left(H, \Sigma, \widehat{U}_{\Sigma}, |s\rangle, F\right), \tag{53}$$

onde:

h) H é o espaço de Hilbert dos estados quânticos, $|q\rangle$, de máquina;
i) Σ é o alfabeto de símbolos de entrada de M, cujas concatenações formam a cadeia de símbolos que devem ser verificadas na forma de medida $\chi_L(w)$ do grau de pertinência à linguagem regular quântica L;
j) $\widehat{U}_{\Sigma}$ é o conjunto de transições unitárias associadas aos símbolos de Σ;
k) $|s\rangle \in H$ é o estado inicial de M;
l) $F \subseteq H$ é o espaço de Hilbert de aceitação, cujo projetor é utilizado para realizar a medida do resultado

No caso clássico, um autômato finito determinístico pode ser representado por um grafo, onde os nodos são os estados de máquina e as conexões são as transições de um estado para outro, dependendo do símbolo que vier. Para o caso quântico, como descrito na quíntupla acima, é um pouco diferente. Primeiramente, o fato de ser no espaço de Hilbert nos dá a dimensão necessária para trabalharmos com sistemas complexos, o que é fundamental para a mecânica quântica. Outra diferença, é que não temos a transição de um estado para outro, e sim matrizes de transição que operam ou não a partir do estado inicial até o espaço de aceitação. É importante frisar que existe um erro a interpretar para considerarmos uma linguagem como aceita ou recusada.

Podemos definir, portanto, uma linguagem quântica reconhecida por M como sendo a função:

$$f_M(w) = \left| |q_{init}\rangle \widehat{U}_{\Sigma} F \right|^2. \tag{54}$$

Considerando $w = \sigma_1 \sigma_2 \ldots \sigma_{|máx|}$, onde σ_j são os símbolos do alfabeto Σ, cada um deles com m símbolos. Este autômato pode ser representado graficamente pela **Figura 15**, onde as portas quânticas $\widehat{U}$ são controladas por estados quânticos puros, $|\sigma_j\rangle$ de dimensão 2^m, rotulados por símbolos do alfabeto. No caso do código ASCII, $m = 8$, teríamos uma base com 256 estados puros, resultantes do produto tensor entre 8 qubits.

Ainda com base na **Figura 15**, os estados quânticos de máquina, $|q\rangle$, são oriundos do produto tensor entre n qubits, onde n é grande o suficiente para realizar todas as transições necessárias para definir o autômato quântico.

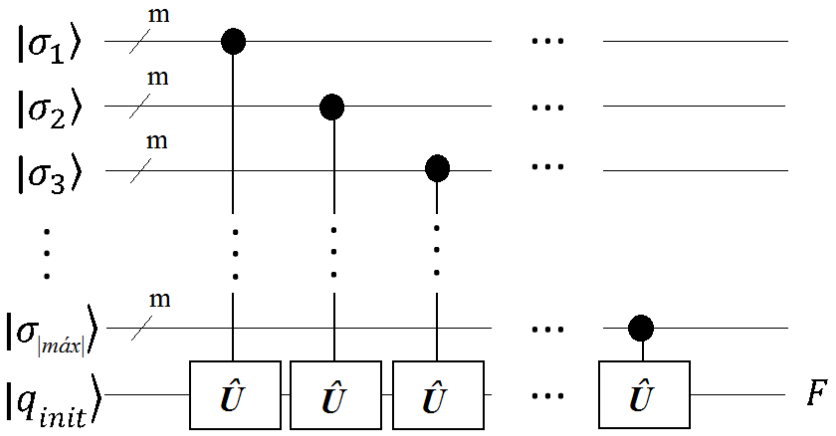

Figura 15 - Representação do autômato finito determinístico quântico.

Esse circuito simula, através de portas $\hat{U}$, um autômato cuja palavra ou sentença w já está definida anteriormente. Cada símbolo $|\sigma_j\rangle$ passa por uma matriz de transição $\hat{U}_j$ e, a partir do estado inicial seguido pelo produto das matrizes, obtemos uma probabilidade pertencente ao estado de aceitação F desta palavra pertencer ou não àquela linguagem.

Este modelo é generalizado, onde é aceito uma linguagem regular, mas não tendo garantia de aceitar linguagens regulares quânticas. Isto deve-se ao fato de que as matrizes de transição não são necessariamente unitárias e a norma do estado inicial não é necessariamente 1 (por ser uma função probabilística, esta regra deve ser seguida).

Attila Kondacs e John Watrous (KONDACS & WATROUS, 1997) propõem uma outra forma de autômato. Agora, ao invés de termos apenas uma projeção que indicará se a linguagem foi aceita ou não, teremos uma projeção para cada símbolo lido. Para melhor entendermos, considere a seguinte sêxtupla:

$$M = \left(Q, \Sigma, \delta, |q_0\rangle, Q_{acc}, Q_{rej}\right), \tag{55}$$

onde:

1. Q é um conjunto de estados finitos;
2. Σ é o alfabeto de entrada;
3. δ é a função de transição $\delta: Qx\Gamma xQx\{-1,0,1\} \rightarrow \mathbb{C}$, onde Γ é o alfabeto da fita e $\{-1,0,1\}$ indica a direção da leitura;
4. $|q_0\rangle$ é o estado inicial pertencente a Q;
5. Q_{acc} é o conjunto de estados de aceitação pertencente a Q;
6. Q_{rej} é o conjunto de estados de rejeição pertencente a Q.

Algumas características adicionais são propostas nesta definição. É conveniente, por exemplo, adicionarmos 2 símbolos ¢ e $ ∈ Σ, que serão utilizados para marcar o fim da string tanto pelo lado direito quanto pelo lado esquerdo, sendo o alfabeto da fita $\Gamma = \Sigma \cup \{¢, \$\}$. Outra diferença, é com o intuito de limitar a ida do leitor da fita para além das extremidades, considerando-a circular. Agora, ao atingir o limite em um dos lados, o próximo símbolo será o correspondente ao extremo oposto.

Ao contrário do autômato definido por Moore e Crutchfield, temos um operador diferente para cada uma das transições δ. Em outras palavras, não teremos uma projeção que estará ou não no espaço de aceitação, e sim uma superposição de observáveis resultante das projeções de cada transição nos estados de aceitação e rejeição (KONDACS & WATROUS, 1997).

4.4 Máquinas de Turing Quânticas

A máquina descrita por Deutsch, como citado na seção 3.5.2, consiste de dois componentes: um processador finito, $\hat{n}_i$, com $i \in \mathbb{Z}_M$, sendo M o número de qubits, e uma memória infinita, $\hat{m}_i$, com $i \in \mathbb{Z}$. Nos referiremos neste texto simplesmente como $\hat{\boldsymbol{n}}$ e $\hat{\boldsymbol{m}}$. Dessa memória infinita, apenas uma parte é utilizada a cada passo do processamento do computador. Além disso, temos que ter uma cabeça móvel para a fita quântica, a qual representará o endereço atual nesta fita. A chamaremos de $\hat{x}$. Esse cabeçote é capaz de mover-se tanto para a direita quanto para a esquerda.

A princípio, o estado quântico $|\psi\rangle$ iniciará no tempo t=0, portanto x e $\boldsymbol{n}$ são preparados com o valor zero:

$$|\psi(0)\rangle = \Sigma_m \psi_m |0,0,\boldsymbol{m}\rangle, \tag{56}$$

onde $\Sigma_m |\psi_m|^2 = 1$

Q é um vetor unitário no espaço de Hilbert medido pelos autovetores de $\hat{x}$, $\hat{\boldsymbol{n}}$ e $\hat{\boldsymbol{m}}$.

Para simularmos a ida de $\hat{x}$ para qualquer um dos lados, podemos utilizar o conceito de sobreposição visto na seção 2.2, onde o estado pode ir para a direita (+1) ou para a esquerda (-1). Além disto, é preciso limitar para que este passo seja de apenas uma unidade. Sendo assim:

$$\langle \mathrm{x}'; \mathbf{n}'; \mathbf{m}'|U|\mathrm{x}; \mathbf{n}; \mathbf{m}\rangle = \delta_{\hat{x}'}^{x+1} U^{+}(\mathbf{n}', {m'}_x|\mathbf{n}, m_x) + \delta_{\hat{x}'}^{x-1} U^{-}(\mathbf{n}', {m'}_x|\mathbf{n}, m_x). \tag{57}$$

Deutsch sugere a ideia de que, para sabermos que a máquina chegou ao seu estado de aceitação, podemos adicionar um bit interno, $\hat{n}$, que seja setado em 1 quando o programa acabar. Isto é necessário devido à propriedade explicada anteriormente de que o sistema existe virtualmente enquanto não observado. Se observarmos, afetaremos a operação.

Outro propósito que a mecânica quântica necessita, é que o sistema seja reversível, ou seja, deve haver um mapeamento um pra um a partir do estado inicial até o estado final. Bennett (BENNETT, 1973) prova que não é necessário construir explicitamente um modelo computacional que gera a mesma função computável. Uma Máquina de Turing reversível pode ser obtida da seguinte forma:

$$U^{\pm}(\boldsymbol{n}', m'|\mathbf{n}, \mathrm{m}) = \frac{1}{2}\delta_{\mathrm{n}'}^{\boldsymbol{A}(\boldsymbol{n},\mathrm{m})}\delta_{\mathrm{m}'}^{B(\boldsymbol{n},\mathrm{m})}[1 \pm C(\boldsymbol{n}, \mathrm{m})], \tag{58}$$

onde $\boldsymbol{A}: U \longmapsto (\mathbb{Z}_2)^M$ e $B: U \longmapsto \mathbb{Z}_2$, $C: U \times U \longmapsto \{-1,1\}$ é a função de controle da cabeça de leitura/escrita na fita, e U é o espaço dos operadores unitários sobre o espaço de Hilbert associado à máquina de Turing.

Em computação, funções estritas de $\mathbb{Z}$ para $\mathbb{Z}$ geram precisamente as funções recursivas clássicas, devido ao princípio da correspondência de Niels Bohr (BOHR, 1913), onde conceitua a necessidade de colocar em paralelo as realidades clássica e quântica. Partindo do mesmo conceito da porta U_{CN} vista na seção 3.4.1, para cada função recursiva f, existe um programa $\pi(f, a, b)$ que computa a função sobre o conteúdo do slot a e coloca o resultado no slot b (se o mesmo não for inicialmente zero), mantendo o conteúdo do slot a inalterado:

$$\left|\pi(f,a,b), \overset{\text{slot a}}{\overbrace{i}}, \overset{\text{slot b}}{\overbrace{j}}\right\rangle \rightarrow |\pi(f,a,b), i, j \oplus f(i)\rangle. \tag{59}$$

Se o slot b inicialmente não conter zero, a reversibilidade requer que o seu valor antigo seja sobrescrito.

No caso de uma função recursiva bijetora g, existe um programa $\phi(g, a)$ que substitui qualquer inteiro i no slot a por $g(i)$.

Para ambos os casos, as propriedades também são válidas para um computador quântico universal.

5 CONCLUSÃO

Neste trabalho, foi possível sintetizar os principais conceitos sobre a história da computação quântica, desde o surgimento até os fundamentos básicos da mecânica quântica.

Um computador clássico é capaz de simular grandiosos algoritmos com uma rapidez que evolui ano após ano. Mas como é de se esperar, por tratarmos de dispositivos físicos, seus recursos são finitos, como por exemplo a memória, e levam determinado tempo para serem processados. De fato, mesmo com a evolução de pesquisas na área, não há como considerarmos que poderemos obter uma memória infinita ou um tempo de processamento que extrapola até mesmo os fenômenos físicos. Mas é possível, através da mecânica quântica, continuarmos evoluindo.

Como visto em toda a discussão deste trabalho, um algoritmo quântico é capaz de resolver eficientemente e com maior rapidez problemas que no caso clássico são inviáveis. Alguns empecilhos, porém, inviabilizam termos atualmente um computador totalmente quântico. Como obteremos a leitura do estado de aceitação de uma máquina quântica se, ao realizarmos a medição da mesma, alteramos todo o seu estado relativo, interferindo no sistema? Como é possível estruturar fisicamente o movimento do cabeçote de leitura e escrita ao utilizarmos partículas? Como construir circuitos em que a transição da leitura de um símbolo controlará a escrita de outro símbolo? Como utilizar canais perfeitamente isolados para que não haja ruídos indesejáveis? Qual o limite destes canais? Como obter uma memória quântica?

Apesar destas limitações, a área da computação quântica é extremamente promissora. A evolução de algoritmos para resolução de problemas ajudou a desenvolver diversas outras áreas como a criptografia quântica, de modo a permitir a transmissão de informação de forma muito mais segura. Tal feito foi visto, por exemplo, com o problema do teletransporte.

Vale destacar que a computação quântica não é uma substituição de uma tecnologia em vias de esgotamento. Estamos falando de um novo paradigma, que poderá ter consequências não só para a tecnologia, mas para a teoria da informação, ciência da computação, e para a ciência em geral.

Enfim, a busca por uma máquina universal quântica ainda será extensa, mas o resultado obtido irá revolucionar toda uma geração.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERT, A. Z. **A Quantum-Mechanical Automation**. Philosophy of Science, 1987.

ARNOLD, V.I. **Métodos Matemáticos da Mecânica Clássica**. Moscou: Ed. Mir, 1987.

BELL, J. S. **On The Einstein Podlsky Rosen Paradox**. Physics, 1, 1964.

BENIOFF, P. **Quantum Mechanical Models of Turing Machines That Dissipate No Energy**. Physical Review Letters, 1982.

BENNETT, C. H. **Logical Reversibility of Computation**. IBM Journal of Research and Development, 1973.

BOHR, N. **On the Constitution of Atoms and Molecules**. Philosophical Magazine, 1913.

CHESMAN, C.; ANDRÉ, C.; MACÊDO, A. **Física Moderna Experimental e Aplicada**. São Paulo: Editora Livraria da Física, 2004. 1ª edição.

DEUTSCH, D. **Quantum theory, The Church-Turing Principle and the Universal Quantum Computer**. Proceedings of the Royal Society of London, 1985.

DEUTSCH, D.; JOZSA R. **Rapid Solution of Problems by Quantum Computation**. Royal Society, 1992.

DIRAC, P. A. M. **A New Notation for Quantum Mechanics**. St John's College Cambridge, 1939.

EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. **Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?**. Princeton: Institute for Advanced Study, 1935.

FEYNMAN, R. P. **Simulating Physics with Computers**. International Journal of Theoretical Physics, Vol 21, Nos. 6/7, 1981.

GROVER, L. K. **A Fast Quantum Mechanical Algorithm for Database Search**. Bell Labs, 1996.

HADAMARD, J. S. **Résolution d'une question relative aux déterminants**. Bulletin des Sciences Mathématiques, 1893.

HEISENBERG, W. **Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik**. Copenhague, 1927.

HUANG, K. **Statistical Mechanics**. John Wiley & Sons, 1987. 2ª edição.

KONDACS, A.; WATROUS, J. **On the power of quantum finite state automata**. Foundations of Computer Science, 1997.

LIMA, P. C. **Fundamentos de Análise I**. Belo Horizonte: CAED-UFMG, 2013.

MARINHO, E. P. **Notas de Aula de Teoria da Computação: autômatos e linguagens formais**. 2013.

MESSIAH, A. **Quantum Mechanics**. Nova York: John Wiley & Sons, 1961, Vol I.

MOORE C.; CRUTCHFIELD J. P. **Quantum Automata and Quantum Grammars**. Theoretical Computer Science, 1997.

MOTTA, V. S.; CARVALHO, L. M.; MACULAN, N. **Esfera de Bloch: algumas propriedades**. São Paulo: 2005.

NEUMANN, J.V. **Mathematische Grundlagen der Quantenmechanik**. Berlin: J. Springer, 1932.

NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information**. Cambridge: Cambridge University Press, 2000.

OLIVEIRA, I. **Computação Quântica e Informação Quântica**. 2004. Presente em: <http://mesonpi.cat.cbpf.br/e2004/docs/PG5-cqiq.pdf>. Acesso em: 05 set. 2015.

SHOR, P. W. **Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer**. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.

TIPLER, P. **Ótica e Física Moderna**. Rio de Janeiro: Ed. Guanabara Koogan, 1995. Vol. 4.

TURING, A. M. **On Computable Numbers, with an application to the Entscheidungsproblem**. Proceedings of the London Mathematical Society, 1936.

VIANA, R. L. **Teoria dos Grupos**. 2010. Presente em: <http://fisica.ufpr.br/viana/metodos/grupos.pdf>. Acesso em: 29 nov. 2015.