A utilização da computação quântica em algoritmos de busca em banco de dados

Marvin Willian Machry Pocahy[1]

Ricardo Vanni Dallasen[2]

ABSTRACT

The purpose of this work is to compare the quantum database search algorithm (Grover) with classical algorithms. For that, this work proposes to provide an introduction to quantum computing, exposing its fundamentals and relevant physics, describing how the architecture of a quantum computer and its properties would be. Quantum computing is a possible replacement (or at least a complement) to traditional computing, based on physical principles that diverge from classical physics, not necessarily having to follow them. In this form of computation there is no concept of 2 (two) possible outcomes ("0" and "1") of conventional computers, but works through states of probabilities (0, 1 and a "maybe"). The work will be developed with the help of Qiskit and OpenQASM tools (available by IBM Quantum Experience), and the creation of search algorithms in databases using the C++ language.

Keywords: *Grover, quantum algorithms, quantum computing, Qiskit, OpenQASM.*

RESUMO

A proposta deste trabalho é comparar o algoritmo quântico de busca em banco de dados (Grover) com algoritmos clássicos. Para isso, este trabalho propõe-se a fornecer uma introdução à computação quântica, expondo seus fundamentos e física relevantes, descrevendo como seria a arquitetura de um computador quântico e suas propriedades. A computação quântica é uma possível substituta (ou pelo menos complemento) da computação tradicional, baseada em princípios físicos que divergem da física clássica, não necessariamente tendo que acompanhá-las. Nesta forma de computação não existe o conceito de 2(dois) possíveis resultados ("0" e "1") dos computadores convencionais, mas trabalha por meio de estados de probabilidades (0, 1 e um "talvez"). O trabalho será desenvolvido com o auxílio das ferramentas Qiskit e OpenQASM (disponibilizadas pelo IBM Quantum Experience), e a criação de algoritmos de busca em banco de dados com a linguagem C++.

Palavras-chave: *Grover*, *algoritmos quânticos, computação quântica, Qiskit, OpenQASM.*

---

[1] Trabalho de Conclusão de Curso (TCC) apresentado ao Curso de Ciência da Computação do Instituto Federal Sul-rio-grandense, Câmpus Passo Fundo, como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação, na cidade de Passo Fundo, em (2021).

[2] Aluno do curso de Ciência da Computação, IFSul campus Passo Fundo.

[3] Professor do curso de Ciência da Computação, IFSul campus Passo Fundo.

1 INTRODUÇÃO

Na teoria da informação quântica, os circuitos quânticos são modelos para computação quântica, onde a computação é uma série de portas quânticas, que são transformações reversíveis em registradores quânticos de *n* bits. Basicamente, um circuito quântico é uma coleção de portas quânticas interconectadas por fios quânticos. Eles são blocos de construção de computadores que usam efeitos mecânicos para realizar tarefas. Essa estrutura semelhante é chamada de registrador n-qubit.

Com a computação atual, há problemas insolúveis com tempos viáveis. Porém, a computação quântica conseguiu resolver alguns destes problemas com eficiência (VIGNATTI, 2004). Se considerarmos os sistemas físicos, podemos comparar a eficiência da computação quântica em relação à computação clássica. Então a forma atual (levando em consideração sistemas físicos que realizam computações) da tese de Church-Turing pode ser resumida informalmente como sendo todas implementações fısicas de dispositivos computacionais podendo ser simuladas com uma sobrecarga de ordem polinomial em seu tempo de execução pela Máquina de Turing (CHURCH, 1936).

Os computadores quânticos são baseados em princípios físicos que divergem da física clássica, não necessariamente tendo que acompanhá-los. Nesta forma de computação não existe o conceito de 2 (dois) possíveis resultados (0 e 1) dos computadores convencionais, mas trabalha por meio de estados de probabilidades (0, 1 e “ambos”). Por este motivo, o estudo da computação quântica, bem como seus circuitos, se tornam muito importantes.

Este trabalho tem como finalidade apresentar estes recursos, bem como um estudo aprofundado da ferramenta para posteriores avanços e/ou utilizações do mesmo para projetos de pesquisa ou ensino metodológico para a computação quântica. A comparação entre circuito quântico e clássico será produzida para fins de estudo e comparação do sistema, através de comparações entre os tempos de execução e análises de construção. Com a utilização dos meios de execução disponibilizados (computador convencional e computador quântico de até 32-qubits), será possível medir os resultados finais através das janelas de visualização e por fim disponibilizar a conclusão do mesmo.

A ferramenta IBM *Quantum Experience* fornece uma grande gama de opções para a criação de circuitos quânticos de maneira didática, rápida e fácil. Janelas de visualizações intuitivas permitem analisar os resultados imediatamente após a execução do circuito, de maneira fácil e dinâmica, auxiliando o usuário em sua conclusão sobre o circuito. A IBM disponibiliza uma grande variedade de exemplos de circuitos, variando de problemas famosos, tais como o algoritmo de Grover, algoritmo de Shor, algoritmo Deutsch-Jozsa e entre outros, até circuitos simples para iniciação e aprendizado da ferramenta (IBM, 2020). Cada exemplo possui uma página dedicada explicando seu problema e seu funcionamento junto da solução quântica.

2 METODOLOGIA

Neste capítulo será abordado quais os métodos que foram utilizados para realizar a pesquisa, qual o instrumento que foi utilizado para a coleta de dados e o cenário. Nesta pesquisa foi utilizado a abordagem quantitativa para a coleta de dados.

Foram utilizadas algumas técnicas de pesquisa, como a pesquisa bibliográfica, através de livros e periódicos sobre o assunto, a pesquisa documental, análises em portais que ainda não receberam tratamento analítico, e por fim, a pesquisa experimental, que torna possível a manipulação direta de variáveis relacionadas com o objeto de assunto.

Como instrumento de coleta de dados, foram utilizados dois algoritmos de busca em listas, ordenada e genérica. Calculando a média de iterações que cada tipo de busca atinge, através de cinquenta testes unitários de cada busca, se obteve resultados relevantes para meios de comparação. Os algoritmos de busca (Binária e Sequencial) foram implementados na linguagem C++, e seus resultados foram salvos em uma tabela para melhor visualização e comparação dos resultados.

Utilizando a ferramenta da IBM Quantum Composer, foi possível analisar circuitos quânticos e verificar se seus resultados podem ser precisos. O trabalho apresenta o algoritmo de Grover de dois qubits, como um modelo mais simplificado, para a visualização de como o circuito funciona. Segundo Grover (1996), com seu

algoritmo é possível fazer uma busca em uma lista não ordenada (genérica) e encontrar seu resultado com apenas $\sqrt{N}$ iterações com o banco, e com isso, foi possível comparar este algoritmo quântico com os demais algoritmos clássicos citados acima.

3 COMPUTAÇÃO CLÁSSICA

Conhecer os conceitos básicos da computação clássica é essencial para o entendimento da computação quântica. Tais conceitos serão mostrados a seguir.

3.1 MÁQUINA DE TURING

Em 1936, Alan M. Turing apresentou uma teoria aos seus colegas matemáticos de que era possível executar operações computacionais em uma máquina que possuísse as regras de um sistema formal. Essa máquina foi chamada de Máquina de Turing (VIGNATTI, 2004). Sua teoria foi publicada em um artigo com o título "*On Computable Numbers, with an application on the Entscheidungsproblem*" (TURING, 1936). *Entscheidungsproblem*, é uma expressão alemã que significa "problema de decisão", quando o matemático David Hilbert esclareceu o problema Entscheidungsproblem, muitos problemas matemáticos foram resolvidos de forma algorítmica. Ou seja, é uma maneira de encontrar um algoritmo genérico que decida se, para uma dada ordem lógica a sentença seja válida ou não, utilizando da lógica simbólica (TURING, 1936). No mesmo artigo, Turing provou que não existe uma possível solução para o Entscheidungsproblem apresentando o Problema da Parada, ou seja, não há algoritmo que decide se uma dada Máquina de Turing irá parar ou não (terminar a computação).

3.2 PROBLEMAS EFICIENTEMENTE COMPUTÁVEIS

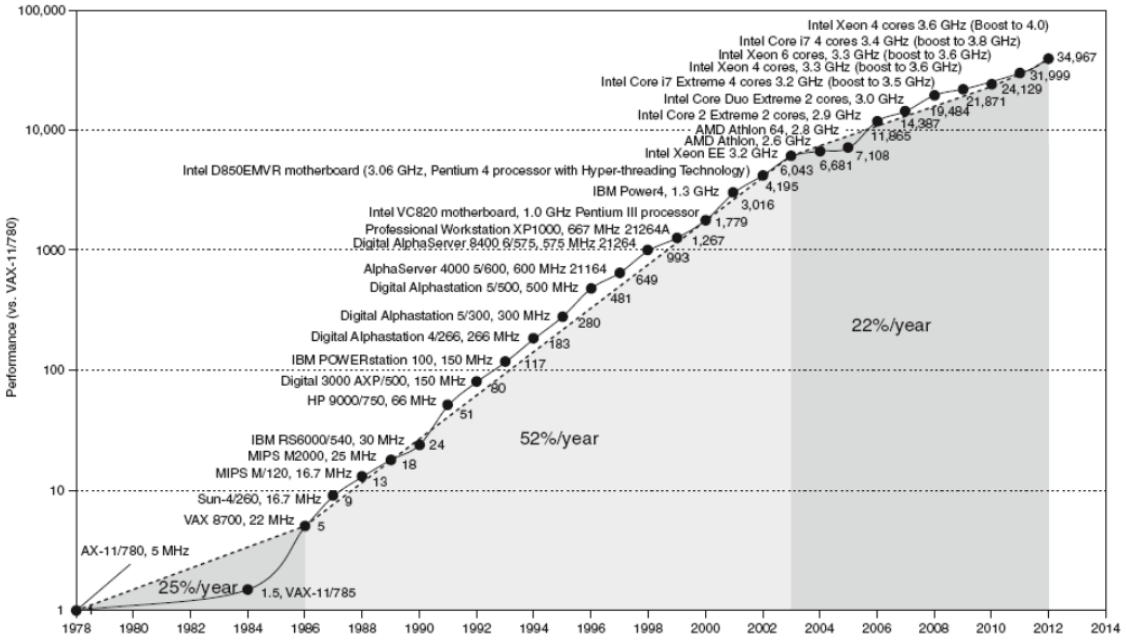
Alonzo Church em 1936 (no mesmo ano em que Alan M. Turing apresentou sua teoria) também desenvolveu um trabalho para responder o desafio de Hilbert, porém, o trabalho de Turing é considerado mais acessível e intuitivo. A tese *Church-Turing* afirma que todos os problemas ditos computáveis são problemas que são resolvidos por uma Máquina de Turing (CHURCH, 1936).

Problemas computados rapidamente com resposta são chamados de *eficientemente computáveis.* De maneira formal, na teoria da complexidade computacional, os problemas eficientemente computáveis são denominados de classe *P*, cuja classe define que os problemas podem ser resolvidos em tempo Polinomial (Problemas tratáveis). Porém, ainda existem muitos problemas importantes que são ditos não computáveis por não possuírem algoritmos eficientes para resolvê-los. Esse fato se deve ao tempo muito elevado necessário para a resolução do problema. Tais problemas não necessariamente são inexistentes, mas sim, ainda não foram descobertos algoritmos eficientes para sua resolução. Ou seja, não é possível afirmar com certeza que este problema não pertence a classe P, mas com certeza está em uma superclasse denominada NP, que consiste nos problemas que podem ser verificados em tempo polinomial (Problemas Intratáveis). Em outras palavras, sabemos que $P \subseteq NP$, mas não sabemos se $P = NP$ (TURING, 1936).

3.3 LEI DE MOORE

No ano de 1965, Gordon E. Moore, cofundador e presidente da Intel, constatou que a quantidade de transistores dos chips dobrava aproximadamente um fator a cada 18 meses. Em outras palavras, o número de transistores dos chips duplicava a cada período de 18 meses. Essa previsão ficou conhecida como a Lei de Moore, que mais tarde foi revista, alterando o período para 24 meses (ou 2 anos)(MOORE, 1965). Na Figura 1 podemos ver o gráfico da evolução da quantidade de transistores nos processadores e da Lei de Moore.

Figura 1: *Gráfico da evolução dos transistores.*



Fonte: PATTERSON, 2016.

Por 50 anos, a Lei de Moore tem sido “cumprida” pelas grandes empresas do setor, que lançaram novos processadores e memórias cuja quantidade de transistores dobravam a cada dois anos. Como mostrado na Figura 1, é possível notar que por volta de 2004 a evolução da tecnologia de fabricação deixou de acompanhar o postulado da Lei de Moore. Devido a isto, a Intel mudou a forma do seu ciclo de evolução de processadores. Este novo ciclo é denominado informalmente de "tick-tock", onde "tick" é a introdução de novos processos de litografia e miniaturização da fabricação, nos quais o espaço entre os transistores é reduzido para que mais componentes possam ser inseridos. O “tock” é a realização de mudanças profundas no microcódigo com o objetivo de otimizar o consumo de energia e fornecer uma nova arquitetura. Em resumo, "tick-tock" é um ciclo de dois anos de processos e arquitetura (INTEL, 2020).

4 COMPUTAÇÃO QUÂNTICA

4.1 QUBIT (Q-BIT)

Atualmente os computadores seguem os paradigmas da física clássica. Em seu interior, seus dados só podem ser representados por 0 e 1, simulados por um transistor, pela magnetização de um disco rígido, ou qualquer outro mecanismo que

nos forneça apenas um resultado de cada vez (SILVA, 2013). Para uma apresentação mais didática, essa obra traz uma analogia sobre a representação de um bit como uma moeda, possuindo cara ou coroa. Se fosse arremessada, cairia com o valor de “cara” ou “coroa”, representando assim, um bit normal (0 ou 1). No entanto, se as moedas se comportassem como os objetos microscópicos, que obedecem os princípios da mecânica quântica, teríamos as faces “cara” e “coroa” vistas ao mesmo tempo, ou seja, no lançamento de uma moeda, o resultado cara e coroa coexistiriam. Esse resultado é possível graças a uma das propriedades da mecânica quântica, denominada de superposição. Nesse sentido, se uma moeda quântica fosse arremessada, ela não possuiria apenas um lado sobreposto, mas sim, poderia ser visto os dois resultados simultaneamente (MATTIELO et al., 2012).

Qubit ou q-bit (pronuncia-se "cue bit", abreviação de bit quântico) é o portador físico da informação quântica. É a forma quântica de bits, e seu estado quântico pode ser representado por dois níveis marcados **|0**⟩ e **|1**⟩, e pode ser representado na "base computacional" por um vetor bidimensional (IBM, 2020):

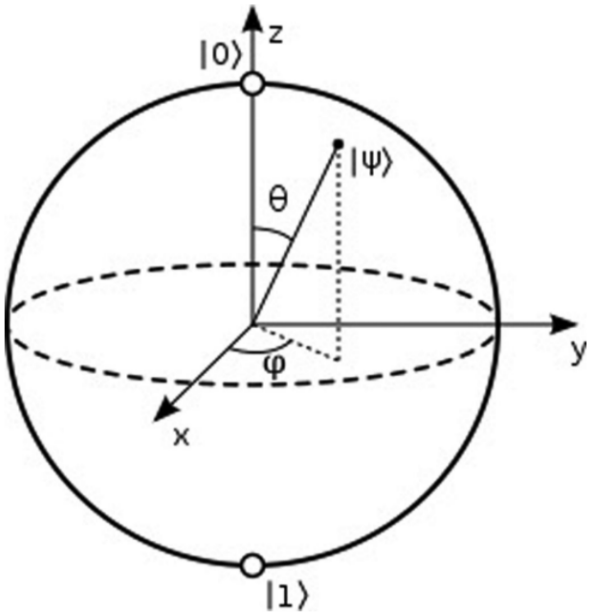
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Portanto, o qubit pode ser escrito como a superposição do estado da base computacional e formar uma base ortogonal neste espaço vetorial. Matematicamente, podemos escrever: **|ψ**⟩ **= α|0**⟩ **+ β|1**⟩, onde **ψ** representa o vetor de bits e **α** e **β** são as amplitudes de probabilidade do estado fundamental correspondente, e **|α|² + |β|² = 1**. Também podemos mapear essas amplitudes das probabilidades **α** e **β** como funções dos ângulos **θ** e **φ**, por exemplo:

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + sin(\theta/2)\,e^{i\varphi}\,|1\rangle.$$

Através da descrição do estado de q-bit, podemos agora obter uma visualização de todos os estados possíveis (em função de **θ** e **φ**) na superfície de uma esfera com raio unitário. Esta descrição geométrica do qubit é chamada de representação esférica de Bloch, onde um ponto na esfera é dado pela representação acima, e os pólos são bases computacionais **|0**⟩ e **|1**⟩, conforme a Figura 2 (NIELSEN, 2000).

Figura 2: *Esfera de Bloch, uma representação geométrica dos estados de 1-qubit. Os polos são os autoestados computacionais,* $|0\rangle$ *e* $|1\rangle$*.*



Fonte: NIELSEN, 2000.

4.2 ALGORITMOS QUÂNTICOS

Podemos dizer que um algoritmo é um conjunto de procedimentos necessários para se realizar uma determinada tarefa. Atualmente já existem alguns algoritmos quânticos propostos, que de certa forma apresentam considerável vantagem sobre os algoritmos clássicos. Um desses algoritmos quânticos foi desenvolvido por Peter Shor em 1993 (MATTIELO et al., 2012). Shor formulou um algoritmo quântico que permite decompor um número com muitos algarismos em seus fatores primos. O detalhe fundamental é que o algoritmo de Shor realiza essa tarefa em tempos muito menores do que os gastos por algoritmos clássicos.

Outro grande pesquisador, Lov Grover (1996), propôs um algoritmo capaz de realizar buscas em banco de dados extremamente mais rápidas que uma busca normal (utilizada atualmente). Uma busca normal necessita em média de $n/2$ iterações para uma busca em seu banco de dados, já no algoritmo quântico de Grover, necessitaria apenas $\sqrt{n}$. Para comparação, imagine uma busca de 10000 dados, o algoritmo quântico levaria apenas 100 passos para chegar ao resultado no pior caso.

4.3 COMPUTAÇÃO QUÂNTICA

Da mesma forma, algumas alternativas práticas estão sendo testadas para simular os qubits da computação quântica, dentre as quais podemos mencionar: pontos quânticos, ressonância magnética nuclear em líquidos, armadilhas de íons, supercondutores e outros sistemas. Portanto, vários protótipos de computadores quânticos usando uma dúzia de qubits foram testados com sucesso em laboratórios ao redor do mundo.

O desafio atualmente é o aumento do número de qubits de forma controlada. Nesse contexto aparece uma dificuldade adicional na implementação dos computadores quânticos: ler os dados durante a execução do programa sem perder todo o processamento. Essa grande dificuldade emerge de um dos princípios da mecânica quântica que torna a computação quântica interessante, pois segundo a mecânica quântica, não é possível medir ou observar um sistema quântico sem destruir a superposição de estados. Porém, isso foi conseguido mediante a utilização de uma técnica conhecida como coerência de fase, a qual permite a correção de erros sem comprometer o sistema. Para esse fim, a técnica utiliza a observação indireta para efetuar a correção de erros e manter a coerência do sistema.

5 IBM QUANTUM EXPERIENCE

Nas duas últimas décadas, o interesse pela computação quântica vem da motivação de que seus algoritmos fornecem ganhos computacionais consideráveis, em relação aos análogos clássicos. E como resultado, nos últimos anos podemos experimentar avanços tecnológicos que nos permitem contornar alguns problemas antes tidos como insolúveis (NIELSEN e CHUANG, 2000). Os computadores quânticos usam um tipo especial de função de superposição, que pode exibir muitos estados lógicos na forma exponencial de cada vez, todos os estados de $|00...0\rangle$ a $|11...1\rangle$. Este é um feito poderoso e nenhum computador clássico pode alcançá-lo (IBM, 2020).

Um dos primeiros resultados do interesse pela computação quântica foi o surgimento dos simuladores quânticos (QUANTIKI, 2020), sendo assim, circuitos quânticos simulados em uma arquitetura de computação clássica. O objetivo

principal do simulador é fornecer ferramentas de teste de circuitos e algoritmos quânticos, seja para pesquisa e/ou para prática de ensino. Pois este é o momento certo para construir e participar de uma nova comunidade de aprendizes quânticos, estimulando o interesse de pessoas que são curiosas e promover a intuição quântica na comunidade mais ampla. Ao tornar os conceitos quânticos mais amplamente compreendidos, mesmo em um nível geral, podemos explorar ainda mais todas as possibilidades oferecidas pela computação quântica e levar seu poder excitante a um limite da física clássica (IBM, 2020).

O verdadeiro desafio da física quântica é internalizar ideias que são contra-intuitivas na experiência diária no mundo físico. Essas ideias são, obviamente, limitadas pela física clássica. Para compreender o mundo quântico, você deve desenvolver novas intuições para um conjunto de leis simples, mas muito diferentes (e muitas vezes surpreendentes). Há dois princípios contra-intuitivos pregados na física quântica (IBM, 2020):

1. Um sistema físico em um estado definido ainda pode se comportar aleatoriamente.
2. Dois sistemas que estão muito distantes para influenciar um ao outro podem, no entanto, se comportar de maneiras que, embora individualmente aleatórias, são de alguma forma fortemente correlacionadas .

5.1 CIRCUIT COMPOSER

O IBM-Q é um processador quântico com até 32 qubits que pode ser acessado remotamente via internet. Depois de montar um determinado circuito usando as portas quânticas disponíveis, a plataforma permite duas possibilidades: simular circuitos quânticos em computadores convencionais e/ou realizar processamento em hardware quântico de uso geral de até 32-qubits (IBM, 2020). Portanto, os experimentos em IBM-Q incluem: (a) Especificar o circuito usando uma interface gráfica ou um editor de texto disponível na plataforma; (b) Executar o circuito no simulador e / ou dispositivo real; (c) Medir os qubits.

A IBM também disponibiliza um glossário de operações clássicas e quânticas que podem ser usadas para manipular os qubits no circuito quântico. As operações

incluem portas quânticas, como por exemplo a porta de Hadamard, e operações que não são portas quânticas, bem como a operação de medição. Após executar um circuito, é criado um projeto ("*job*") que fica salvo na conta do usuário para um posterior acesso, informando os dados principais como, tempo decorrido de algumas etapas, tipo de computador quântico utilizado e histograma, sendo ainda possível fazer o *download* de cada documento.

6 CIRCUITO ALGORITMO DE GROVER

Uma das vantagens que um computador quântico tem sobre um computador clássico é sua velocidade superior de busca em bancos de dados. O algoritmo de Grover demonstra essa capacidade. Esse algoritmo pode acelerar um problema de pesquisa não estruturada quadraticamente, mas seu uso não se estende apenas a isso, pode servir como um truque geral ou sub-rotina para obter melhorias de tempo de execução quadrático para uma variedade de outros algoritmos. Isso é chamado de truque de amplificação de amplitude (IBM, 2020).

6.1 PESQUISA NÃO ESTRUTURADA

Suponha que você receba uma grande lista de *N* itens. Entre esses itens está um item com uma propriedade exclusiva que desejamos localizar. Chamaremos este de vencedor (w). Pense em cada item da lista como uma caixa de uma cor específica. Digamos que todos os itens da lista estejam cinza, exceto o item desejado (w), que é azul. Como o exemplo da Figura 4.

Figura 4: *Lista de tamanho N representando os itens cinzas e o item vencedor (azul).*

Fonte: Própria, 2021.

Para encontrar a caixa azul usando computação clássica, seria necessário verificar em média *N/2* dessas caixas e, na pior das hipóteses, todas *N* delas. Em um computador quântico, no entanto, podemos encontrar o item marcado em aproximadamente $\sqrt{N}$ passos com o truque de *amplificação de amplitude de Grover*. Um aumento de velocidade quadrático é, de fato, uma economia de tempo substancial para localizar itens marcados em listas longas. Além disso, o algoritmo não utiliza a estrutura interna da lista, o que a torna genérica; é por isso que ele fornece imediatamente uma aceleração quântica quadrática para muitos problemas clássicos.

6.2 ORÁCULO

Uma maneira de codificar essa lista é em termos de uma função f, que retorna para todos os itens não marcados (x) e $f(w)$ = 1 para o vencedor. Para usar um computador quântico para este problema, devemos fornecer os itens em superposição a esta função, então codificamos a função em uma matriz unitária chamada *oráculo*. Primeiro, escolhemos uma codificação binária dos itens (x,w) ∈ {0,1}^{n} de modo que $N = 2^n$. Agora podemos representá-lo em termos de qubits em um computador quântico. Em seguida, definimos a matriz do oráculo Uf para agir em qualquer um dos estados de base simples e padrão $|x\rangle$ de$Uf|x\rangle = (-1)^{f(x)}|x\rangle$. Nós vemos que se x é um item não marcado, o oráculo não faz nada para o estado. No entanto, quando aplicamos o oráculo ao estado básico $|w\rangle$, mapeia $Uf|w\rangle = -|w\rangle$. Geometricamente, esta matriz unitária corresponde a uma reflexão sobre a origem do item marcado em um $N = 2^n$ espaço vetorial dimensional.

O oráculo marca o estado procurado negando a sua amplitude caso seja o qubit de estado desejado, caso contrário, nada é modificado. Como a probabilidade de observação de um qubit é dada pela norma de sua amplitude ao quadrado, negar a amplitude não afetará esse valor.

6.3 AMPLIFICAÇÃO DE AMPLITUDE

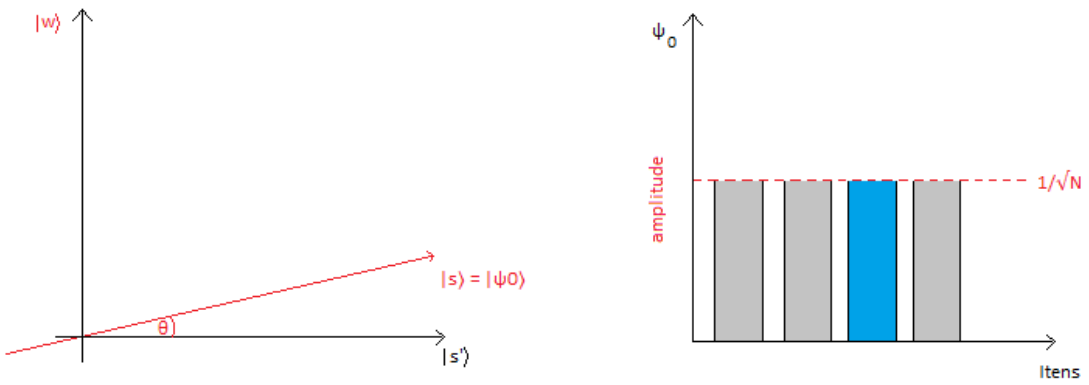
Antes de olhar a lista de itens, não temos ideia de onde está o item marcado. Portanto, qualquer suposição de sua localização é tão boa quanto qualquer outra. Então, as chances de adivinhar o valor certo (w) é 1 em 2^n, sendo a média de

tentativas para adivinhar o item correto $N = 2^n$. No procedimento chamado de *amplificação de amplitude*, aumenta-se (amplifica) a amplitude do item marcado, o que diminui a amplitude dos outros itens, de modo que a medição do estado final retornará o item certo (w) com quase certeza.

Este algoritmo tem uma boa interpretação geométrica em termos de duas reflexões, que geram uma rotação em um plano bidimensional. Os únicos dois estados especiais que devemos considerar são o vencedor $|w\rangle$ e a superposição uniforme |s⟩. Esses dois vetores abrangem um plano bidimensional, não sendo muito perpendiculares porque $|w\rangle$ ocorre na superposição com amplitude $N^{-1/2}$também. No entanto, pode-se introduzir um estado adicional |s'⟩ que está no intervalo destes dois vetores, que é perpendicular ao $|w\rangle$, e é obtido de |s⟩ removendo $|w\rangle$ e o reescalonando.

Na primeira etapa o procedimento de amplificação de amplitude começa na superposição uniforme |s⟩. Em $t = 0$, o estado inicial é $|\psi_0\rangle = |s\rangle$. Como na Figura 5, o gráfico a esquerda corresponde ao plano bidimensional medido por $|w\rangle$ e |s⟩. O gráfico à direita é um gráfico de barras das amplitudes do estado para o caso $N = 2^2 = 4$. A amplitude média é indicada por uma linha tracejada.

Figura 5: *Gráfico a esquerda em plano bidimensional e a direita com as barras de amplitudes.*

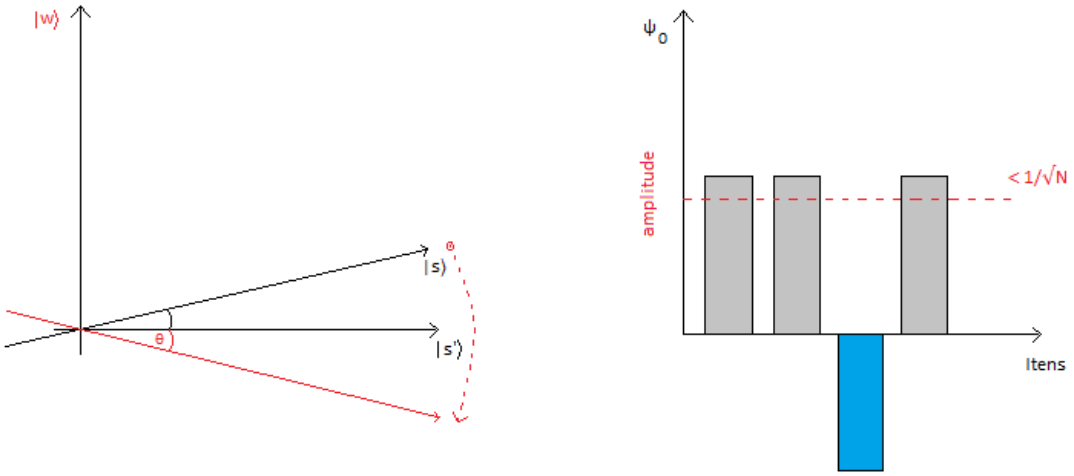


Fonte: Própria, 2021.

No próximo passo, aplicamos a reflexão do *oráculo Uf* para o estado $Uf|\psi_t\rangle = |\psi_{t'}\rangle$. Geometricamente, isso corresponde a um reflexo do estado $|\psi_t\rangle$ sobre -$|w\rangle$. Esta transformação significa que amplitude na frente do $|w\rangle$ torna o

negativo, o que por sua vez significa que a amplitude média foi reduzida, como mostra a Figura 6.

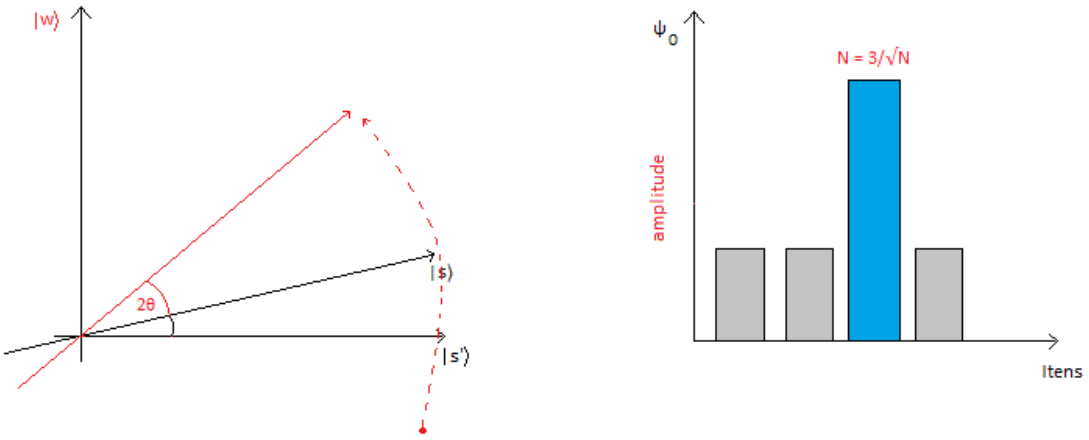
Figura 6: *Gráficos apresentando a reflexão gerada pelo oráculo.*



Fonte: Própria, 2021.

Por fim, é aplicada uma reflexão adicional U_s sobre o estado |s⟩. Na notação de Dirac esta reflexão é escrita $U_s = 2|s\rangle\langle s| - 1$. Esta transformação mapeia o estado $U_s|\psi_{t'}\rangle$e completa a transformação $|\psi_{t+1}\rangle = U_s U_f|\psi_t\rangle$. Como segue a figura 7.

Figura 7: *Reflexão aplicada ao oráculo.*

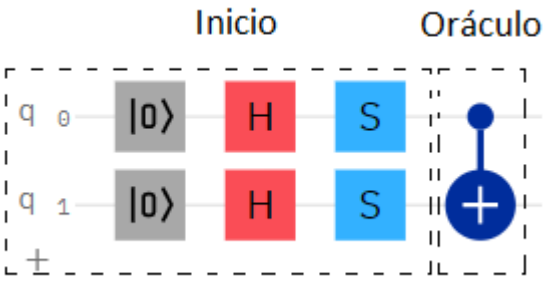


Fonte: Própria, 2021.

Esta rotação sempre corresponderá a duas reflexões. Esta transformação, gira o estado inicial |s⟩ para mais perto do estado |w⟩. No diagrama de barras de amplitude, a ação da reflexão pode ser entendida como uma reflexão sobre a amplitude média. A cada passo da primeira reflexão, que reduz a amplitude média, a amplitude negativa de |w⟩ é aumentada para cerca de três vezes o seu valor original enquanto diminui as outras amplitudes. Este procedimento é repetido aproximadamente $\sqrt{N}$ de vezes. Neste caso, pode-se observar que a amplitude de |w⟩ cresce linearmente com o número de aplicações. Portanto, é a amplitude, e não apenas a probabilidade que estão sendo ampliadas neste procedimento.

O menor circuito para a implementação desta estratégia envolve apenas dois qubits ($N = 2^2$), existindo então, apenas quatro oráculos possíveis (um para cada escolha), ou seja, são possíveis somente para |00⟩, |01⟩, |10⟩, |11⟩. Para a criação do circuito com a saída |01⟩, primeiramente é necessário inicializar o circuito com as superposições setadas em |0⟩, como na figura 8.

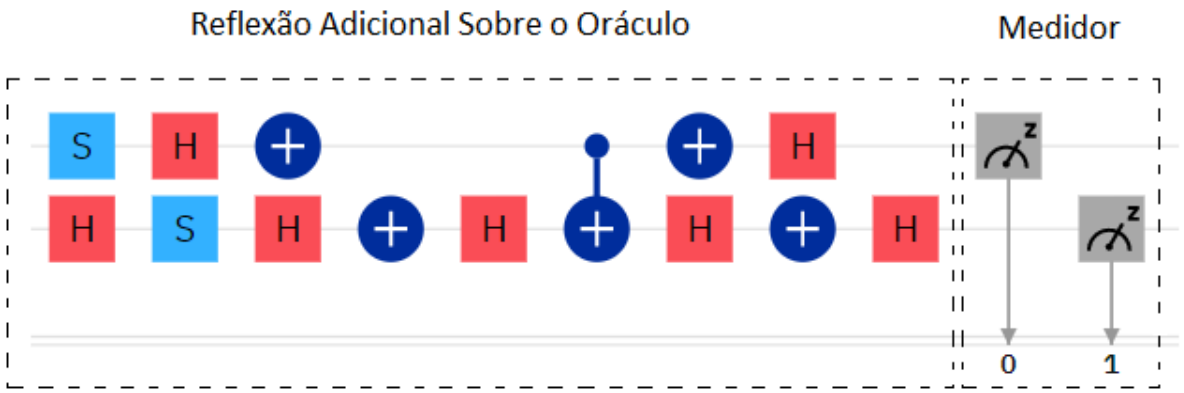
Figura 8: *Inicializando o circuito com as superposições* |0⟩ *e logo em seguida se aplica o Oráculo.*



Fonte: Própria, 2021.

Em seguida aplica-se o Oráculo (Uf) , o que faz a matriz unitária sofrer uma reflexão sobre sua origem, como citado anteriormente. Por fim, a reflexão e a medição são aplicadas como na Figura 9.

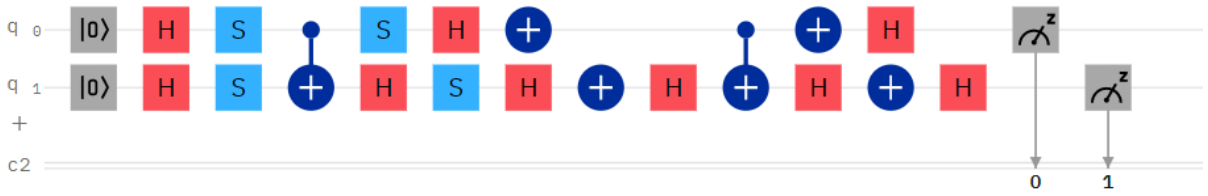
Figura 9: *Reflexão adicional sobre o Oráculo U_s,e por fim o Medidor.*



Fonte: Própria, 2021.

O circuito completo pode ser visualizado na Figura 10, quanto mais qubits forem adicionados na busca, mais linhas horizontais "*q*" terão que ser inseridas.

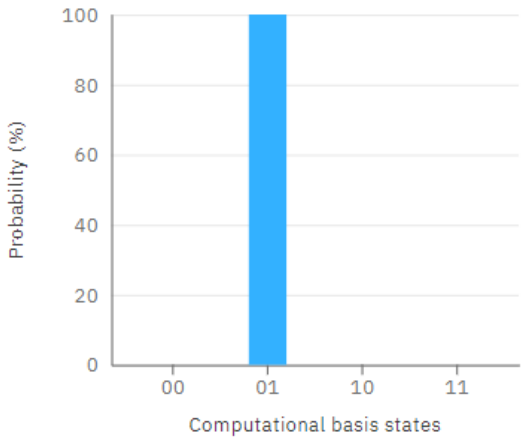
Figura 10: *Algoritmo de Grover apresentado na ferramenta Circuit Composer.*



Fonte: Própria, 2021.

O resultado na janela de visualização de probabilidade, Figura 11, retorna em 100% de probabilidade de ser o valor "01" como resultado. Este efeito somente acontece com simulações dos algoritmos quânticos, se o circuito for executado em um computador quântico físico, o resultado não será o ideal, pois ocorrerá ruídos e erros, e assim, retornará o valor um pouco abaixo de 100% de probabilidade para o valor "01".

Figura 11: *Resultado apresentado na janela de visualização da ferramenta Circuit Composer.*



Fonte: Própria, 2021.

7 RESULTADOS E ANÁLISE

Através da aplicação de um algoritmo de Busca Sequencial (BS) é possível analisar a média de iterações que este algoritmo possui em uma busca em banco de dados, e então, utilizando a ideia de que o algoritmo de Grover (AG) possui uma iteração média com o banco de dados de $\sqrt{N}$, podemos criar uma tabela para comparar ambos e determinar a eficiência de um algoritmo quântico em relação a um algoritmo clássico. Após analisar 8 tamanhos diferentes de arrays, cada um com uma amostra de 50 medidas, foi possível obter uma média que é ilustrada a seguir na Tabela 1. Nos dois algoritmos, a simulação usa uma lista não ordenada com N elementos.

A Busca Sequencial é um algoritmo simples e não é utilizado para tratar banco de dados, pois é eficientemente inviável. Porém, para meios de comparação ele se torna muito útil, pois é o único algoritmo clássico que pode ser usado em uma lista não ordenada (genérica), a mesma utilizada no algoritmo de Grover. Como pode-se observar, o algoritmo de Grover possui uma vantagem exponencial à medida que o tamanho do vetor aumenta, o que pode ser mais um fator de grande importância para provar que a computação quântica possui grande potencial de se tornar um meio usado em computadores comerciais em um futuro próximo.

Tabela 1: *Comparação entre algoritmo de Grover e Busca Sequencial.*

Tamanho do Vetor	Algoritmo	Nº de Iterações
4	G	2
	BS	2
8	G	3
	BS	4
16	G	4
	BS	8
32	G	6
	BS	15
64	G	8
	BS	29
128	G	12
	BS	65
256	G	16
	BS	145
512	G	23
	BS	282

Fonte: Própria, 2021.

Na simulação entre o algoritmo de Grover (G) e uma busca binária (BB), conforme Tabela 2, é possível perceber que mesmo a lista sendo ordenada para BB e lista desordenada para G, os valores não se tornam muito distintos, o que prova que a busca utilizando a computação quântica pode ser muito eficiente mesmo em condições não favoráveis.

Tabela 2: *Comparação entre algoritmo de Grover e Busca Binária.*

Tamanho do Vetor	Algoritmo	Nº de Iterações
4	G	2
	BB (lista ordenada)	2
8	G	3
	BB (lista ordenada)	2
16	G	4
	BB (lista ordenada)	2
32	G	6
	BB (lista ordenada)	4
64	G	8
	BB (lista ordenada)	5
128	G	12
	BB (lista ordenada)	6
256	G	16
	BB (lista ordenada)	6
512	G	23
	BB (lista ordenada)	8

Fonte: Própria, 2021.

8 CONCLUSÃO

Para concluir, desenvolver esse circuito permitiu compreender o alcance e o potencial da computação quântica sobre a tecnologia do futuro, restando agora criar novas ferramentas que não procuram apenas acelerar e melhorar os tempos de resposta na resolução de problemas, mas também, dar espaço para o desenvolvimento de novos softwares que permitam resolver problemas como por exemplo a segurança da informática, o que poderá ocasionar em algoritmos preferenciais aos da computação clássica e eventualmente se tornar o meio de computação atual.

Mais uma vez, é importante apontar o potencial que a computação quântica tem para solucionar certos problemas insolúveis para a computação clássica, porém, ainda é incerto se a computação quântica se tornará um meio único de computação devido aos fatores físicos que a mecânica quântica a impõe.

9 REFERÊNCIAS

MOORE, GORDON E. Moore. *Cramming more components onto integrated circuits. Electronics Magazine*. 1965.

GROVER, L. K. *A fast quantum mechanical algorithm for database search.* In Proceedings of 28th ACM Annual STOC, pp. 212-219. ACM Press New York. Philadelphia-PA/USA:1996.

CHURCH A. A note on the Entscheidungsproblem. Journal of Symbolic Logic, 1:40–41 and 101–102, 1936.

PATTERSON, David A.; HENNESSY, John L.. Computer Organization and Design: the hardware/software interface. Cambridge: Morgan Kaufmann, 2016.

The Quantiki, List of QC simulators, https://www.quantiki.org/wiki/list-qc-simulators, acessado em: 31/10/2020.

NIELSEN, M. A., CHUANG, I. L., Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, 2000).

Disponível em: <https://www.research.ibm.com/ibm-q>. Acesso em: 31/10/2020

VIGNATTI, André Luís, F. S. Netto, and L. F. Bittencourt. "Uma introdução à computação quântica." Departamento de Informática. UFPR (2004).

TURING, A. M.. On computable numbers, with an application to the entscheidungsproblem. Proceedings of the London Mathematical Society, Series 2(42):230–265, 1936-1937.

Complexidade de Algoritmos. Disponível em: <http://www.inf.ufrgs.br/~prestes/Courses/Complexity/aula26.pdf>. Acesso em: 20/11/2020.

The Tick-Tock Model Through the Years. Disponível em: <https://www.intel.com/content/www/us/en/silicon-innovations/intel-tick-tock-model-general.html?wapkw=tick>. Acesso em: 23/11/2020

SILVA, Leandro Mengue da. Estudo e Análise de Algoritmos Quânticos. 30 f. TCC (Graduação) - Curso de Física, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2013.

MATTIELLO, Felipe et al. Decifrando a computação quântica.14 f. Tese (Doutorado) - Curso de Técnico Integrado em Mecânica, Universidade Estadual de Feira de Santana, Feira de Santana, 2012.

RABELO, Wilson R.M., COSTA, Maria Lúcia M.. Uma abordagem pedagógica no ensino da computação quântica com um processador quântico de 5-qbits. Rev. Bras. Ensino Fís., São Paulo , v. 40, n. 4, 2018 .

OLIVEIRA, I. S., et al, Ciência Hoje, vol. 33, n. 193, (2003).