UNIVERSIDADE FEDERAL DO RECÔNCAVO DA BAHIA

CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

CURSO DE BACHARELADO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

COMPUTAÇÃO QUÂNTICA - ALGORITMOS QUÂNTICOS

ORLANDO DOS SANTOS CONCEIÇÃO JÚNIOR

Trabalho de Conclusão de Curso

Cruz das Almas/BA

2016

ORLANDO DOS SANTOS CONCEIÇÃO JÚNIOR

COMPUTAÇÃO QUÂNTICA - ALGORITMOS QUÂNTICOS

Trabalho de Conclusão de Curso apresentado à Banca Examinadora da Universidade Federal do Recôncavo da Bahia como requisito parcial para obtenção de título em bacharel em Ciências Exatas e Tecnológicas.
Professor Orientador: Jilvan LM.

Cruz das Almas/BA

2016

ORLANDO DOS SANTOS CONCEIÇÃO JÚNIOR

COMPUTAÇÃO QUÂNTICA - ALGORITMOS QUÂNTICOS

Trabalho de Conclusão de Curso apresentado à Banca Examinadora da Universidade Federal do Recôncavo da Bahia como requisito parcial para obtenção de título em bacharel em Ciências Exatas e Tecnológicas.

APROVADA PELA **COMISSÃO EXAMINADORA**
EM CRUZ DAS ALMAS, **12 DE AGOSTO DE 2016**

Prof. Dr. Jilvan LM, (UFRB/BA)
Orientador

Prof. Dr. Kilder Leite Ribeiro, (UFRB/BA)
Examinador

Prof. Ms. Yuri Tavares dos Passos, (UFRB/BA)
Examinador

Dedicado a minha família, amigos e mestres.

AGRADECIMENTOS

Sou grato a Deus, que tem me dado inspiração para continuar meus estudos e realizar meus sonhos. De forma muito especial quero agradecer aos meus pais, que munidos de humildade e simplicidade sempre zelaram pela minha educação e lutaram para ajudar seus filhos a terem sucesso e principalmente por compreenderem o motivo pelo qual me fiz ausente em inúmeras ocasiões. Aos meus irmãos, pessoas pelas quais tenho um apreço imenso e que sempre apoiaram minhas escolhas em especial a Letícia Conceição que me inspirou desde o ensino médio ao lado dos professores do colégio João Durval Carneiro dos quais não posso esquecer de agradecer pela contribuição de Félix, Cláudio, Elesbão, Ronaldo Fiúza e Rita Guedes. A todos meus amigos que de certa forma já fazem parte da minha vida. Em especial aos "bróders" Breno Prazeres e Joshua Gandhi pelas perguntas, acolhimento e pela marabilíssima amizade. Também não posso esquecer de Guilherme Jaqueira, Silene Costa, Daniele do Anjos, Uiliam Santana, Luciano Santos, Biancha Sabino, Meg Nadine e Celina Bahule esta galera é de fato companhia para toda hora. Agradeço imensamente a Dorenice (Dóra), Renato (Tiquila) e a minha vó Maria que na minha necessidade concederam o aconchego do seu lar e outros recursos sem êxitar. Também quero agradecer às meninas da Pro Reitoria de Políticas Afirmativas e Assuntos Estudantis (PROPAAE) em especial a Luciane (Ane), grande conselheira que ouviu alguns dos meus momentos de angústia e soube acalmar meu desassussego. Aos professores da graduação, são tantos mas sem os conselhos de João Cláudio e Alex Santana concerteza eu não estaria aqui. A Jilvan LM pela orientação, paciência e por ter se disponibilzado a ler a primeira versão deste trabalho e me ajudar melhorá-lo para um texto apresentável. Agradeço ainda pelas vezes que ele foi para além de seu papel como orientador. A UFRB por oferecer para cada estudante a estrutura que permite desenvolver-se como pesquisador. Aos funcionários do Centro de Ciências Exatas e Tecnológicas da UFRB, que sempre nos ajudam nas tarefas burocráticas. A Fapesb por ter concedido a bolsa e criar programas que influenciam ao desenvolvimento da ciência, sem esta ajuda este trabalho teria sido muito mais difícil de ser concretizado.

"Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível"

(CHARLES CHAPLIN)

COMPUTAÇÃO QUÂNTICA - ALGORITMOS QUÂNTICOS/ ORLANDO DOS SANTOS CONCEIÇÃO JÚNIOR. – Cruz das Almas/BA, 2016-
54 p.

Orientador: Jilvan LM

CONCEIÇÃO JÚNIOR, O. S.

Trabalho de Conclusão de Curso – UNIVERSIDADE FEDERAL DO RECÔNCAVO DA BAHIA
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
CURSO DE BACHARELADO DE CIÊNCIAS EXATAS E TECNOLÓGICAS , 2016.

1. Algoritmos Quânticos. 2. Mecânica Quântica. 2. Computação Quântica.

RESUMO

Os computadores e as facilidades que eles trazem estão cada vez mais presentes no nosso dia-a-dia. Mesmo assim, existem propostas para melhorar ainda mais a performance de tais equipamentos através da criação de novos materiais que, entre muitos objetivos, evitem perda de energia da forma que os equipamentos tradicionais o fazem. Outras propostas consistem em construir equipamentos que executem as tarefas que os tradicionais já executam com muito mais eficiência. Uma dessas propostas é a Computação Quântica. Nesse trabalho é feita uma revisão da base conceitual, tanto matemática quanto física, da computação quântica. Área da ciência que vem se desenvolvendo e tem como característica principal, o uso da propriedade quântica chamada de paralelismo quântico. Este por sua vez, consiste na evolução do estado quântico do sistema por todos os possíveis auto estados simultaneamente. Será apresentado também, os algoritmos quânticos mais conhecidos: função, funcionamento e aplicações. Será dada uma atenção especial ao algoritmo de busca conhecido por, algoritmo de Grover.

Palavras-chave: Algoritmos Quânticos. Mecânica Quântica. Computação Quântica.

ABSTRACT

Computers and the facilities that they bring are increasingly present in our daily. Even so, there are proposals to further improve the performance of such equipment by creating new materials, among many purposes, to avoid loss of energy in the way that traditional devices do. Other proposals are to build equipment that perform the tasks that traditional already perform much more efficiently, one of these proposals is the Quantum Computation. In this work will be presented the conceptual basis, both mathematical and physical, of this proposal. And yet, it will be presented the best known quantum algorithms: function, operation and applications.

Key-words: Quantum Algorithms. Quantum Mechanics. Quantum Computing.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A máquina de Turing criada na primeira metade do século XX e a teoria da informação de Shanon, como conta (SARAIVA; ARGIMON, 2007) propiciou a *Von Neumann* os primeiros passos para a construção do computador tal como se conhece ou seja, aquele que faz a distinção entre parte física e parte programável. Como explica (ALEGRETTI, 2004), um computador de *Von Neumann* é organizado em memória e métodos de processamento. Essa é a característica principal desta arquitetura, pois possibilita ao computador tudo que está associado a ele, além de ser responsável pela eficiência obtida nestas máquinas.

O computador foi idealizado e em seguida aperfeiçoado, em um contexto de corridas políticas como guerras e disputas econômicas das quais experimenta-se atualmente em pequena escala. Naquela época, o advento da tecnologia da informação foi considerada a terceira revolução tecnológica pela qual a humanidade passava; havia a necessidade de que as máquinas operassem mais depressa e este era um fator preponderante para alcançar os resultados desejados.

Tal tecnologia tem propiciado até hoje, avanços nas relações diplomáticas entre nações, economia, agricultura, segurança e melhorado a precisão dos diagnósticos médicos além de nos dar uma noção de fenômenos pertinentes aos padrões da natureza e do universo. Sua aplicação se tornou vasta. Hoje as pessoas usam celulares, smartfones, computadores e uma gama de dispositivos eletrônicos para criar e trafegar dados por meio das redes que lhe estão disponíveis. É difícil sair a algum centro urbano a qualquer hora do dia, e não deparar-se com usuários portando diversos tipos de aparelhos eletrônicos bem como um tráfego intenso de dados.

É graças ao emprego de algoritmos que estas tarefas são executadas nos mais diversos dispositivos eletrônicos. Um algoritmo pode ser entendido como uma sequência lógica que resolve um problema e gera um resultado bem definido, como explicado por (FORBELLONE; EBERSPACHER, 2005). São muito utilizados em computadores, uma vez que as rotinas extensas de execução de uma mesma tarefa pelo hardware são requisitadas diversas vezes. Com isto, entende-se que a performance de um computador está relacionada ao quão rápido um algoritmo consegue ser para alcançar o objetivo. Isto inevitavelmente faz com que a eficiência das máquinas esteja nos softwares criados pelos desenvolvedores dos mesmos. Além disso, como explica (ALEGRETTI, 2004) este pode ser um fator preponderante à ausência, de soluções para problemas de criptografia, Inteligência Artificial bem como, o motivo para os computadores atuais não serem utilizados para fatoração de números com mais de 1024 bits.

É fato que o contexto corriqueiro ao qual a sociedade moderna vive acarretou mudanças significativas aos computadores se comparado com os primeiros criados (veja a figura 1). Não obstante, (ALEGRETTI, 2004) explica que ouve apenas uma evolução na velocidade com que as informações são processadas e nunca, um computador mais poderoso que o XT; uma vez que

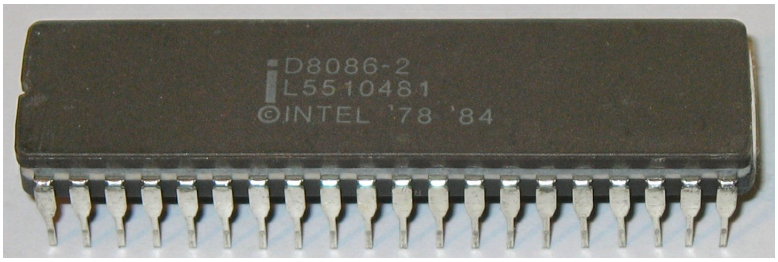
tudo que os processadores atuais fazem o primeiro computador pessoal da IBM já fazia. A figura

Figura 1 – XT - Primeiro computador pessoal da IBM

Fonte: Wikimedia - Disponível em: https://commons.wikimedia.org/w/index.php?curid=623707

abaixo (2) é um microprocessador de 16 bits da Intel, funcionava no XT como a Unidade Central de Processamento, hoje conhecida como CPU.

Figura 2 – Chip 8086 - CPU do XT, faixa dos 5 MHz

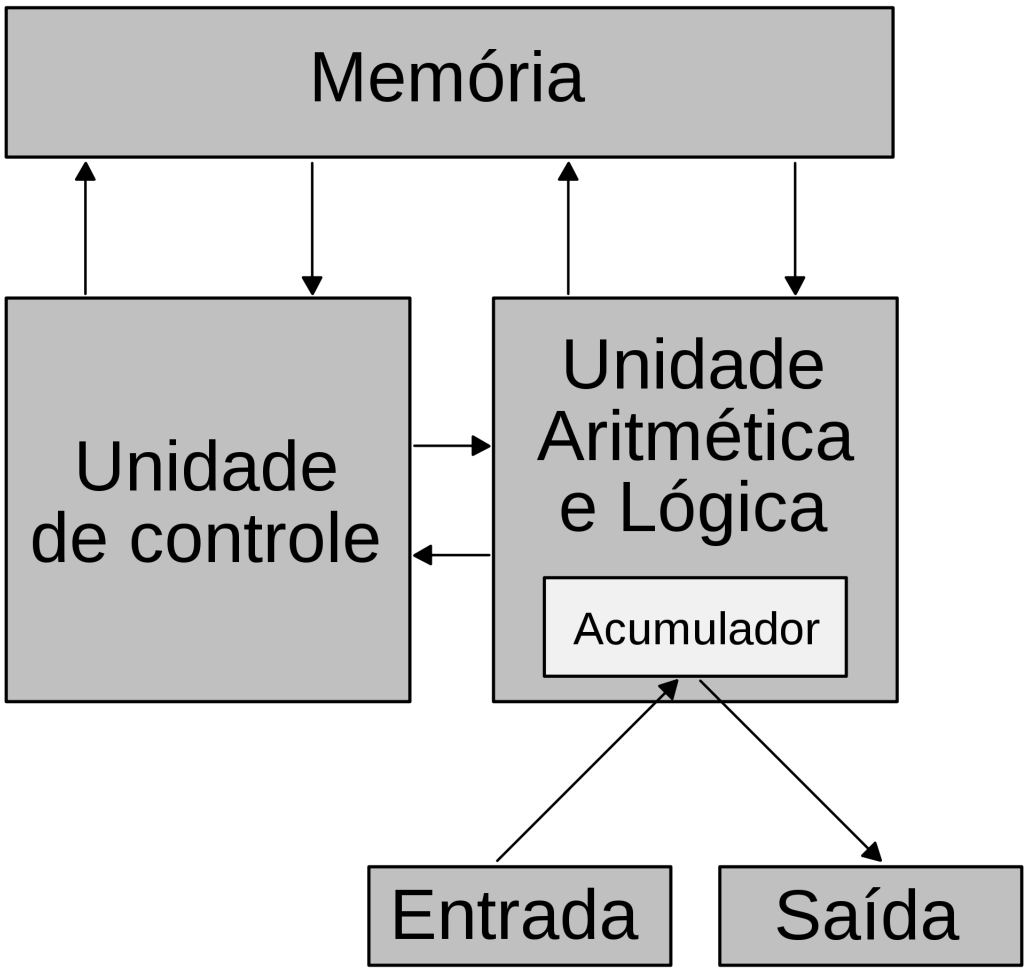


Fonte: Wikimedia - Disponível em: https://commons.wikimedia.org/w/index.php?curid=97778

Ainda segundo o mesmo autor, é a arquitetura de *Von Neumann* que impõe certas limitações as máquinas atuais, sendo necessário a descoberta de uma nova forma de computação no sentido de que possa remover as limitações que a arquitetura atual (ver figura 3) impõe.

Existem propostas para a construção de tecnologias que até então, aparentam ser mais eficientes em termos de consumo de energia e também, velocidade de processamento para que a

Figura 3 – Arquitetura de Von Neumann



Fonte: Wikimedia - Disponível em: http://commons.wikimedia.org/wiki/File:Von_Neumann_architecture.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=5537926

execução de tarefas como a criptografia, serviços de busca e confidencialidade no transporte de informação sejam realizadas de maneira mais efetiva. Uma destas propostas é a Computação e Informação Quântica.

A Computação e a Informação Quântica podem ser entendidas como, o estudo de tarefas que podem ser executadas valendo-se do processamento de informações contidas em sistemas quânticos. De forma mais direta, é uma jovem promessa da Física e é a responsável por estudar métodos que possam caracterizar, armazenar, compactar e usar informações contidas em sistemas tratados sob as leis da Física Quântica. A proposta da mesma, está fundamentada principalmente na Lei de Moore. Esta lei enuncia que a velocidade de processamento de informações por uma CPU, se tornará duas vezes mais rápida a cada um ano e meio para a mesma quantidade de recursos. Embora não defina um limite, essa lei tem se mantido válida desde o surgimento do primeiro microprocessador em 1981. Moore percebeu que a quantidade de transistores por unidade de área, dentro dos processadores aumentava a cada um ano e meio e, empiricamente

formulou sua lei.

A quantidade aproximada de transistores em um processador nos anos 70 eram de apenas 2300 transistores operando a 400 KHz. Atualmente um processador como o da figura 4 chega a possuir mais de 40 milhões de transistores e frequência de operação acima de 3 GHz (ALEGRETTI, 2004).

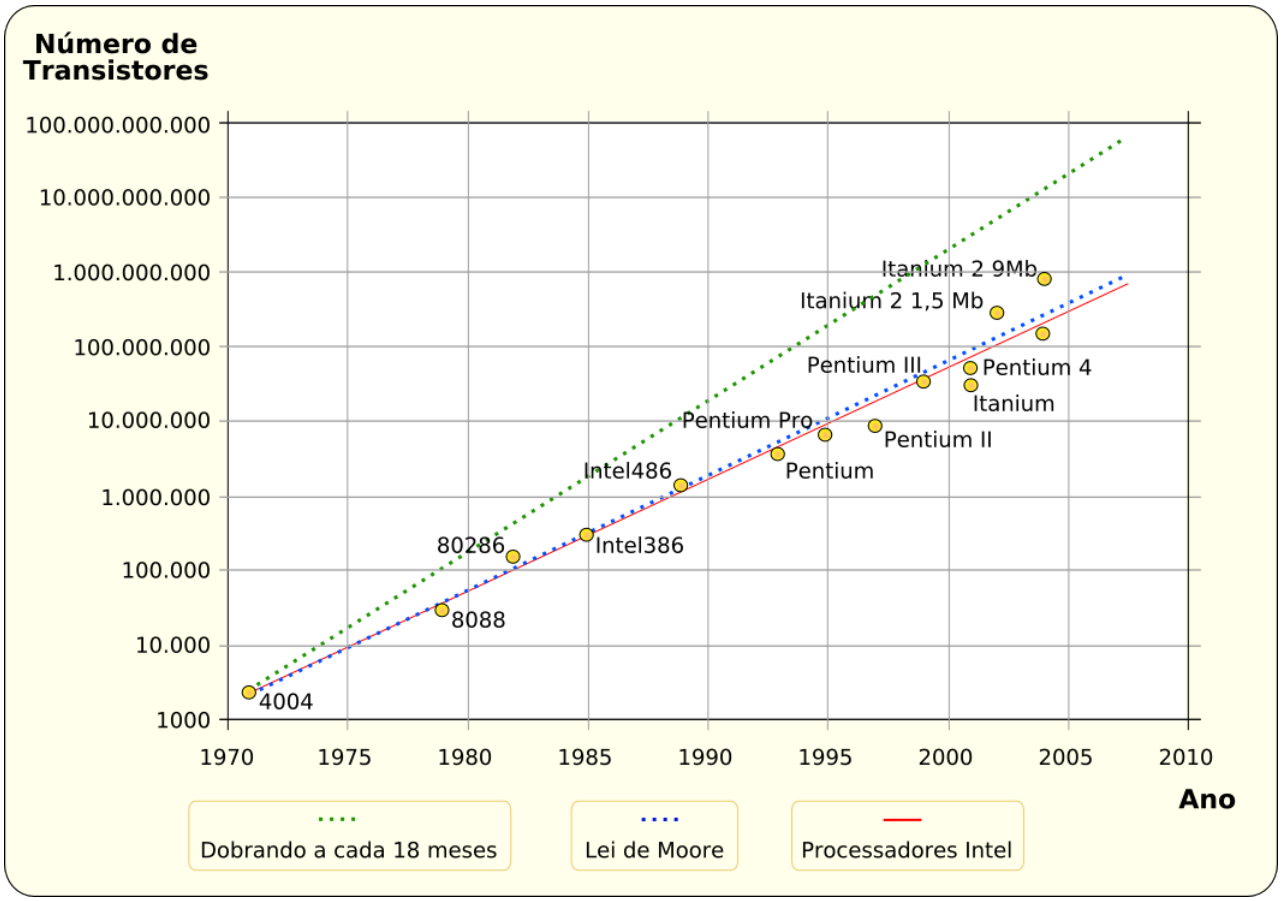
Figura 4 – Chip Intel i7 - 860 cerca de 3 GHz

Fonte: Anandtech - Disponível em :http://images.anandtech.com/reviews/cpu/intel/Corei7/860/chipfront.jpg

Na figura 5 está ilustrada a lei de Moore. É certo que se ela continuar a valer em breve não haverá mais como agrupar tantos transistores por unidade de área sem sofrer os efeitos quânticos do sistema. Por exemplo, a superposição explicada pela metáfora do *gato de Schrodinger* e que pode ser vista no trabalho de (OSVALDO, 2003) que induz ao seguinte raciocínio: após considerar o átomo como transistor, podemos codificar e manipular os dados computacionais através dos estados do átomo. A partir daí, os estados do átomo (as informações computacionais codificadas) evoluirão interagindo com todo o sistema sob as leis da mecânica quântica e nada garante que a informação obtida apos a medida será igual a medida inicial. A questão chave é que um sistema no regime subatômico as leis da Física Clássica deixam de valer.

Em um processador o elétron é um dos agentes fundamentais para o funcionamento. Uma vez que se cria uma diferença de potencial elétrico, ele pode percorrer o circuito fazendo com que se crie ou destrua informações. Mas o elétron possui comportamento dual isto é, pode se comportar como onda e como partícula. Dentro do contexto de que um transistor poderá vir a ter o tamanho de um átomo, sabendo que as leis da Física Clássica são limitadas para regimes

Figura 5 – Lei de Moore



Fonte: Wikimedia - Disponível em: https://commons.wikimedia.org/w/index.php?curid=898084

subatômicos e conhecendo o modelo atômico atual que é o modelo quântico; entende-se que caberá a mecânica quântica descrever um sistema como este. Ela é dotada de um arcabouço que dá conta da descrição do comportamento probabilístico partículas subatômicas ou ainda da ideia de superposição (que será explicada mais para frente). Portanto, para não impedir o avanço da tecnologia e permitir o advento de outra revolução tecnológica, será necessário a adesão de uma nova forma de computação - a Computação Quântica. Portanto, ela é tópico principal deste trabalho.

1.1 JUSTIFICATIVA

A forma de computação atual se mostra eficiente para situações simples do dia-a-dia como escrever textos, criar planilhas, e algumas outras aplicações mais abrangentes como editar filmes, simular jogos etc.. Porém, sabe-se que atividades como a fatoração de números, busca em banco de dados e criptografia são exemplos na qual esta eficiência deixa a desejar, pois demandam tempo e recursos demasiados. Somado a lei de Moore, citada acima, este foi um dos

motivos pelo qual nasceu a computação quântica no século passado, e ela vem com a proposta de solucionar em tempo hábil tais problemas. Como a computação quântica, a mecânica quântica é uma área relativamente nova e portanto, faz-se necessário um estudo do conhecimento já desenvolvido acerca do assunto. Isto permitirá que se agregue experiências, que contribuirão para trabalhos futuros na área.

1.1.1 Objetivo geral

Fazer uma revisão bibliográfica acerca da computação quântica e também formalizar o conteúdo sobre os princípios que regem a mesma. Além disso, apresentar alguns dos algorítimos quânticos conhecidos, explanando a física e a matemática por traz dos mesmos, de maneira que se possa construir uma base de conhecimento sólida no que tange a mecânica quântica.

1.1.2 Objetivos específicos

- Fazer um estudo da mecânica quântica em livros e revistas acerca dos princípios que norteiam a mesma, operadores hermitianos, notações mais utilizadas, estados quânticos, princípio da superposição, paralelismo quântico, os seus postulados etc., com o propósito de adquirir o conhecimento básico sobre mecânica quântica.
- Explanar o espaço vetorial em que trabalha a computação quântica e como, as leis da mecânica quântica são utilizadas, bem como as ferramentas que ela utiliza e seus constituintes principais: os bits quânticos (qubits) e sua estrutura, as portas lógicas e seu papel, o uso do produto tensorial na caracterização de muitos qubits e uma descrição de como os postulados atuam.
- Descrever a matemática do algoritmo quântico de Deutsch, de Teleporte e de Grover bem como a ideia que por traz dos mesmos para resolver problemas. Conectando os postulados da mecânica quântica aos algoritmos sempre que necessário.
- Detalhar o algoritmo de Grover e esmiuçar a matemática e os princípios da física que o norteiam. O algoritmo de Grover foi escolhido devido ao fato de, entre os apresentados, possuir um objetivo ambicioso e matemática de fácil compreensão.

1.2 METODOLOGIA

A princípio houve uma explanação da área em questão e suas ramificações por meio de aulas, seminários e filmes. Logo depois foi feito o levantamento de bibliografia, que permitiu conhecer o trabalho de colabores na computação quântica e suas propostas. Esta fase foi de extrema importância pois houve a familiarização com alguns termos e a desmistificação de outros

bem como a percepção da necessidade de estudar as leis da Mecânica Quântica para cumprir o objetivo. Seguiu-se a lógica de começar com o estudo em nível crescente de dificuldade e explanação de conceitos sem desnortear-se dos objetivos do trabalho.

1.3 ESTRUTURA DO TRABALHO

Este trabalho está dividido na forma que segue. No capítulo 2 será enunciado e explicado os postulados da Mecânica Quântica. No capítulo 3 é explanada a base da Computação Quântica, sua definição e a apresentação de seus fundamentos além da base matemática e os conceitos da física necessários para os objetivos deste estudo. No capítulo 4 serão apresentados: o algoritmo de Deutsch, de Teleporte e o de Shor, mostrando seu funcionamento e sua aplicação. Já no capítulo 5 será estudado, de maneira mais aprofundada que os outros algoritmos, o algoritmo de Grover. Por fim virão as conclusões e perspectivas deste trabalho.

2 POSTULADOS DA MECÂNICA QUÂNTICA

A Mecânica Quântica é uma ciência com uma estrutura matemática fundamentada em conceitos físicos, que consegue descrever com grande formalismo eventos, desde o regime subatômico à alguns macroscópicos. Ela representa um dos ramos da Física originada por Erwin Schrödinger e Werner Heisenberg na virada do século XIX para o XX e desenvolvida desde então como explica (BUTKOV, 1988). (CARUSO; OGURI, 2006) explicam ainda que ela surgiu em meio a um alvoroço causado pela emoção de pensar que na Física só haveriam dois problemas em aberto. O primeiro era a *Nuvem de Éter*, que consiste em concepções adotadas para tentar descrever um meio especial para a propagação da luz que não violasse as leis de Maxwell nem a relatividade de Galileu. O segundo, a *radiação do Corpo Negro*, consiste em descrever o comportamento de ondas eletromagnéticas oriundas do Corpo Negro, corpo esse definido como objeto que absorve toda radiação eletromagnética incidida sobre ele, e emite energia em forma de radiação térmica com perfil de radiância relacionada com sua temperatura(ANDRADE, 2013). No início do século passado, estes problemas foram resolvidos e como consequência houve o surgimento de duas novas teorias, Teoria da Relatividade Restrita e Física Quântica, respectivamente. Neste contexto, a Mecânica Quântica emerge então como um dos ramos da Física Quântica e possui uma não trivialidade intrínseca no seu entendimento devido aos postulados que foram definidos por meio dos experimentos. Tais postulados serão abordados neste capítulo e a intenção é dar-lhes uma descrição simples e clara.

2.1 POSTULADO I - DESCRIÇÃO DOS ESTADOS QUÂNTICOS

O estado de qualquer sistema físico é especificado, em cada instante, por um vetor no espaço de Hilbert. Tal vetor, também conhecido como vetor de estado, possui todas as informações necessárias sobre o sistema, além disto a superposição destes vetores também descreve um estado quântico do sistema. O espaço de Hilbert é portanto o espaço vetorial onde a mecânica quântica se desenrola.

O espaço de Hilbert é um espaço vetorial definido em termos do produto interno e que dispensa um número finito de dimensões (vetores na base), como ocorre no espaço de Euclides. Isto permite trabalhar com uma quantidade extensa de vetores linearmente independentes (L.I.) além disto, as coordenadas dos vetores no espaço de Hilbert podem ser representadas por números complexos. Propriedades como estas são muito úteis e nortearão os próximos capítulos, uma vez que a descrição das funções apropriadas para os possíveis estados de sistema físico fica completa.

Na Mecânica Clássica, um vetor no $\Re^3$, é comumente utilizado para descrever a posição de uma partícula em função de um tempo t. Um vetor velocidade genérico por exemplo, $\vec{r}(x, y, z)$

em física clássica, pode ser descrito em termos de uma combinação linear (superposição) de suas componentes, seus estados:

$$\vec{r}(x, y, z) = \dot{x}\hat{i} + \dot{y}\hat{j} + \dot{z}\hat{k}$$

Na Mecânica Quântica, pode ser feita uma analogia a esta maneira de trabalhar, porém alguns significados são diferentes. O comportamento ondulatório e incerto de partículas como fótons e elétrons faz com que se trabalhe com valores de possibilidades para seu estado e consequentemente o de um sistema quântico qualquer como um todo. (PEREIRA et al., 2012) explicam que, um sistema quântico exibe aspectos corpusculares ou ondulatórios e isto depende muito da natureza do experimento, mas nunca ambos os aspectos ao mesmo tempo. O mesmo afirma ainda, que determinar a posição exata de um observável (um elétron, um fóton etc.), implica numa falta de exatidão no valor da grandeza conjugada. Por exemplo, tentar medir a posição no espaço de um elétron implica imediatamente numa impossibilidade grande de determinar o momento linear do mesmo.

Em outras palavras, há uma incerteza associada a medição simultânea de pares de grandezas subatômicas. De forma grosseira; não é possível obter com exatidão duas informações conjugadas (momento e velocidade, posição e tempo) sobre o estado quântico de uma partícula simultaneamente e sim uma probabilidade de obter cada uma. Por exemplo, se os estados $|\psi_1\rangle$, $|\psi_2\rangle$ e $|\psi_3\rangle$ são estados de um sistema físico, então o estado $|\psi\rangle$ correspondente a este sistema, será uma superposição de seus três estados. Matematicamente tem-se:

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle + \alpha_3|\psi_3\rangle.$$

Como explica (ZETTILI, 2009). Para n estados esta notação pode ser expressa de forma mais robusta, escrevendo-a como:

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle + ... + \alpha_n|\psi_n\rangle = \sum_{i=1}^{n} \alpha_i|\psi_i\rangle \tag{2.1}$$

onde o símbolo $|\ \rangle$ é devido notação de Dirac, e α_i são números complexos que representam as amplitudes de possibilidades de cada estado ser obtido em uma observação (uma medida). Vetorialmente são encarados como uma projeção sob o vetor de estados ($|\psi\rangle$), ou ainda como o produto interno $\alpha_i = \langle\psi|\psi_i\rangle$. Estes números devem satisfazer a condição de unitariedade, que está relacionada com uma completude destas possibilidades. Ou seja

$$\sum_{i=1}^{n} |\alpha_i|^2 = 1.$$

A equação 2.1 é a notação matemática para este primeiro postulado. É uma representação de fato robusta pois, no vetor $|\psi\rangle$ estão todas as informações do sistema. Algumas vezes este postulado é lembrado por princípio da superposição. Isto porque a combinação linear de auto estados $|\psi_i\rangle$ do sistema gera um vetor $|\psi\rangle$ no espaço de Hilbert (equação 2.1). Neste caso, cada auto-estado é uma base de $|\psi\rangle$ no espaço de Hilbert. O entendimento deste princípio torna mais fácil a compreensão

de como aje o paralelismo quântico. Sabe-se que este fenômeno físico, muito intrigante, permite que estados quânticos de sistemas no mesmo regime sejam computados simultaneamente. Ele será visto em ação mais adiante e por agora basta entender que esta propriedade quântica permite que todas as possibilidades físicas para um evento em regime subatômico discorram ao mesmo tempo. A grosso modo é como se todos os auto-estados da equação 2.1 fossem avaliados ao mesmo tempo por algum "agente"da mecânica quântica com privilégios para fazer observações.

2.2 POSTULADO II - DESCRIÇÃO QUÂNTICA DE OBSERVÁVEIS

Toda quantidade física observável ou variável dinâmica de um sistema físico possui um operador linear hermitiano correspondente, cujos autovetores formam uma base completa. Neste trabalho, os operadores lineares (hermitianos ou não) estão representados por letras maiúsculas. Um operador hermitiano A é um operador linear igual ao seu adjunto $A^\dagger$. É costume representá-lo desta forma:

$$A^\dagger = (A^*)^T = A.$$

onde A^* representa a conjugação complexa da matriz A e A^T a transposição de A.

Um conceito fundamental à mecânica quântica é o de observável. Um observável, a grosso modo, é um operador hermitiano ao qual pode-se associar uma base ortonormal (L.I.) no espaço de estados que seja formada pelos autovetores do operador. Os operadores hermitianos representam observáveis devido ao fato de sua aplicação em um estado do sistema produzirem autovalores reais como pode ser visto na seção 2.3. Por exemplo, a matriz $N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ é um operador Hermitiano, assim como a matriz $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ pois, satisfazem a condição de serem adjuntas.

2.3 POSTULADO III - MEDIDAS SOBRE ESTADOS QUÂNTICOS

A medida de um observável ou sistema dinâmico X pode ser representada formalmente pela ação do operador hermitiano linear $\hat{X}$ correspondente, sobre o vetor de estados $|\psi\rangle$ do sistema. Tal medida, retorna somente um autovalor x_n associado ao operador $\hat{X}$ e imediatamente após a medida o vetor de estados $|\psi\rangle$ muda para $|\psi_n\rangle$. Matematicamente escreve-se:

$$\hat{X}|\psi_n\rangle = x_n|\psi_n\rangle \tag{2.2}$$

onde $x_n = \langle\psi_n|\psi(\vec{r},t)\rangle$ e é o auto valor de $\hat{X}$ em $|\psi_n\rangle$. Operadores hermitianos são interessantes principalmente, pelo fato de representarem um observável, ou seja; sua aplicação em um vetor de estados $|\psi\rangle$ retorna uma quantidade física mensurável - um autovalor como discutido na seção anterior. A matriz N que foi citada, serve como exemplo. Nisto, a aplicação de N em

um estado $|\psi\rangle$ resulta em: $N|\psi_i\rangle = n_i|\psi_i\rangle \Rightarrow N|\psi_i\rangle - n_i|\psi_i\rangle = 0 \Rightarrow (N - n_iI)|\psi\rangle = 0 \Rightarrow det(N - n_iI) = 0$

ou seja,

$det\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} n_i & 0 \\ 0 & n_i \end{pmatrix}\right] = 0 \Rightarrow {n_i}^2 - 1 = 0 \Rightarrow n_i = \pm 1$. Portanto, $n_i = \pm 1$ são os autovalores associados ao observável que o operador hermitiano N representa. Para saber quem são os autovetores que formam a base no espaço de estados, basta prosseguir com as contas utilizando os autovalores encontrados (1 e -1) daí: $N|\psi_1\rangle = n_1|\psi_1\rangle = N|\psi_1\rangle = (1)|\psi_1\rangle \Rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} = (1)\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}$

que fornece $\alpha_1 = \beta_1$ e portanto

$|\psi_1\rangle = \alpha_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Procedendo de maneira análoga para $n_2 = -1$ obtem-se:

$|\psi_2\rangle = \alpha_2 \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

As matrizes $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ e $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ são os autovetores que formam a base no espaço de estados.

2.4 POSTULADO IV - PROBABILIDADE DE MEDIDA

Uma das características marcantes da Mecânica Quântica é certamente a incerteza associada a obtenção de valores de medida. Isto porque em termos físicos, uma partícula subatômica, pode assumir muitos estados quânticos antes que algum agente exteno venha interferir em seu estado. Por exemplo, a maneira mais coerente de definir a posição de um elétron livre dentro de uma sala, é afirmar que ele está em todos os locais da mesma ao mesmo tempo. Mas, há a necessidade de saber por exemplo, qual a probabilidade de ele estar em um dos cantos inferiores da sala? Ou ainda, com qual probabilidade ele colidirá com a parede da sala defletido de um sexto de circunferência? As perguntas podem ser muitas. O fato é que conhecendo as leis que regem o sistema em questão perguntas de probabilidade relacionadas a características do evento podem ser respondidas. Este postulado portanto, cumpre o papel de ensinar como obter estas probabilidades e ele se vale de algo muito familiar e intrínseco ao princípio da superposição que são, as amplitudes de probabilidades que cada auto-estado carrega consigo.

Ele enuncia que a probabilidade de obter um valor específico de medida x_n associada a um estado $|\psi_n\rangle$ é o módulo quadrado da amplitude de probabilidade (α_n) relacionada a este estado, como pode ser visto no trabalho de (PELEG; PNINI; ZAARUR, 1998) e (ZETTILI,

2009). A amplitude de probabilidade é dada pelo produto interno de tal estado, com o auto-estado correspondente ao determinado valor da medida analisado. Então para um sistema isolado que obedece ao princípio da superposição (equação 2.1) isto é,

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |\psi_i\rangle.$$

Então, a probabilidade $P(x_n)$ de encontrar o estado $|\psi_i\rangle$, é o módulo quadrado da amplitude de probabilidade associada a este auto-estado. Formalmente:

$$P(x_n) = \frac{|\langle\psi_n|\psi\rangle|^2}{\langle\psi|\psi\rangle} = \frac{|\alpha_n|^2}{\langle\psi|\psi\rangle} \tag{2.3}$$

onde $\langle\psi|\psi\rangle = 1$ é o produto interno. Portanto, $P(x_n) = |\alpha_n|^2$.

Desta forma, o ato de efetuar uma medida, altera o estado de um sistema de $|\psi\rangle$ para $|\psi_i\rangle$ obedecendo a relação:

$$\hat{X}|\psi_n\rangle = x_n|\psi_n\rangle$$

onde $\hat{X}$ é um operador hermitiano que representa o observável, e x_n é o auto valor de $\hat{X}$ na base $|\psi_n\rangle$. Do quarto postulado, chegar-se-a a conclusão de que a probabilidade de obter $|\psi_n\rangle$ é o módulo quadrado de α_n.

A beleza deste postulado reside no fato de que, ainda que a mecânica quântica esteja de encontro a ideia determinística da mecânica clássica, há como determinar a possibilidade de prever um possível estado para um sistema dinâmico quando uma medida for efetuada.

2.5 POSTULADO V - EVOLUÇÃO COM O TEMPO

A evolução com o tempo de um vetor de estados $|\psi(\vec{r},t)\rangle$ de um sistema é governado pela equação de Schrodinger:

$$i\hbar\frac{\partial}{\partial t}|\psi(\vec{r},t)\rangle = \hat{H}|\psi(\vec{r},t)\rangle \tag{2.4}$$

onde $\hat{H}$ representa o hamiltoniano do sistema ou seja, é o operador relacionado com a energia total do mesmo.

Para sistemas onde o hamiltoniano não possui dependência temporal, ou, em outras palavras, a energia se conserva $\left(\frac{\partial}{\partial t}H = 0\right)$, a equação característica se resume a um problema de auto valor. Daí $|\psi(\vec{r},t)\rangle = A(t)|\psi(\vec{r},0)\rangle$ onde $A(t) = e^{-i\alpha t}$ é um auto valor, "i"é um número complexo e "α"uma constante.

2.6 POSTULADO VI - SISTEMAS COMPOSTOS

De acordo com (AMARAL, 2008), alguns eventos decorridos em sistemas quânticos fazem um forte apelo para a presença de dois ou mais vetores de estados unidos no espaço

de Hilbert, isto significa que sistemas deste tipo comportam-se como um sistema composto e portanto, se faz necessário uma abordagem mais rebuscada para descrevê-lo, uma vez que toda a informação do sistema está nos dois vetores de estados. Sejam dois vetores de estados $|\psi\rangle$ e $|\varphi\rangle$ tais que:

$$|\psi\rangle = \sum_{k=1}^{n} \alpha_k |\psi_k\rangle$$

e

$$|\varphi\rangle = \sum_{j=1}^{m} \beta_j |\varphi_j\rangle$$

O espaço de Hilbert $|\chi\rangle$ associado ao sistema composto $|\psi\rangle|\varphi\rangle$, é o produto tensorial dos espaços de Hilbert associados aos sistemas simples $|\psi\rangle$ e $|\varphi\rangle$. Em outras palavras

$$|\chi\rangle = |\psi\rangle \otimes |\varphi\rangle = \begin{bmatrix} \psi_1\varphi_1 \\ \psi_1\varphi_2 \\ \vdots \\ \psi_1\varphi_m \\ \psi_2\varphi_1 \\ \psi_2\varphi_2 \\ \vdots \\ \psi_2\varphi_m \\ \vdots \\ \psi_n\varphi_1 \\ \psi_n\varphi_2 \\ \vdots \\ \psi_n\varphi_m \end{bmatrix} = |\psi\rangle|\varphi\rangle = \alpha_1\beta_1|\psi_1\rangle|\varphi_1\rangle + \alpha_1\beta_2|\psi_1\rangle|\varphi_2\rangle + \cdots + \alpha_n\beta_m|\psi_n\rangle|\varphi_m\rangle$$

$|\chi\rangle$ representa um estado composto, ou seja é o produto tensorial de outros vetores de estados. Segundo (NIELSEN; CHUANG, 2005), sistemas compostos são úteis pelo fato de preservarem todas as informações do sistema físico.

3 COMPUTAÇÃO QUÂNTICA

3.1 CONCEITO

A computação quântica pode ser entendida como o estudo de tarefas que podem ser executadas através da análise de informações contidas em sistemas quânticos. Logo, a ideia é caracterizar, transportar e manipular a informação em meios exclusivamente quânticos. Ela surgiu em meio as limitações que a física clássica impõe à fabricação de componentes eletrônicos em escala atômica, e a dificuldade de se simular sistemas quânticos em um computador clássico. Desde que foi proposta pelo físico norte americano Richard Feynman em 1982, ela passou a ser desenvolvida assiduamente por volta de 1990, quando Lov Grover e Peter Shor chegaram a resultados encorajadores com algoritmos quânticos, estes foram motivados pelos resultados de David Deutsch em 1985 como explicam (NIELSEN; CHUANG, 2005). O algoritmo de busca de Grover e o de fatoração de Shor mostraram-se capazes de resolver problemas impossíveis a qualquer variante da máquina de Turing, alimentando assim a esperança de haver uma forma de computação mais poderosa que a atual.

3.2 CONSTITUINTES BÁSICOS

Analogamente à maneira fundamental de codificar a informação clássica (números binários (o ou 1)), a computação quântica é constituida sobre mesmo conceito, *bit quântico* (qubit). O qubit é um objeto com uma estrutura matemática definida, bem como a mecânica quântica, cuja conexão com um sistema físico real é feita obedecendo-se aos postulados da mecânica quântica.

Um bit clássico pode ser representado pelo estado 0 ou 1, comumente diz-se que um computador usa linguagem binária, pois estes dois estados podem codificar a informação e armazená-la na memória do computador manipulando a base computacional. A tabela abaixo ilustra situações deste tipo.

Tabela 1 – Exemplos de informação codificada em binário

Informação	Informação codificada
5	101
12	1100
"off"	0
"on"	1
"Cara"	0
"Coroa"	1

Fonte: do autor

Desta forma os dois possíveis estados de uma informação num computador clássico é 0

ou 1. Analogamente a um bit clássico, os dois estados possíveis de um qubit são $|0\rangle$ e $|1\rangle$ onde $|\ \rangle$, é a representação de um estado quântico; é a notação de *Dirac* para estados quânticos.

A diferença entre o bit e o qubit é que os qubits podem assumir estados diferentes de $|0\rangle$ ou $|1\rangle$. Para eles é possível formar superposições de estados (combinações lineares) daí um estado quântico genérico $|\psi\rangle$ é representado por:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{3.1}$$

onde α_0 e α_1 representam amplitudes de probabilidade ($|\alpha_0|^2 + |\alpha_1|^2 = 1$) podendo ser iguais ou não, elas pertencem ao espaço vetorial complexo (C^2) de forma que, $|0\rangle$ e $|1\rangle$ são os estados da base computacional portanto são Linearmente Independentes (L.I.).

A ideia de superposição (continuidade) não é comum e pode ser interpretada como se um qubit pudesse guardar até o estado de uma moeda defeituosa e não apenas "cara"ou "coroa". O fato é que eles são reais e até que seja realizado um processo de medida, eles podem assumir muitos estados. Na prática, um qubit pode ser uma partícula de *spins* onde, $|1\rangle = -\frac{1}{2}$ e $|0\rangle = \frac{1}{2}$ ou ainda os feixes de fótons passando por um espelho divisor de feixes (CABRAL; LIMA; JUNIOR, 2004). Uma maneira de enxergar o comportamento do qubit é observar a representação geométrica no R^3 dada pela esfera de *Bloch* (figura 6).

Desta forma, o vetor de estados em computação quântica é o vetor

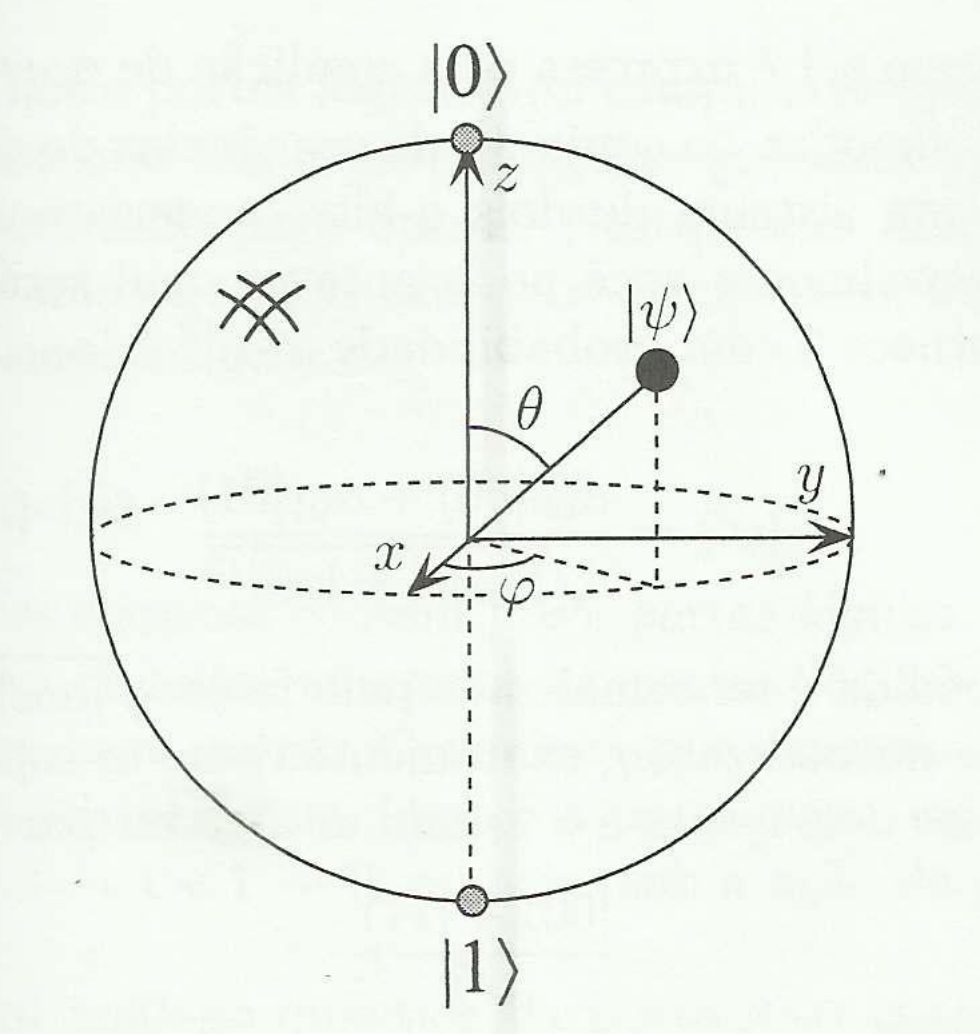
$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{3.2}$$

mas, α_0 e α_1 são números complexos daí vale a relação: $\alpha_0 = x + yi$ e $\alpha_1 = w + zi$ onde $x, y, w, z \in R$ e $i = \sqrt{-1}$; da representação em coordenadas polares para um número complexo vem que $\alpha_0 = |\alpha_0|e^{\gamma i}$ e $\alpha_1 = |\alpha_0|e^{(\gamma+\varphi)i}$ fazendo $|\alpha_0| = \cos(\frac{\theta}{2})$ e $|\alpha_1| = \sin(\frac{\theta}{2})$ segue que
$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
$|\psi\rangle = e^{\gamma i}\cos(\frac{\theta}{2})|0\rangle + e^{(\gamma+\varphi)i}\sin(\frac{\theta}{2})|1\rangle = e^{\gamma i}\left(\cos(\frac{\theta}{2})|0\rangle + e^{\varphi i}\sin(\frac{\theta}{2})|1\rangle\right)$. O fator $e^{\gamma i}$ pode ser suprimido, uma vez que ele não representa uma grandeza física mensurável, ou melhor, ele não possui informações que ajudem a localizar o estado na esfera de Bloch (ver figura 6) portanto não é útil para esta aboradgem e pode ser descartado.

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{\varphi i}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{3.3}$$

Os ângulos θ e φ representam o ponto sobre a esfera unitária, onde está o estado $|\psi\rangle$. Olhando a esfera de *Bloch* pode se pensar que dá para guardar muita informação (muitos estados) em um qubit porém, a mecânica quântica ensina que ao realizar uma medida sobre um qubit, obtêm-se apenas um bit de informação. Por exemplo, na equação 3.2 a probabilidade de obter 0 é de $|\alpha_0|^2$ assim como para 1 é de $|\alpha_1|^2$, o fato é que não dá para realizar uma medida sobre um qubit sem alterá-lo, o que não ocorre com os bits clássicos.

Figura 6 – Esfera de Bloch



Fonte: Nielsen e Chuang

Os estados $|0\rangle$ e $|1\rangle$ são representados pelas matrizes: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ os quais também representam uma base de C^2. Os computadores clássicos são constituídos por fios e portas lógicas clássicas, bem como registradores de n bits que podem armazenar até 2^n números diferentes, um de cada vez. Os computadores quânticos seguem a mesma ideia, no entanto com portas lógicas quânticas.

Por exemplo, a porta quântica NÃO é a matriz:

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

cuja primeira linha é a negação da segunda, além disso,

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

e da mesma forma

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Há também a porta lógica quântica Z, dada por

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

Existe outra porta lógica quântica muito importante e útil que é a porta H ou de *Hadamard* em homenagem a seu criador:

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

Esta porta é interessante, ela causa reflexões e rotações do plano dos qubits, como se pode ver na esfera de Bloch na figura 7.

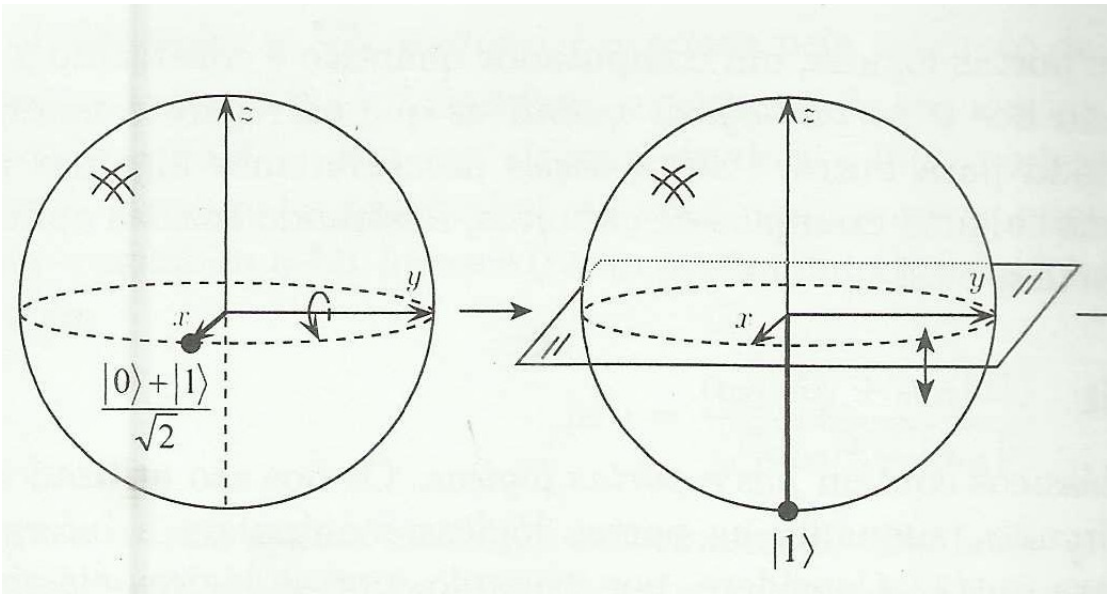
Aplicando H nos auto-estados $|0\rangle$ e $|1\rangle$ respectivamente vem que:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

e

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Figura 7 – Ação do operador de Hadamard



Fonte: Nielsen e Chuang

A interpretação do efeito de H sob os qubits é que este operador cria superposições de estados, figurando assim o comportamento exibido. Estas portas são operadores unitários, importantes para a computação quântica princialmente por permitir a reversibilidade.

Outra porta lógica quântica importante é a porta *C-NOT* ou "Não-controlado"em português. Esta porta se faz importante quando há a necessidade de trabalhar com muitos qubits, ou estados compostos. Em sua entrada vão dois qubits, um de controle e o outro o qubit alvo, se o qubit de controle (o primeiro) é colocado no estado "0"nada acontece, porém se escolhe-se o estado "1"para o qubit de controle então o qubit alvo troca seu estado. (NIELSEN; CHUANG, 2005) salientam que a porta lógica quântica C-NOT é importante para computação quântica, uma vez que dela pode-se derivar qualquer outra porta quântica para estados compostos.

Exemplo de atuação da porta C-NOT:

$|0\rangle|0\rangle \xrightarrow{C-NOT} |0\rangle|0\rangle = |00\rangle$

ou ainda, se trocando o qubit alvo

$|01\rangle \xrightarrow{C-NOT} |0\rangle|1\rangle = |01\rangle$

perceba que nada aconteceu, até porque o qubit de controle está no estado "0", mudando este estado vem que,

$|10\rangle \xrightarrow{C-NOT} = |11\rangle$

e também

$|11\rangle \xrightarrow{C-NOT} |1\rangle|0\rangle = |10\rangle$

e fica visível o efeito da porta sobre o qubit alvo.

A representação abaixo é da porta C-NOT.

$$C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Uma característica importante do operador C_{NOT} é que ele atua exclusivamente em estados que obedeçam também ao sexto postulado (estados compostos seção 2.6). Além disto, ela combinada com o operador de Hadamard (H) atuando sobre um vetor de estados, geram um vetor de estados denominado *estados EPR* em homenagem a Eintein, Podolsky e Rosen ou *estados de Bell*. Esses estados são também conhecidos como estados emaranhados, ou seja, estados que não podem ser fatorados como o produto tensorial de dois outros estados. No caso dos qubits, diz-se que o estado $|01\rangle$ por exemplo, pode ser decomposto como um produto

tensorial. Isto é verídico, uma vez que

$$|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

No entanto, o estado

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |00\rangle + |11\rangle, \tag{3.4}$$

não pode ser escrito como um produto tensorial de outros dois estados. Por causa deste comportamento ele é chamado de estado emaranhado e a maneira proposta por Bell para construí-los (já que é impossível obtê-los por uma fatoração) está enunciada na equação 3.5, logo abaixo.

O estado:

$|00\rangle$ é um estado composto. Primeiro aplica-se H e depois C-NOT logo,

$|00\rangle \ \underrightarrow{H} \ H \otimes |00\rangle = H|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$.

Agora aplica-se C-NOT na superposição de estados causada por H nisto,

$\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \ \underrightarrow{C-NOT} \ \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Com outro estado composto,

$|10\rangle \ \underrightarrow{H} \ = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \ \underrightarrow{H} \ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

No geral, um *estado de Bell* qualquer $|\beta_{xy}\rangle$ obedece a relação:

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x|1, \neg y\rangle}{\sqrt{2}} \tag{3.5}$$

onde $\neg y$ é a negação de y.

Há ainda outro operador importante. Ele é denotado aqui por U_f e quanticamente realiza o papel de uma função f qualquer que computa uma entrada $x_1, x_2, x_3, \cdots, x_n$ e que retorna $f(x_i) = y$. No entanto, um circuito quântico trabalha sob a ação de operadores unitários permitindo assim a reversibilidade isto é, que operações sejam desfeitas e que estados iniciais sejam recuperadoss. Outro fato importante de U_f é que é ele o operador que realiza o efeito do paralelismo quântico sobre o vetor de estados do sistema quântico em estudo. Por enquanto basta saber que U_f é um operador unitário que computa, sob as leis da mecânica quântica, uma função que caracterize matematicamente algum problema. Mais adiante, será visto como se dá sua atuação.

3.3 DIREÇÕES FUTURAS

Embora a Mecânica Quântica seja não-trivial, a física que ela descreve sustenta uma teoria que se diz capaz de quebrar qualquer código gerado pelo RSA rapidamente. Desta forma, senhas bancárias, contas na internet, números de cartões de crédito seriam violados com certa facilidade e rapidez, o que denuncia que a maneira atual de guardar a informação não é a mais segura fazendo-se necessário, o desenvolvimento de tecnicas mais robustas de encriptar a informação. A respeito disto já se pode citar as contribuições do emaranhamento quântico, que permite a estados fortemente ligados a impossibilidade de serem clonados ou observados sem que a informação seja destruída após a observação.

O fato é que a ciência está avançado e conforme isto se dá novas limitações vão surgindo. Nesse ínterin, começam a aparecer outras áreas de estudo e novas considerações vão sendo feitas. A história revela que acontecimentos que revolucionaram a maneira de encarar a Natureza e se fazer ciência decorreram de momentos como este. Por exemplo, a Teoria da Relatividade de Albert Einstein, surgiu em meio ao fato de o eletromagnetismo apontar irregularidades sobre como interpretavam a natureza da luz. A Física Quântica foi fundada mediante um esforço extraordinário de cientistas e outros profissionais, pois as teorias existentes conspiravam para a existência de eventos inconcebíveis como a catástrofe do ultravioleta. Tal teoria se desenvolveu e hoje já exitem explicações mais sólidas desde o interior do Sol até as moléculas de gene dos seres vivos. Avanços na astronomia permitiram que a humanidade entendesse sobre a natureza das estrelas e permitiu o desenvolvimento de métodos mais efetivos de resfriar materiais. Muitos benefícios decorreram da observação de sistemas, e um sistema quântico ainda não foi tão trabalhado e observado, a computação quântica é então uma oportunidade para aprender mais e estudar como sistemas quânticos se comportam e podem ser manipulados.

No próximo capítulo serão mostrados alguns algoritmos quânticos e ficará mais visível de onde vêm o estímulo de desenvolver a computação quântica.

4 ALGORITMOS QUÂNTICOS

Os primeiros passos que denunciaram os benefícios da computação quântica, surgiram com do esforço de cientistas para mostrar os benefícios do paralelismo quântico bem como do princípio da superposição de estados. Os algoritmos abaixo exibem situações onde o uso de tais princípios torna perceptível a eficiência das aplicações.

4.1 ALGORITMO DE DEUTSCH

O algoritmo de Deutsch consiste em saber se uma dada função binária $f : \{0,1\} \rightarrow \{0,1\}$ é constante ou balanceada, calculando a função apenas uma vez. Tarefa semelhante a de verificar se uma moeda é viciada com apenas uma observação. Classicamente isto não é possível devido ao fato de que duas observações nas faces da moeda devem ser feitas, a primeira avalia um lado da moeda e a segunda o outro lado e depois conclui-se se esta é viciada ou não. O Algoritmo de Deutsch dificilmente teria alguma utilidade prática, porém este foi um dos primeiros algoritmos quânticos a revelar o poder que a porta Hadamard (H), o paralelismo quântico e a interferência possuiam para resolver determinados problemas de forma mais eficiente que um computador clássico.

A análise começa com o estado de entrada:

$$|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle.$$

Em seguida, envia-se $|\psi_0\rangle$ através de duas portas Hadamard para criar uma superposição de estados. Duas aplicações do operador H em $|\psi_0\rangle$, é o mesmo que escrever o $HH|\psi_0\rangle = H^{\otimes 2}|\psi_0\rangle$ uma vez que $|\psi_0\rangle$ é um estado composto a aplicação de H nos estados da base resultará em outro estado $|\psi_1\rangle$ tal que,

$$|\psi_1\rangle = H^{\otimes 2}|\psi_0\rangle = H|0\rangle H|1\rangle = |+\rangle|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

onde fica definido como $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Continuando as contas vem que

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\right)^2 (|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) \tag{4.1}$$

Agora vem um ponto importante e que requer atenção; $|\psi_1\rangle$ é uma superposição de estados e é aqui que se aplica a ideia do paralelismo quântico. A autor (SILVA, 2002) discorre sobre o assunto deixando claro que os computadores quânticos oferecem a grande vantagem de fazer cálculos de funções em paralelo, isto é consegue computar ao mesmo tempo, todas as saídas para uma função $f(x) = y$ para as diferentes entradas x. Para esta tarefa é necessário

definir um operador apropriado. Tal operador é o U_f, que para o algoritmo de Deustch é definido como:

$$U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle, \tag{4.2}$$

onde $\oplus$ representa a operação de soma binária. Computadores quânticos permitem operações de reversibilidade devido a unitariedade dos operadores que atuam nos estados da base computacional, esta operação sugere que para uma entrada x em uma função $f(x)$ deve possuir um registrador para guardar também o valor da entrada como explica (CABRAL; LIMA; JUNIOR, 2004). E o operador U_f como foi definido acima, cumpre este papel pois é capaz de avaliar $f(x)$ para todos valores que x puder assumir. Por exemplo, se $f(x) : \{0,1\} \rightarrow \{0,1\}$ então, pela definição de U_f (equação 4.2) retornará como resultado o estado:

$|0\rangle$ se $y = f(x)$ pois $|x\rangle|x \oplus f(x)\rangle = |0\rangle$ e retornará o estado quântico $|1\rangle$ se $y \neq f(x)$. Portanto, a transformação $|x, y\rangle \rightarrow |x\rangle|x \oplus f(x)\rangle$ é coerente para o problema em questão. Para uma abordagem mais detalhada ou conteúdo sobre este tópico, a consulta ao trabalho de (PORTUGAL et al., 2004) é útil.

Agora que U_f foi definido e a ideia do paralelismo quântico foi discutida, cabe voltar ao algoritmo de Deutsch. O passo agora é aplicar a definição do operador U_f sobre os estados da base de $|\psi_1\rangle$ (equação 4.1).

$$U_f(|+\rangle|-\rangle) = \left(\frac{1}{\sqrt{2}}\right)^2 [U_f(|0\rangle|0\rangle) - U_f(|0\rangle|1\rangle) + U_f(|1\rangle|0\rangle) + U_f(|1\rangle|1\rangle)]$$

surge então outro estado, o

$$|\psi_2\rangle = U_f(|+\rangle|-\rangle) = \left(\frac{1}{\sqrt{2}}\right)^2 (|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle) + |1\rangle|1 \oplus f(1)\rangle)$$

ψ_2 fica melhor representado pela sentença

$$|\psi_2\rangle = \left\{ \begin{array}{ll} +\frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & f(0) = f(1) = 0 \\ -\frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & f(0) = f(1) = 1 \\ -\frac{|0\rangle - |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & f(0) \neq f(1) = 0 \\ +\frac{|0\rangle - |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & f(0) \neq f(1) = 1 \end{array} \right\}$$

ou ainda que

$$|\psi_2\rangle = \left\{ \begin{array}{ll} +|+\rangle|-\rangle, & f(0) = f(1) = 0 \\ -|+\rangle|-\rangle, & f(0) = f(1) = 1 \\ -|-\rangle|-\rangle, & f(0) \neq f(1) = 0 \\ +|-\rangle|-\rangle, & f(0) \neq f(1) = 1 \end{array} \right\} \tag{4.3}$$

que pode ser rearranjada para

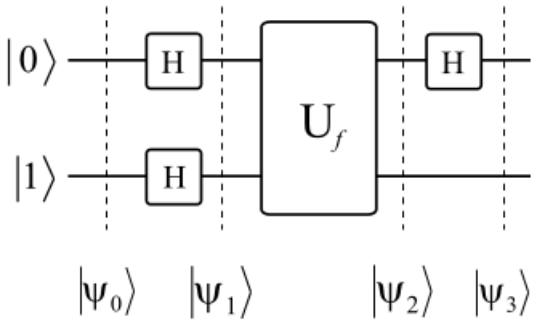
$$|\psi_2\rangle = \begin{cases} (-1)^{f(0)}|+\rangle|-\rangle, & f(0) = f(1) \\ (-1)^{f(0)}|-\rangle|-\rangle, & f(0) \neq f(1) \end{cases} \tag{4.4}$$

ou de forma generalizada

$$|\psi_2\rangle = (-1)^{f(0)}\left[(1 - |f(0) - f(1)|)|+\rangle + |f(0) - f(1)||-\rangle\right]|-\rangle \tag{4.5}$$

Novamente aplica-se o operador Hadamard no primeiro qubit, como ilustra a Figura 8: Usando a

Figura 8 – Esquema do Algoritmo de Deutsch



Fonte: Cabral et al. - Revista Brasileira de Ensino de Fisica, v. 26, n. 2, p. 109 - 116, (2004)

equação 4.4, vem que $|\psi_3\rangle$ pode ser escrito como

$$|\psi_3\rangle = H|\psi_2\rangle = \begin{cases} \pm H|+\rangle|-\rangle, & f(0) = f(1) \\ \pm H|-\rangle|-\rangle, & f(0) \neq f(1) \end{cases}$$

mas $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = H|0\rangle$ e $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} = H|1\rangle$ logo,

$$|\psi_3\rangle = \begin{cases} \pm H^2|0\rangle|-\rangle, & f(0) = f(1) \\ \pm H^2|1\rangle|-\rangle, & f(0) \neq f(1) \end{cases}$$

mas H é um operador unitário, e pelo Postulado II (Descrição Quântica de Observáveis) $H^2 = I$ portanto

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle|-\rangle, & f(0) = f(1) \\ \pm|1\rangle|-\rangle, & f(0) \neq f(1) \end{cases}$$

ou ainda, (da equação 4.5), pode-se generalizar $|\psi_3\rangle$ logo:

$$|\psi_3\rangle = (H \otimes I)|\psi_2\rangle$$

(NIELSEN; CHUANG, 2005) generalizam ψ_3 em termos do estado $|-\rangle$, da forma que segue

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle|-\rangle$$

Por fim, vê-se que o algoritmo verifica o *comportamento global* de f com apenas uma verificação de $f(x)$ pois basta uma leitura para avaliar a soma $f(0) \oplus f(1)$, uma vez que $f(0) \oplus f(1)$ será zero (será constante) se $f(0) = f(1)$ e 1 (balanceada) caso contrário. Este é um dos exemplos do que o paralelismo quântico pode fazer, o estado $|f(0) \oplus f(1)\rangle$ é uma superposição de estados e isto permite que uma alternativa para f interfira na outra, algo que não é permitido num computador clássico. Algoritmos como este, atestam a possibilidade de que os computadores quânticos possam superar os clássicos para tarefas específicas importantes. Adiante será discutido brevemente o Algoritmo de Shor e esta discussão se tornará mais clara.

4.2 ALGORITMO DE TELEPORTE QUÂNTICO

O algoritmo de Teleporte Quântico foi criado pelo físico da IBM Charles Benett em 1993 e segundo (NIELSEN; CHUANG, 2005), o teleporte quântico é uma técnica que permite o transporte de estados quânticos, e portanto informação quântica, de um lugar para outro no espaço sem a necessidade de um canal de comunicação em específico, isto é possível devido a propriedade que estados EPR possuem. São estados fortemente ligados ou seja, estão em um emaranhamento quântico, o que significa que a descrição de um dos estados sem mencionar o outro não é uma alternativa viável. A grosso modo, um estado emaranhado é aquele cuja descrição de um dos estados sempre implica em mencionar o outro estado.

Suponha que se deseje teleportar o estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ para obter informações sobre o estado quântico de um dos estados que obedeçam a relação 3.5 (para estados de Bell) $|\beta_{00}\rangle$, inicia-se o algoritmo de teleporte com o estado composto $|\psi_0\rangle$. A entrada é portanto:

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = [\alpha|0\rangle + \beta|1\rangle] \otimes |\beta_{00}\rangle = [\alpha|0\rangle + \beta|1\rangle] \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

ou ainda

$$|\psi_0\rangle = \left[\frac{\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)}{\sqrt{2}}\right] \tag{4.6}$$

Seguindo o algoritmo, agora deve-se aplicar o operador C-NOT sob o estado que se quer copiar ($|\psi\rangle$) e um dos estados emaranhados ($|0\rangle$).

$$|\psi_1\rangle = \left[\frac{\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|01\rangle + |10\rangle)}{\sqrt{2}}\right]$$

Agora, aplica-se H nos estados de $|\psi_1\rangle$

$$|\psi_2\rangle = \left[\frac{|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)}{\sqrt{2}}\right]$$

Observe que foram gerados quatro novos estados compostos ($|00\rangle, |01\rangle, |10\rangle$ e $|11\rangle$), sendo que o primeiro representa um estado original do sistema e na superposição $(\alpha|0\rangle + \beta|1\rangle)$ está a informação que se quer transmitir relacionada ao estado $|00\rangle$.

Agora realiza-se uma medida em ($|\psi\rangle$ e em um dos estados emaranhados, dessa forma obtêm-se bits clássicos e as linhas duplas na figura 9, representam dois bits clássicos. Tais bits e seus estados quânticos associados são:

$$00 \rightarrow |\psi_3^{00}\rangle = (\alpha|0\rangle + \beta|1\rangle)$$

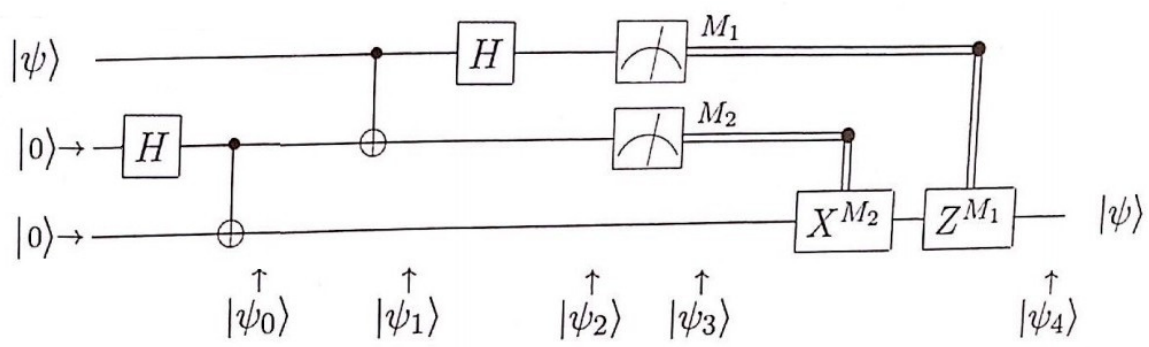
$$01 \rightarrow |\psi_3^{01}\rangle = (\alpha|1\rangle + \beta|0\rangle)$$

$$10 \rightarrow |\psi_3^{10}\rangle = (\alpha|0\rangle - \beta|1\rangle)$$

$$11 \rightarrow |\psi_3^{11}\rangle = (\alpha|1\rangle - \beta|0\rangle)$$

e segundo o Postulado IV, a probabilidade de obter cada um destes estados clássicos é de 25% então, são quatro possíveis resultados para $|\beta_{00}\rangle$. Sendo que para recuperar a informação contida em $|\psi\rangle$, faz-se necessário aplicações das portas X e Z após as medidas, uma vez que esta fará a função de onda colapsar para um estado clássico. A Figura 9 ilustra o esquema do teleporte quântico. Se $M_2 = 0$ a porta X se torna um operador identidade I e o mesmo

Figura 9 – Esquema do algoritmo de teleporte



Fonte: Nielsen e Chuang - Adaptado

vale para a porta Z quando M_1 for obtido, o fato é que a aplicação delas depende da medida realizada, e nestas manipulações, acaba que o estado de Bell agora contém a informação de $|\psi\rangle$ estado que se desejava teleportar anteriormente. É bem verdade que é cedo, para afirmar acerca do entendimento de como funcionam as ferramentas do algoritmo de teleporte, no entanto as próximas seções tornarão a ideia do uso destas ferramentas mais perceptíveis. Pode-se salientar que as manipulações acima, são mais do que aparentam, elas apontaram a possibilidade de a computação quântica quando percebeu-se que havia a possibilidade de se trabalhar com bits clássicos e bits quânticos, bem como utilizar as esquisitas propriedades dos estados EPR para compartilhar informações de dois bits de informação clássica em um único qubit. Mais tarde descobriu-se que o teleporte quântico permitiu a construção de portas que permitiram corrigir algo inevitável nos processos de tráfego de informação - o ruído. Textos sobre o ruído, podem ser visto no trabalho de (NIELSEN; CHUANG, 2005), capítulo 10.

4.3 ALGORITMO DE SHOR - UMA BREVE DISCUSSÃO

A descrição do algoritmo de Shor é um pouco técnica, e exige uma matemática nada simples, que não é adequada ao corpo deste trabalho. Portanto não será abordado os detalhes do algorítmo. Discussão semelhante pode ser encontrada no trabalho de (JúNIOR,) capítulo 7 e a análise completa do algoritmo no trabalho de (NIELSEN; CHUANG, 2005) e também (PORTUGAL et al., 2004).

Cientistas de computação bem como engenheiros sempre se depararam com o problema da fatoração, este é um problema clássico na área e sua principal dificuldade está na complexidade, ela é dita exponencial a saber, dado um número de n bits ou 2^n algarismos, fatorá-lo requer um número de operação proporcional a 2^n, ou seja a complexidade da fatoração cresce exponencialmente com o número de algarismos do número que se deseja decompôr em fatores primos. Por exemplo, fatorar um número de 2 bits ($n = 2$) requeria em torno de 4 operações, para 5 bits seria necessário algo em torno de 32 operações; até aí nada demais porém, quando a proposta é para um número de 15 bits a quantidade de operações é de cerca de $2^{15} \approx 33000$. Se cada uma operação matemática for executada em $1s$ significa que um computador clássico levará mais de 9 horas para decompor um número deste tamanho, o que é um tempo significativo, a situação com certeza é pior se os números tiverem 512 bits ou até 1024, os computadores atuais levariam muito tempo. Na verdade esta é a ideia por traz dos métodos de proteger informação sigilosa moderno, usado por muitas empresas e outros órgãos.

Porém, motivados pelo trabalho de David Deutsch em 1985, Peter Shor e seus colaboradores, novamente na IBM, propuseram uma solução para este problema por volta de 1993. O algoritmo quântico de fatoração proposto por Shor, conseguiu realizar operações com proporcionalidade polinomial em relação ao algoritmo de fatoração clássico. O Shor, se preocupou em tentar enxergar uma forma de encontrar os fatores primos que constituem um número, sem fatorá-lo.

Se um número N é grande, 1024, 2048 etc., o número de divisores primos que ele terá será no máximo $n = log_2\ N$ e alguns qubits podem guardar N. O truque é se perguntar: existe um algoritmo que fatora N em um número de passos que seja um polinômio de ordem n? Nesse ínterim, o algoritmo de Shor vai em busca de um fator de ordem "x"para a quantidade de divisores primos de N, é procurado então o Máximo Divisor Comum de um conjunto de números primos entre si isto é, MDC(x,N) onde $x^r \equiv 1\ mod\ N$, "r"é o menor inteiro ímpar positivo permitido por $x\ mod\ N$. Se "r"for par pode-se realizar as operações de cálculo de ordem seguindo a relação $x^{\frac{r}{2}} \equiv y\ mod\ N$ onde y é o resto da divisão, e $0 \leq y < N$. O fato é que os fatores $y + 1$ e $y - 1$ não podem dividir N separadamente, significa que ambos possuem fatores de N, então o $MDC(y - 1, N)$ e $MDC(y + 1, N)$ produzem os fatores desconhecidos de N.

Então, na busca por um número aleatório x, pode-se encontrar um coprimo de N ou um fator de N, se for coprimo faz-se as considerações de paridade no fator de ordem de x e utilizar o

Tabela 2 – Fatoração por algoritmo clássico

Tamanho do número em bits	Tempo para fatoração
512	4 dias
1024	100 mil anos
2048	100 trilhões de anos

Tabela 3 – Fatoração por algoritmo de Shor

Tamanho do número em bits	Tempo para fatoração
512	34 segundos
1024	4,5 minutos
2048	36 minutos
4096	4,8 horas

$MDC(y-1)$ e $MDC(y+1)$ para determinar os fatores de N, não dando certo tenta-se outro número x até achar o candidato apropriado como explicado por (PORTUGAL et al., 2004). O truque é armazenar todos os inteiros x em um registrador de n qubits ($|0\cdots0\rangle$ por exemplo) e preparar um segundo registrador também de n qubits, depois é criado um estado composto e em seguida uma superposição dos vetores da base através da aplicação de H. Depois há a aplicação de um operador unitário de leitura U_x que por meio do paralelismo quântico, calcula todas as potências de x de uma única vez. Grosso modo, é desta forma que o código de Shor consegue um ganho sobre o algoritmo clássico. As tabelas 2 e 3 ilustram o desempenho dos dois algoritmos como explica (JúNIOR,) em um de seus trabalhos. O algoritmo de Shor foi testado, e até 2012 havia fatorado o número 15 usando a tecnologia de ressonância Magnética nuclear (MARTíN-LóPEZ et al., 2012).

5 O ALGORITMO DE GROVER

Péssima ideia a de uma pessoa ensinar outra a fritar ovos sem que ela saiba o que é um ovo, uma frigideira, óleo, ou mesmo o fogo.
Texto do autor.

Antes de dar início ao algoritmo algumas ferramentas serão explicadas mas antes delas, deve-se haver uma familiarização com o problema. O mesmo ficará perceptível considerando a necessidade de se detectar um número de telefone específico numa lista telefônica em forma de livro, sabe-se que não segue nenhum padrão nem tão pouco alguma facilidade a mais que os outros para ser detectado. O que se pode fazer para encontrá-lo? Bom, pode-se a princípio memorizar este objeto, e folhear algumas páginas da lista de forma a comparar a autenticidade do número registrado e aquele observado, tal número pode está logo no começo da lista, permitindo obter o objeto procurado com poucas comparações, no entanto pode ocorrer diferente, o número pode está próximo ao meio da lista e é o suficiente para tornar o trabalho pouco produtivo. A situação pode piorar pois o elemento desejado pode está no final da lista, o que resulta ao fim em um número de comparações feitas idêntico ao de elementos, este seria o pior caso.

Problemas como estes são situações costumeiras, e portanto campo de empenho de cientistas afim de obter a solução. Claro que para outras situações que não um livro de telefones mas sim, para análise de uma cadeia de moléculas, documentos na internet e banco de dados em geral, onde existem milhares de objetos. Um recurso empregado, entre tantos motivos por ser acessível, para este fim é o computacional onde implementa-se em computadores aplicações com sequências de operações munidas de alguma lógica, e que instruirá como a central de processamento da máquina deve proceder.

Tais aplicações são comumente conhecidas como Algoritmos de Busca, e em sua essência o que é feito é o mesmo que uma pessoa faria com aquela lista de telefones: registra um número desejado e vai em busca dele na lista por meio das comparações. O problema é que dependendo do número de objetos desta lista um computador pode levar mais tempo do que o disponível, limitando assim algum avanço desejado. Ainda que haja vantagem em usar uma máquina para fazer a tarefa em questão devido ao desempenho, o que ela faz é realizar os processos comparacionais de forma mais rápida que um humano ou seja, seu desempenho, sua velocidade é superior a humana. Então o que há na verdade é um ganho de velocidade enquanto que a eficiência permanece inerte! A grande questão então é: é possível que um algoritmo seja mais eficiente que o melhor algoritmo existente para realizar buscas em um banco de dados desordenado?

Como será visto dar um "sim"a esta pergunta foi o trabalho do cientista Lov Grover por volta dos anos 90. O Algoritmo de Grover é um algoritmo quântico de busca que se propõe,

valendo-se de princípios da Mecânica Quântica, propiciar um ganho quadrático sobre o algoritmo clássico de busca mais eficiente (de menor complexidade) existente. Quando este é aplicado sob uma lista de N (N é um número inteiro), elementos desorganizados garante que o resultado desejado será exposto após uma quantidade de operações proporcional a $\sqrt{N}$, diz-se que a complexidade deste é $\sqrt{N}$. Por exemplo, uma busca a um único elemento em uma lista com 100000 elementos desordenados, seriam realizados no pior caso 100000 buscas, enquanto que o algoritmo de Grover precisa de $\sqrt{100000}$ que é cerca de 320 operações, e portanto uma vantagem quadrática sobre o algoritmo clássico mais eficiente.

O melhor caso seria uma única consulta porém, esta situação é um tanto abstrata ou não trivial de ser considerada classicamente, uma vez que ela fica a mercê de situações probabilísticas que podem descaracterizar o conjunto se forem alteradas. Além do paralelismo quântico, o algoritmo de Grover utiliza o artificio de controlar a probabilidade de cada elemento do conjunto ser medido sem interferir nas características deles (esta é uma sutileza do algoritmo), e isto só é permitido graças ao fato de ser um algoritmo quântico de busca.

Além da eficiência, este algoritmo permite também o determinismo ou seja, se o tamanho do banco de dados, da lista, do conjunto, etc. for N então, será previsível o número de operações necessárias para o resultado desejado ser medido e portanto uma estimativa do tempo para tanto. Será abordado a seguir a matemática e a física por trás do Algoritmo de Grover, mas antes disto é imprescindível definir e entender algumas ferramentas. De início, caracteriza-se matematicamente o problema físico, dessa forma, uma lista com N elementos desordenados pode ser representada pelo conjunto $\{0, 1, 2, 3, \cdots, N-1\}$, onde $N = 2^n$ e n representa o número de qubits do conjunto portanto um número natural. Em seguida, define-se uma função $f : \{0, 1, 2, 3, \cdots, N-1\} \longrightarrow \{0, 1\}$ tal que

$$f(i) = \begin{cases} 1, i = i_0 \\ 0, \forall i \neq i_0 \end{cases} \tag{5.1}$$

onde i_0 é o único elemento desejado dentro do conjunto $\{0, 1, 2, 3, \cdots, N-1\}$. Esta é basicamente a maneira clássica se fazer uma busca, ou seja é uma maneira baseada em física clássica, mas o Algoritmo de Busca de Grover é um algoritmo quântico, e a diferença entre ambos surgi a partir de agora.

(NIELSEN; CHUANG, 2005) explicam que para descrever a evolução de qualquer sistema quântico fechado, é necessário definir transformações unitárias. Um sistema quântico qualquer, pode ser um objeto que se quer estudar e que obedece aos postulados da Mecânica Quântica. Logo, é necessário definir um operador unitário U que reproduza quanticamente o papel da função f ()equação5.1), de forma que dada uma entrada $|i\rangle$ do primeiro registrador e outra $|j\rangle$ do segundo registrador a transformação causada pela ação do operador U não altere a dimensão do espaço vetorial W^2 que estar se trabalhando (mais tarde isto será verificado).

Nesse ínterim, faz-se necessário um operador unitário U_f que transforme o estado

quântico $|i\rangle$ em $|f(i)\rangle$ convenientemente tem-se:

$$|i\rangle|0\rangle \underrightarrow{U_f} |i\rangle|f(i)\rangle$$

onde $|0\rangle$ é a representação do primeiro registrador. O operador U_f altera o estado dos registradores conforme representado abaixo para o primeiro e segundo registrador respectivamente:

$$U_f\left(|i\rangle|0\rangle\right) = \begin{cases} |i\rangle|1\rangle, i = i_0 \\ |i\rangle|0\rangle, \forall i \neq i_0 \end{cases}$$

e

$$U_f\left(|i\rangle|1\rangle\right) = \begin{cases} |i\rangle|0\rangle, i = i_0 \\ |i\rangle|1\rangle, \forall i \neq i_0 \end{cases}$$

Se estas sentenças forem combinadas com a definição da função f surgirá uma generalização da aplicação de U_f em dois estados dada por:

$$U_f\left(|i\rangle|j\rangle\right) = |i\rangle|j \oplus f(i)\rangle \tag{5.2}$$

onde $|j\rangle$ é o estado do segundo registrador e $\oplus$ representa a operação de soma módulo 2.

Iniciando o algoritmo: no algoritmo de Grover é fundamental dois registradores quânticos, conforme foi exposto na seção 4.1. O primeiro com n qubits é inicializado como $|0\cdots0\rangle$ e o segundo registrador de 1 qubit, é inicializado como $|1\rangle$. O primeiro registrador (um vetor de n qubits) será um representante dos elementos da lista, pode-se ainda associá-los a cada estado quântico $|i\rangle$ e o valor i a "posição"onde se encontra o elemento desejado na "fila"de elementos, portanto, a priori, i_0 está dentro do conjunto e só é necessário identificar seu estado quântico. Pode-se ainda, utilizar o Postulado VI e escrever um estado composto inicializado como

$$|\varphi_0\rangle = |0\cdots0\rangle|1\rangle.$$

Iniciado os registradores, agora usa-se o operador de Hadamard (H), para criar uma superposição desses auto estados quânticos e dá-lhes mesma amplitude de probabilidade. Aplicando o operador H no primeiro registrador e no segundo vem que,

$$|\varphi_1\rangle = \left(H^{\otimes n+1}|\varphi_0\rangle\right) = \left(H^{\otimes n}|0\cdots0\rangle\right) H|1\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|-\rangle = |\psi\rangle|-\rangle$$

onde $|\psi\rangle = \dfrac{1}{\sqrt{N}}\displaystyle\sum_{i=0}^{N-1}|i\rangle$ que representa uma combinação linear dos estados do primeiro registrador, associado aos elementos da lista. O auto estado $|-\rangle$ é decorrente das operações entre as matrizes como abaixo

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}$$

usando a representação matricial de $|0\rangle$ e $|1\rangle$ vem que

$$\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle$$

Com um vetor de estados quânticos que representa a lista definido (ψ), o próximo passo agora é identificar o elemento i_0, e portanto utilizar o representante legal da função f ou seja, é a vez do operador U_f. Aplicando U_f sobre o estado já inicializado $|\psi\rangle|-\rangle$,

$$U_f(|i\rangle|-\rangle) = U_f\left(\left(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\right)|-\rangle\right)$$

por ser um operador linear pode-se escrever

$$U_f(|i\rangle|-\rangle) = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}U_f(|i\rangle|-\rangle),$$

substituindo a definição do estado $|-\rangle$ vem que

$$U_f(|i\rangle|-\rangle) = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}U_f\left(|i\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}U_f\left(\frac{|i\rangle|0\rangle - |i\rangle|1\rangle}{\sqrt{2}}\right),$$

que pode ser reescrita como

$$U_f(|i\rangle|-\rangle) = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\left(\frac{U_f(|i\rangle|0\rangle) - U_f(|i\rangle|1\rangle)}{\sqrt{2}}\right),$$

E usando a definição do operador U_f (equação 5.2) e a distributividade no produto tensorial vem que:

$$U_f(|i\rangle|-\rangle) = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\frac{1}{\sqrt{2}}\left(|i\rangle|f(i)\rangle - |i\rangle|1\oplus f(i)\rangle\right) = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\frac{|i\rangle}{\sqrt{2}}\left(|f(i)\rangle - |1\oplus f(i)\rangle\right)$$

Da definição da função f (equação 5.1)

$$U_f(|i\rangle|-\rangle) = \frac{1}{\sqrt{N}}\left(\left(\sum_{i=0|i\neq i_0}^{N-1}\frac{|i\rangle(|0\rangle - |1\rangle)}{2}\right) + \frac{|i_0\rangle(|1\rangle - |0\rangle)}{2}\right)$$

mas $\frac{|i_0\rangle(|1\rangle - |0\rangle)}{2} = -\frac{|i_0\rangle(|0\rangle - |1\rangle)}{2} = -|i_0\rangle|-\rangle$ daí

$$U_f(|i\rangle|-\rangle) = \frac{1}{\sqrt{N}}\left(\left(\sum_{i=0|i\neq i_0}^{N-1}|i\rangle|-\rangle\right) - |i_0\rangle|-\rangle\right)$$

Desta forma a aplicação do operador U_f sobre os estados quânticos dos dois registradores ($|0\cdots 0\rangle$ e $|1\rangle$) pode ser escrita por:

$$U_f(|i\rangle|-\rangle) = \left(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle(-1)^{f(i)}\right)|-\rangle$$

ou ainda

$$U_f(|i\rangle|-\rangle) = |\psi_1\rangle|-\rangle \tag{5.3}$$

onde $|\psi_1\rangle = \left(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{f(i)}|i\rangle\right)$ e finalmente

$$U_f(|i\rangle|-\rangle) = \begin{cases} -|i\rangle|-\rangle, i = i_0 \\ |i\rangle|-\rangle, i \neq i_0 \end{cases} \tag{5.4}$$

Na equação (5.4), o operador linear U_f atua nos elementos da base do espaço vetorial, e uma única aplicação do operador U_f alterou o estado ψ para um novo estado ψ_1 fazendo uma leitura de todos os elementos da lista. Isto é o paralelismo quântico! Além disto, foi identificado o estado do elemento i_0 e com o auxílio do segundo registrador alterou sua amplitude de probabilidade para $-\frac{1}{\sqrt{N}}$. O segundo registrador apesar de não ter sido alterado se faz fundamental, ele "marca"o elemento procurado e claramente, o elemento i_0 é o único com amplitude de probabilidade alterada. Vale salientar que toda informação está acessível apenas ao nível quântico, e conforme foi visto no Postulado IV (ver seção 2) qualquer medida que for realizada afim de obter a informação física do estado de i_0 após a primeira aplicação do operador U_f terá uma probabilidade de sucesso de $|\frac{-1}{\sqrt{N}}|^2 = \frac{1}{N}$ e representa um valor muito pequeno uma vez que está se considerando o fato a quantidade de elementos do conjunto é muito grande isto é, que $N \to \infty$.

Por exemplo, se $N = 100$ elementos desordenados, a chance de sucesso será de apenas $|\frac{-1}{\sqrt{N}}|^2 = \frac{1}{100} = 1\%$, para conjuntos onde N supera os 100000 elementos este número é ainda menor, então não há nenhuma vantagem em realizar uma medição após a primeira aplicação do operador U_f ela serve apenas para causar uma reflexão do vetor de auto estados quânticos sobre o vetor unitário da base $|u\rangle = \frac{1}{\sqrt{N-1}}\sum_{i=0|i\neq i_0}^{N-1}|i\rangle$ ortonormal a o outro vetor da base - o $|i_0\rangle$ conforme explicam (NIELSEN; CHUANG, 2005). A figura 10 elucida a aplicação de U_f. O próximo passo agora é, aumentar a amplitude de probabilidade do elemento i_0, uma vez que este já foi identificado. (PORTUGAL et al., 2004) explicam que isto é feito mediante uma reflexão do vetor de auto estados $|\psi_1\rangle$ em relação ao vetor de auto estados $|\psi\rangle$ criando assim o $|\psi_G\rangle$ conforme ilustrado na figura 11. É fácil verificar que o operador que causa a reflexão de $|\psi_1\rangle$ sobre $|\psi\rangle$ é $(2|\psi\rangle\langle\psi| - I)$ observando a figura 12 e a 13 abaixo.

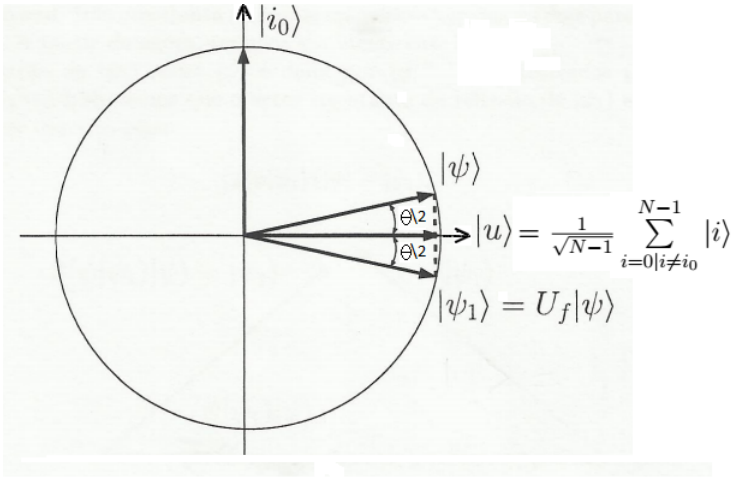
O ângulo α_0 pode ser calculado pela mesma relação que permitiu construir o operador reflexão isto é,

$$\cos(\alpha_0) = \langle\psi|i_0\rangle \Rightarrow \alpha_0 = \cos^{-1}\left(\langle\psi|i_0\rangle\right) = \cos^{-1}\left(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\langle i|i_0\rangle\right)$$

logo

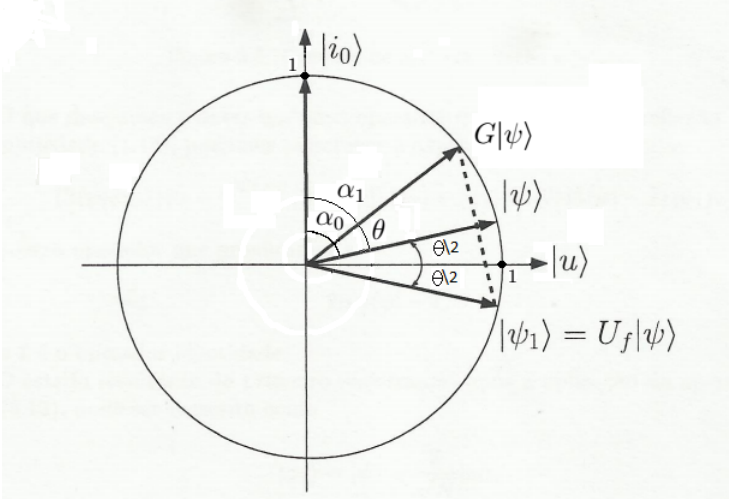
$$\alpha_0 = \cos^{-1}\left[\frac{1}{\sqrt{N}}\left(\langle 0|i_0\rangle + \langle 1|i_0\rangle + \cdots + \langle i_0|i_0\rangle + \langle N-2|i_0\rangle + \langle N-1|i_0\rangle\right)\right]$$

Figura 10 – Ação do operador U_f



Fonte: Adaptado de (PORTUGAL et al., 2004)

Figura 11 – O operador reflexão



Fonte: Adaptado de (PORTUGAL et al., 2004)

que devido a ortonormalidade entre os auto-estados resulta em

$$\alpha_0 = \cos^{-1}\left(\frac{1}{\sqrt{N}}\langle i_0|i_0\rangle\right) = \cos^{-1}\left(\frac{1}{\sqrt{N}}\right),$$

portanto, o ângulo entre $|\psi\rangle$ e $|i_0\rangle$ é menor que $\frac{\pi}{2}$ radiano.

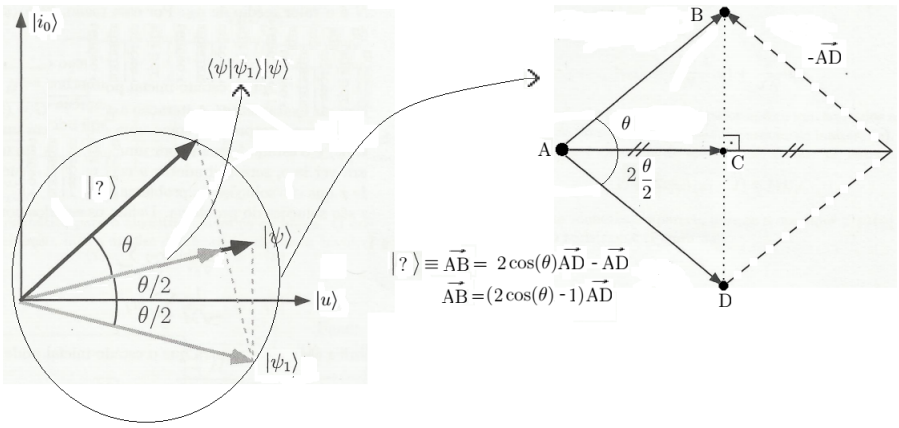
Pode se definir $|\psi_G\rangle$ em termos de $|\psi_1\rangle$:

$$|\psi_1\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{f(i)}|i\rangle = \frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + |2\rangle + \cdots - |i_0\rangle + |N-2\rangle + |N-1\rangle\right),$$

ou ainda

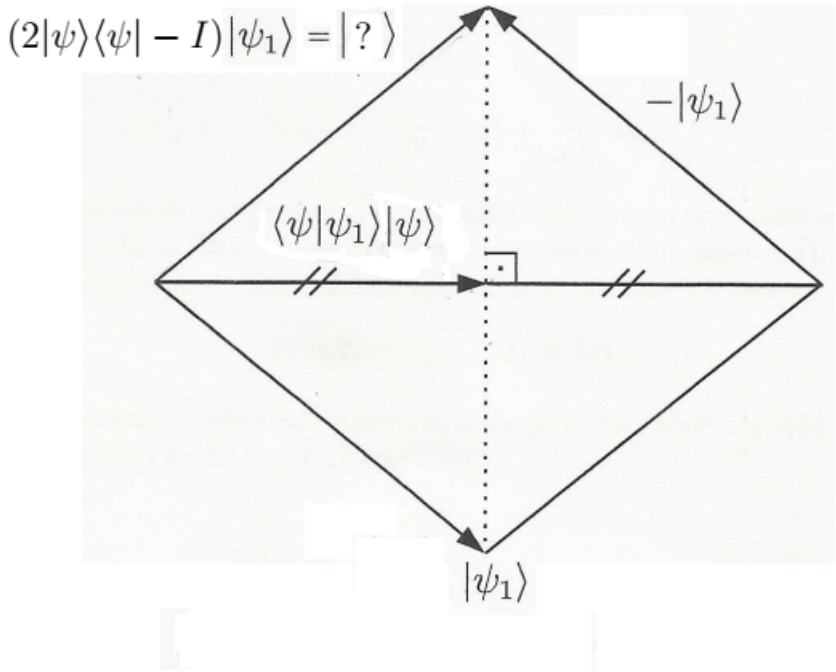
$$|\psi_1\rangle = \frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + |2\rangle + \cdots + |N-2\rangle + |N-1\rangle\right) - \frac{1}{\sqrt{N}}|i_0\rangle,$$

Figura 12 – Dedução ilustrativa do operador reflexão



Fonte: Do autor

Figura 13 – Geometria do operador Reflexão



Fonte: (PORTUGAL et al., 2004)

mas $\frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + |2\rangle + \cdots + |N-2\rangle + |N-1\rangle\right) = |\psi\rangle - \frac{1}{\sqrt{N}}|i_0\rangle$, logo

$$|\psi_1\rangle = |\psi\rangle - \frac{1}{\sqrt{N}}|i_0\rangle - \frac{1}{\sqrt{N}}|i_0\rangle \Rightarrow |\psi_1\rangle = |\psi\rangle - \frac{2}{\sqrt{N}}|i_0\rangle,$$

desta forma,

$$|\psi_G\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle = (2|\psi\rangle\langle\psi| - I)\left(|\psi\rangle - \frac{2}{\sqrt{N}}|i_0\rangle\right),$$

$$= -\left(-2\langle\psi|\psi\rangle) + \frac{4}{\sqrt{N}}\langle\psi|i_0\rangle + 1\right)|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle = -\left(-2 + \frac{4}{N} + 1\right)|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle,$$

ou simplesmente que

$$|\psi_G\rangle = \left(\frac{N-4}{N}\right)|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle = G|\psi\rangle, \tag{5.5}$$

onde $G = [(2|\psi\rangle\langle\psi| - I) \otimes I]\, U_f$ é o operador Interação de Grover.

Vale salientar aqui, que a aplicação de G tem influência direta apenas nas amplitudes de probabilidade de $|\psi\rangle$ isto é, o subespaço vetorial (W) gerado por $|\psi\rangle$ e $|i_0\rangle$ ainda é o mesmo. A indução matemática ajuda a entender isto. Sabe-se que uma aplicação do operador G sobre $|\psi\rangle$ ($k = 1$), dá o seguinte vetor de auto estados:

$$G|\psi_G\rangle = \left(\frac{N-4}{N}\right)|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle \equiv G^1|\psi\rangle$$

daí supondo que, para todo k inteiro e positivo, $G^k|\psi\rangle \in W$. Nisto, esta-se assumindo que existem constantes reais tais que:

$$G^k|\psi\rangle = \beta|\psi\rangle + \gamma|i_0\rangle \tag{5.6}$$

onde β e γ são números reais. Deve-se mostrar então que $G^{k+1}|\psi\rangle \in W$. Aplicando G a ambos os membros da equação 5.6, vem que

$$G\left(G^k|\psi\rangle\right) = G\left(\beta|\psi\rangle + \gamma|i_0\rangle\right) = \beta\left(G|\psi\rangle\right) + \gamma\left(G|i_0\rangle\right) =$$

$G|\psi\rangle$ é conhecido, e $G|i_0\rangle$ se tornará através da definição do operador U_f

$$G|i_0\rangle = (2|\psi\rangle\langle\psi| - I)U_f|i_0\rangle = 2|\psi\rangle\langle\psi||i_0 - |i_0\rangle = -2\langle\psi|i_0\rangle|\psi\rangle - |i_0\rangle = -\frac{2}{\sqrt{N}} + |i_0\rangle$$

portanto, $G|i_0\rangle \in W$ bem como $G|\psi\rangle$. Constata-se portanto que $G\left(G^k|\psi\rangle\right) = G^{k+1}|\psi\rangle \in W$.

Um cálculo rápido, mostra que uma aplicação de G aumentou a amplitude de probabilidade do elemento i_0.

$$\langle\psi_G|i_0\rangle = \left(\frac{N-4}{N}\frac{1}{\sqrt{N}} + \frac{2}{\sqrt{N}}\right) = \frac{3N-4}{N\sqrt{N}} = \left(3 - \frac{4}{N}\right)\frac{1}{\sqrt{N}} > \frac{1}{\sqrt{N}}$$

. Para $N = 4$ por exemplo, a probabilidade $P_4 = |\langle\psi_G|i_0\rangle|^2 = |\left(3 - \frac{4}{4}\right)\frac{1}{\sqrt{2^2}}|^2 = 100\%$. A afirmação da proporcionalidade com $\sqrt{N}$ será vista adiante.

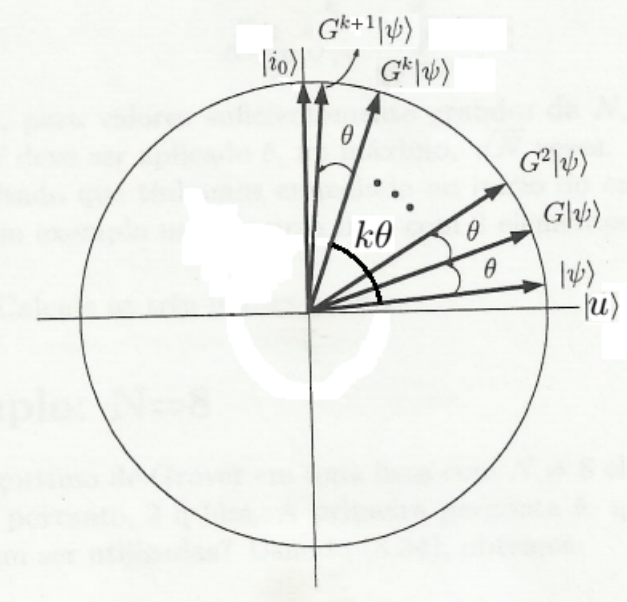
Para um sistema de 3 qubits ($N = 8$) vem que, $P_8 = |\langle\psi_G|i_0\rangle|^2 = |\left(3 - \frac{2^2}{2^3}\right)\frac{1}{\sqrt{2^3}}|^2 \approx 40\%$

O ângulo α_1 entre $|\psi_G\rangle$ e $|i_0\rangle$ é portanto

$$\alpha_1 = \cos^{-1}\left(\langle\psi_G|i_0\rangle\right) = \cos^{-1}\left(\frac{N-4}{N}\langle\psi|i_0\rangle + \frac{2}{\sqrt{N}}\langle i_0|i_0\rangle\right) = \cos^{-1}\left(\frac{3N-4}{N\sqrt{N}}\right)$$

Uma vez que a função $\cos^{-1}(t)$ é decrescente no intervalo $[-1, 1]$ pode-se dizer então que $\alpha_1 < \alpha_0$. Outro ponto importante a ser ressaltado sobre a aplicação do operador G, é que o ângulo formado entre o vetor $|\psi\rangle$ e $|\psi_G\rangle$ é θ e isto ocorre em todas as interações de G com $|\psi\rangle$ ou seja, o ângulo entre $G^k|\psi\rangle$ e $G^{k+1}|\psi\rangle$ é θ, conforme ilustrado na figura 14 . Isto se verifica

Figura 14 – O operador G



Fonte: Adaptado de Nelson Maculan et al - Uma introdução a computação quântica

através da definição de ângulo entre dois vetores de estados:

$$\cos(\theta) = \langle\psi_{G^k}|\psi_{G^{k+1}}\rangle = \langle\psi_{G^k}|G^kG|\psi\rangle$$

Do Postulado II (Descrição Quântica de Observáveis) e de $G|\psi\rangle = |\psi_G\rangle$ vem que,

$$\langle\psi_{G^k}|G^kG|\psi\rangle = \langle\psi_{G^k}|G^k|\psi_G\rangle = \langle(G^k)^\dagger\psi_{G^k}|\psi\rangle = (G^k)^\dagger(G^k|\psi\rangle) = |\psi\rangle$$

portanto

$$\langle(G^k)^\dagger\psi_{G^k}|\psi\rangle = \langle\psi|\psi_G\rangle = \langle\psi_{G^k}|\psi_{G^{k+1}}\rangle = \cos(\theta).$$

Já foi mostrado ferramental suficiente para entender sobre a complexidade do algoritmo de Grover, a qual foi mencionada anteriormente. A complexidade do Algoritmo de Grover está relacionada ao número k de vezes que o operador $G = [(2|\psi\rangle\langle\psi| - I) \otimes I]U_f$ é utilizado até que o vetor $|\psi\rangle$ esteja próximo o suficiente de $|i_0\rangle$.

Assim, se cada aplicação de G rotaciona $\psi\rangle$ de θrad então deve haver uma rotação máxima de $|\psi\rangle$ tal que

$$\cos^{-1}(\langle\psi|i_0\rangle) - k\theta \to 0$$

A suposição desde o início é que N é um número bem grande ($N \to \infty$), de forma que a aproximação abaixo é válida.

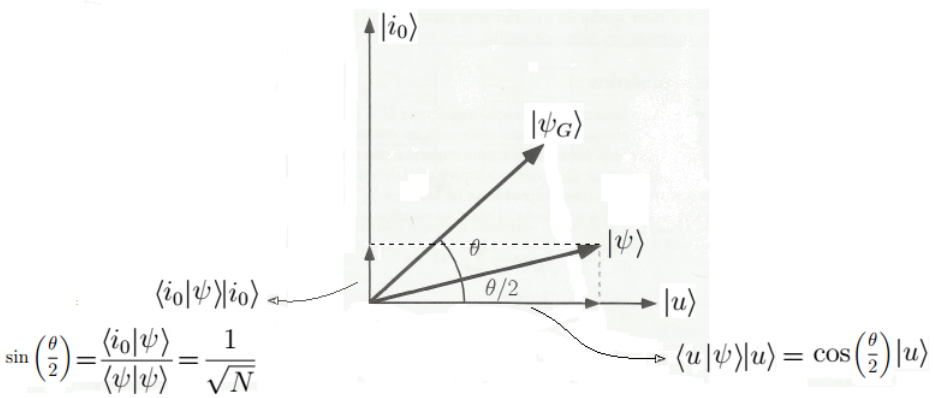
$$\cos^{-1}(\langle\psi|i_0\rangle) - k\theta = 0$$

daí

$$k = \frac{\cos^{-1}\left(\langle\psi|i_0\rangle\right)}{\theta} = \frac{\cos^{-1}\left(\frac{1}{\sqrt{N}}\right)}{\cos^{-1}\left(\frac{N-2}{N}\right)} \tag{5.7}$$

no entanto este é um meio um tanto difícil para estimar o qual a ordem de grandeza da constante k, uma vez que envolve certa criatividade nas manipulações para as aproximações serem coerentes porém. Observando a figura 15, na situação em que $N \to \infty$ alguns argumentos tornam-se intuitivos um deles é que é válida a consideração que $\theta \approx \sin(\theta) = \frac{1}{\sqrt{N}}$ pois, θ é muito pequeno

Figura 15 – Divisão do primeiro quadrante em termos de $\sin(\theta)$



Fonte: Do autor

(quando N é grande) como explicam (NIELSEN; CHUANG, 2005). Da expressão 5.7 parece razoável afirmar que este é inversamente proporcional ao ângulo θ e que dentro do intervalo do primeiro quadrante ($\frac{\pi}{2}$ radiano), vale a relação

$$k \leq \frac{\frac{\pi}{2}}{\theta}$$

Decorre disto que o limite inferior de θ dará a quantidade máxima de k. Da figura acima sabe-se que

$$\frac{\theta}{2} \leq \sin\left(\frac{\theta}{2}\right) = \frac{1}{\sqrt{N}}.$$

Além disto

$$k \leq \frac{\pi}{2\theta},$$

logo

$$k \leq \frac{\pi}{2\frac{2}{\sqrt{N}}},$$

que com um arredondamento para baixo pode-se afirmar com segurança que

$$k = \frac{\pi}{4}\sqrt{N} \tag{5.8}$$

E este era o resultado tão esperado. Ele significa que na k-ésima interação de Grover a solução do problema de busca estará com probabilidade máxima de ser obtida além disto, a equação 5.8

denuncia que o número de interações k é proporcional a $\sqrt{N}$. O ganho quadrático fica visível quando se observa que dado um número de operações $t = \sqrt{N}$ para o algoritmo de Grover determinar o elemento desejado, o algoritmo clássico necessita de $t^2 = N$ ou seja, existe um ganho de tempo nesta igualdade quando optar-se por utilizar o operador interação de Grover, é por este motivo que é considerado muitas vezes o mais eficiente algoritmo de busca num banco de dados, onde a quantidade N de elementos é muito grande, mas sua implementação só é possível em meios exclusimante quânticos.

O Algoritmo de Grover se resume à:

$1 \rightarrow$ Definir estado inicial dos registradores: $|0 \cdots 0\rangle \equiv |0\rangle^{\otimes n}|0\rangle$ e $|1\rangle$ onde n é o número de qubits do conjunto

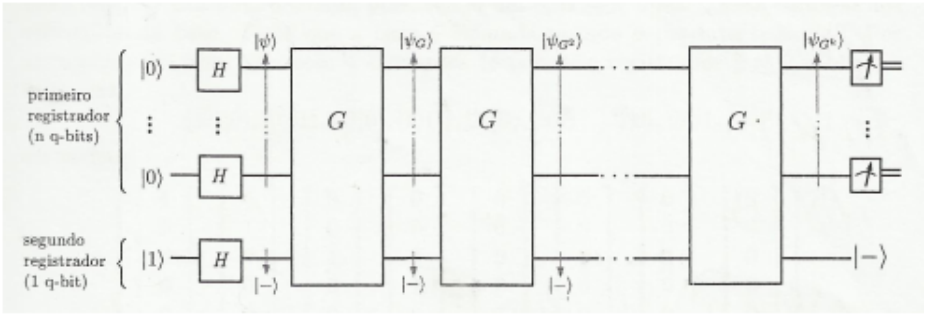
$2 \rightarrow$ Criar a superposição dos estados quânticos do primeiro registrador para utilizar o paralelismo quântico: $|\psi\rangle = H^{\otimes n}|0\rangle H|1\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|-\rangle$

$3 \rightarrow$ Aplicar G em $|\psi\rangle$ k vezes: $G^k|\psi\rangle = \{[2(|\psi\rangle\langle\psi| - I) \otimes I]U_f\}^k \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|-\rangle$

$4 \rightarrow$ Colapse a função de onda e obtenha i_0

A figura 16 ilustra o funcionamento do algoritmo, descrito acima: Para $N = 4 \Rightarrow k =$

Figura 16 – Esquema geral do Algoritmo de Grover



Fonte: Maculan et al. - Uma introdução a Computação Quântica

$\frac{\cos^{-1}\left(\frac{1}{\sqrt{2^2}}\right)}{\cos^{-1}\left(\frac{4-2}{4}\right)} = 1$. Portanto, uma aplicação do operador de Grover é o suficiente para elevar a amplitude de probabilidade de um dos elementos ao máximo e quando for realizada uma medida sobre o sistema, o vetor de estado $|\psi\rangle$ irá colapsar para este auto estado com probabilidade $P_4 = |\langle\psi_G|i_0\rangle|^2 = 100\%$.

Para um sistema de 3 qubits ($N = 8$) tem-se $k = \dfrac{\cos^{-1}\left(\frac{1}{\sqrt{2^3}}\right)}{\cos^{-1}\left(\frac{8-2}{8}\right)} \approx 1.673$. A ideia é fazer um arredondamento para o número inteiro mais próximo, neste caso 2. Portanto na segunda aplicação de G sobre os dois registradores quânticos inicializados ($G^2|\psi\rangle|-\rangle$), a probabilidade

de se obter i_0 será máxima. De forma genérica,

$$G^2|\psi\rangle|-\rangle = G\left(G|\psi\rangle\right)|-\rangle = G|\psi_G\rangle|-\rangle = G\left(\frac{N-4}{N}|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle\right)|-\rangle$$

G atua nos elementos da base, logo pode-se escrever

$$G^2|\psi\rangle|-\rangle = \frac{N-4}{N}G|\psi\rangle|-\rangle + \frac{2}{\sqrt{N}}G|i_0\rangle|-\rangle = \frac{N-4}{N}|\psi_G\rangle|-\rangle + \frac{2}{\sqrt{N}}\left[(2|\psi\rangle\langle\psi| - I)\otimes I\right]U_f\left(|i_0\rangle|-\rangle\right)$$

usando a definição de U_f (5.4) e da distribuitividade do produto tensorial vem que

$$G^2|\psi\rangle|-\rangle = \frac{N-4}{N}\left(\frac{N-4}{N}|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle\right)|-\rangle + \frac{2}{\sqrt{N}}\left(2\langle\psi|i_0\rangle|\psi\rangle - |i_0\rangle\right)|-\rangle$$

Observe que o estado $|-\rangle$ não foi alterado, porém utilizado na atuação do operador U_f. Realizando as contas e simplificando vem que

$$G^2|\psi\rangle|-\rangle = \left\{\left[\left(\frac{N-4}{N}\right)^2 - \left(\frac{2}{\sqrt{N}}\right)^2\right]|\psi\rangle + \left[2\left(\frac{N-4}{N\sqrt{N}}\right) + \frac{2}{\sqrt{N}}\right]|i_0\rangle\right\}|-\rangle$$

A amplitude de probabilidade α_{i_0} de $|i_0\rangle$ para $k=2$ é portanto, a soma

$$\alpha_{i_0} = \left[\left(\frac{N-4}{N}\right)^2 - \left(\frac{2}{\sqrt{N}}\right)^2\right]\frac{1}{\sqrt{N}} + \frac{2}{\sqrt{N}}\left(\frac{(N-4)}{N} + 1\right) \tag{5.9}$$

Substituindo $N=8$ em 5.9 e efetuando as contas, vem que

$$\alpha_{i_0} = \frac{11}{4\sqrt{8}} \Rightarrow P_{i_0} = \alpha_{i_0}^2 \approx 95\%$$

o que mostra que para um conjunto com oito elementos, a probabilidade de se obter um deles é máxima após a segunda aplicação de G.

6 CONCLUSÃO

Neste trabalho foi possível fazer um breve estudo da história da computação, agregando conhecimentos sobre seus avanços e problemas bem como a maneira que alguns cientistas solucionaram os mesmos. A ideia de algoritmo foi trabalhada e foi possível fazer uma conexão deles com a mecânica quântica. Foi feita uma descrição do espaço onde trabalha a Mecânica Quântica e suas leis foram explicitadas, na intenção de permitir a versatilidade no estudo dos algoritmos quânticos. Também foi introduzidos os conceitos e elementos da computação quântica. Foi possível perceber que a mesma é dotada de leis que se sustentam na mecânica quântica e portas lógicas que desempenham o papel fundamental para atingir a proposta dos algoritmos.

A porta Hadamard mostrou que é possível criar uma superposição de estados com mesma amplitude de probabilidade por meio de algumas operações matriciais, a porta Não-Controlado (C-NOT) se mostrou útil, na manipulação dos estados emaranhados. A capacidade de processamento de muitos qubits ao mesmo tempo foi exibida através do operador U_f exibido no algorítmo de Grover. O principal objetivo deste trabalho foi alcançado, uma vez que foi descrito os algoritmos quânticos mais conhecidos, dando uma ideia de sua aplicabilidade e da teoria por traz da aplicação dos algoritmos.

O algoritmo de Deutsch é sem dúvida, um dos algorítmos mais simples e intuitivos para se entender a proposta da computação quântica e suas vantagens pois, em sua essência está o paralelismo quântico; que como foi explicado, permite fazer inúmeras avaliações simultaneamente. Foi ele quem permitiu fazer a análise do comportamento de uma função binária. A importância do algoritmo de teleporte merece destaque, pois exibe que á possível lidar com as adversidades da Mecânica Quântica e utilizar a mesma para fazer transporte de informação.

O algoritmo de Shor foi mencionado e nele foi feita a menção de conceitos que não estão estruturados neste trabalho, mas merece destaque principalmente por mostrar que é possível fazer máquinas que operem sob as leis da mecânica quântica, pelo fato de ter aberto uma nova área da ciência - a criptografia quântica, uma vez que qualquer código RSA pode ser quebrado pelo algoritmo de Shor em tempo hábil. Muitos conceitos matemáticos e físicos foram exibidos no algoritmo de Grover, e faz-se singular dentre os algoritmos de busca por ser o único a conseguir realizar buscas em um banco de dados grande e desordenado com um número de operações proporcional a raiz quadrada do número de objetos dentro do banco de dados.

Muito conhecimento foi adquirido na descrição do algoritmo e algumas generalizações matemáticas foram feitas, dando uma outra visão para o mesmo fenômeno e também qualidade a este material sem tirá-lo do patamar da literatura, além disso o agregado de leis e definições o torna ainda mais rico, o que de certa forma contribui para a área de estudo. De certa forma, percebe-se que ainda existem poucos materiais como este disponíveis na literatura brasileira, e

em alguns os conceitos físicos carecem de atenção, o que geram limitações acerca da atividade de pesquisa e desenvolvimento, outro fator limitante é o quão pouco intuitivos são os métodos como é proposta a computação quântica.

Ao fim, a ideia do que é computação e como a mudança de paradigma pode resolver problemas específicos foi passada, o objetivo foi cumprido. Agora com o conhecimento agregado será possível por exemplo, desenvolver atividades práticas que trabalhem de forma mais simples o funcionamento algoritmo de Grover ou render textos com a criptografia quântica, códigos para correção de erros em sistemas quânticos ou até esmiuçar toda a matemática por traz do algoritmo de Shor.

REFERÊNCIAS

ALEGRETTI, F. J. P. Computação quântica. *Universidade Federal do Rio Grande do Sul - Instituto de Informática*, 2004. Citado 2 vezes nas páginas 12 e 15.

AMARAL, B. L. *Emaranhamento em sistemas de dois qubits*. Dissertação (Dissertação de Mestrado) — Universidade Federal de Minas Gerais - UFMG, 2008. Citado na página 23.

ANDRADE, A. P. *Física Moderna - Parte I*. Ilhéus - Bahia: EDITUS, 2013. Citado na página 19.

BUTKOV, E. *Física Matemática*. Rio de Janeiro - RJ: Livros técnicos científicos - LTC, 1988. Citado na página 19.

CABRAL, G. E. M.; LIMA, A. F. de; JUNIOR, B. L. Interpretando o algoritmo de deutsch no interferômetro de mach-zehnder. *Revista Brasileira de Ensino de Física*, v. 26, n. 2, p. 109–116, 2004. Citado 2 vezes nas páginas 26 e 33.

CARUSO, F.; OGURI, V. *Física moderna: origens clássicas e fundamentos quânticos*. Rio de Janeiro - RJ: Editora Campus, 2006. Citado na página 19.

FORBELLONE, L. V.; EBERSPACHER, H. F. *Lógica de Programação: a contrução de algoritmos e estrutura de dados*. São Paulo - SP: Pearson Prentice Hall, 2005. Citado na página 12.

JúNIOR, I. dos S. O. *Física Moderna para iniciados, interessados e aficionados*. São Paulo - SP: [s.n.]. Citado 2 vezes nas páginas 37 e 38.

MARTíN-LóPEZ, E. et al. Experimental realization of shor's quantum factoring algorithm using qubit recycling. *Nature Photonics*, v. 6, p. 773–776, 2012. Citado na página 38.

NIELSEN, M. A.; CHUANG, I. L. *Computação Quântica e informação quântica*. Porto Alegre - RS: Cambridge University Press, 2005. Citado 10 vezes nas páginas 24, 25, 29, 34, 35, 36, 37, 40, 43 e 48.

OSVALDO, P. J. *Conceitos de física quântica*. 2. ed. São Paulo - SP: Editora Livraria da Física, 2003. Citado na página 15.

PELEG, Y.; PNINI, R.; ZAARUR, E. *Schaum's outline of Theory and problems of quantum mechanics*. Rio de Janeiro: McGraw-Hill, 1998. Citado na página 22.

PEREIRA, A. P. de et al. Uma aboradgem conceitual e fenomenológica dos postulados da física quântica. *Departamento de Física - UFRGS*, v. 29, p. 831–863, 2012. Citado na página 20.

PORTUGAL, R. et al. *Uma introdução à Computação Quântica*. São Carlos - SP: Sociedade Brasileira de Matemática Aplicada e computacional - SBMAC, 2004. Citado 6 vezes nas páginas 33, 37, 38, 43, 44 e 45.

SARAIVA, C. A. E.; ARGIMON, I. I. de L. Ciência da computação e ciência cognitiva: um paralelo de semelhanças. *Ciências e Cognição*, v. 12, p. 150–155, 2007. Citado na página 12.

SILVA, F. L. S. da. Computação quântica: O algoritmo de deutsch e o paralelismo quântico. *Revista Physicae*, n. 3, 2002. Citado na página 32.

ZETTILI, N. *Quantum Mechanics Concepts and Applications*. 2. ed. Jacksonville, USA, 2009. Citado 2 vezes nas páginas 20 e 23.