Evento: XXVI Jornada de Pesquisa

A UTILIZAÇÃO DA COMPUTAÇÃO QUÂNTICA EM ALGORITMOS DE BUSCA EM ARRAYS DE DADOS[1]

THE USE OF QUANTUM COMPUTING IN SEARCH ALGORITHMS IN DATA ARRAYS

Ricardo Vanni Dallasen[2], Marvin Willian Machry Pocahy[3], Maikon Cismoski dos Santos[2], André Fernando Rollwagen[2], Vanessa Lago Machado[2]

[1] Pesquisa desenvolvida no IFSUL - Instituto Federal de Educação Ciência e Tecnologia Sul Rio-Grandense, Câmpus Passo Fundo
[2] Docente do Curso de Bacharelado em Ciência da Computação do IFSUL - Câmpus Passo Fundo
[3] Bacharel em Ciência da Computação

RESUMO

A proposta deste trabalho é a geração do circuito quântico de Lov Grover na ferramenta IBM Quantum Experience e compará-lo com os algoritmos clássicos de Busca Binária e Busca Sequencial em um cenário de busca em arrays de dados. Os algoritmos de Busca Binária e Busca Sequencial foram programados em C++, já no Algoritmo de Grover, foi utilizado em todos os casos o seu pior caso (grau de complexidade) √N. Para a comparação entre os algoritmos de busca, foram utilizados 8 tamanhos de vetores e executados cada um 50 vezes para se obter uma média de resultados mais concretos.

Palavras-chave: algoritmo de Grover, algoritmos quânticos, computação quântica

ABSTRACT

The purpose of this work is to generate the Lov Grover quantum circuit in the IBM Quantum Experience tool and compare it with the classic binary search and sequential search algorithms in a data array search scenario. The Binary Search and Sequential Search algorithms were programmed in C++, while in Grover's Algorithm, its worst case (degree of complexity) √N was used in all cases. For the comparison between the search algorithms, 8 vector sizes were used and each one executed 50 times to obtain an average of more concrete results. With the results, it was possible to understand the scope and potential of quantum computing on the technology of the future, however, it is a computing medium that needs evolution, because in some cases classical computing still has better results.

Keywords:Grover algorithm, quantum algorithms, quantum computing.

INTRODUÇÃO

Na computação clássica existem problemas insolúveis em 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 fisicas 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.

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 raiz de N ($\sqrt{N}$) iterações com o banco, e com isso, foi possível comparar este algoritmo quântico com os demais algoritmos clássicos citados acima.

CIRCUITO DO ALGORITMO DE GROVER

Uma das vantagens que um computador quântico tem sobre um computador clássico é sua velocidade superior de busca em arrays 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).

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 mostrado na Figura 1.

Figura 1: Lista de tamanho N representando um conjunto de dados e o item vencedor em azul.

Fonte: Autoria própria.

Para encontrar a caixa azul usando computação clássica em uma lista não ordenada, 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 √N (GROVER, 1996) 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.

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 $(x,w) \in \{0,1\}^n$ de modo que $N = 2^n$, onde n é o tamanho do array. 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 bidimensional (IBM, 2021).

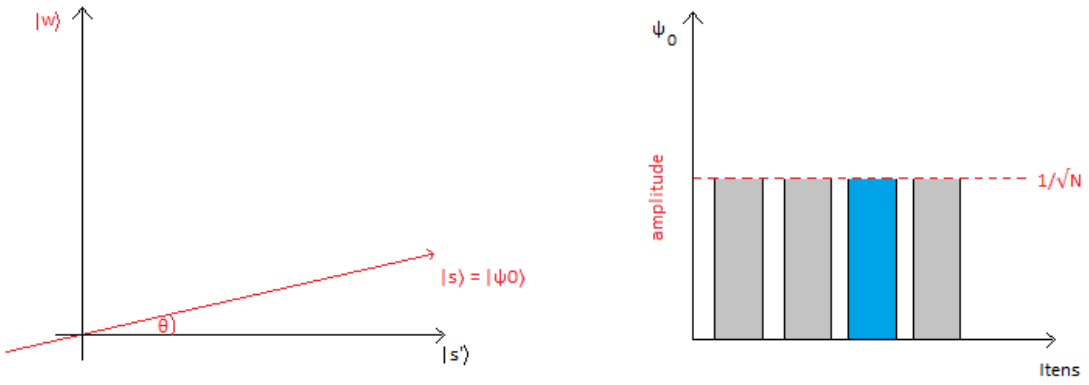
O oráculo marca o estado procurado negando a sua amplitude caso seja o qubit de estado desejado, caso contrário, nada é modificado. Como a probabilidade de observação de um qubit é dada pela norma de sua amplitude ao quadrado, negar a amplitude não afetará esse valor. Antes de olhar a lista de itens, 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 (IBM, 2021).

Os únicos dois estados especiais que devemos considerar são o vencedor $|w\rangle$ e a superposição uniforme $|s\rangle$. 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 $|s'\rangle$ que está no intervalo destes dois vetores, que é perpendicular ao $|w\rangle$, e é obtido de $|s\rangle$ removendo $|w\rangle$ e o reescalonando.

Na primeira etapa o procedimento de amplificação de amplitude começa na superposição uniforme $|s\rangle$. Em t = 0, o estado inicial é $|\psi 0\rangle = |s\rangle$. Na Figura 2 são mostrados dois gráficos, o da esquerda corresponde ao plano bidimensional medido por $|w\rangle$ e $|s\rangle$. 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.

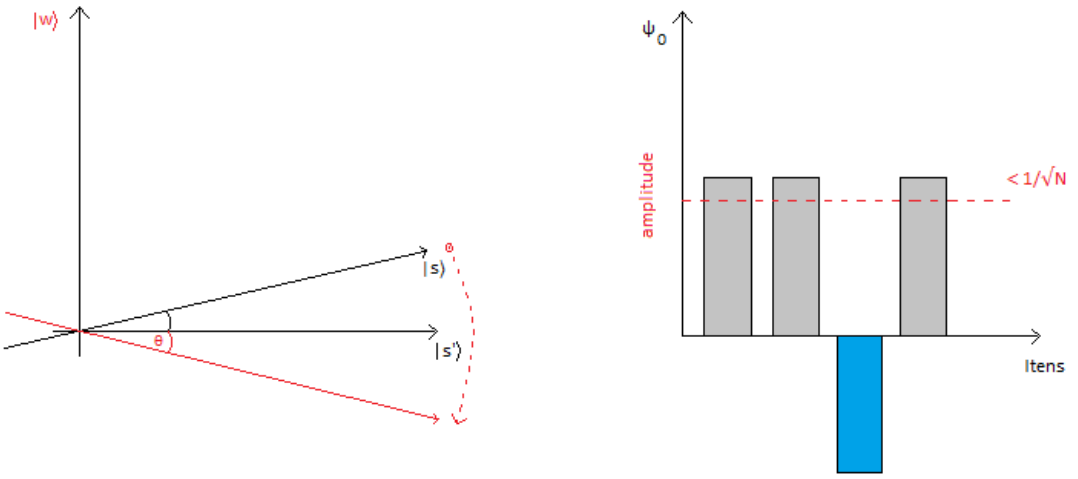
Figura 2: Gráfico a esquerda em plano bidimensional e a direita com as barras de amplitudes.



Fonte: Autoria própria.

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 3.

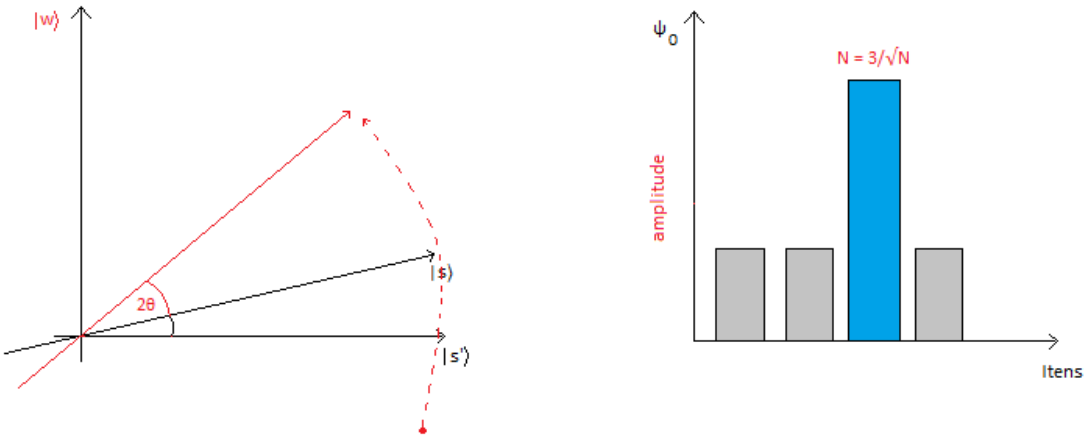
Figura 3: Gráficos apresentando a reflexão gerada pelo oráculo.



Fonte: Autoria própria.

Por fim, é aplicada uma reflexão adicional Us 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 mostrado na figura 4.

Figura 4: Reflexão aplicada ao oráculo.



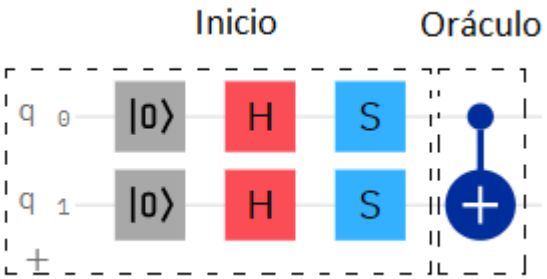
Fonte: Autoria própria.

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 √N de vezes. Neste caso, pode-se observar que a amplitude de $|w\rangle$ 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 $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Para a criação do circuito com a saída $|01\rangle$, primeiramente é necessário inicializar o circuito com as superposições setadas em $|0\rangle$, como mostrado na Figura 4.

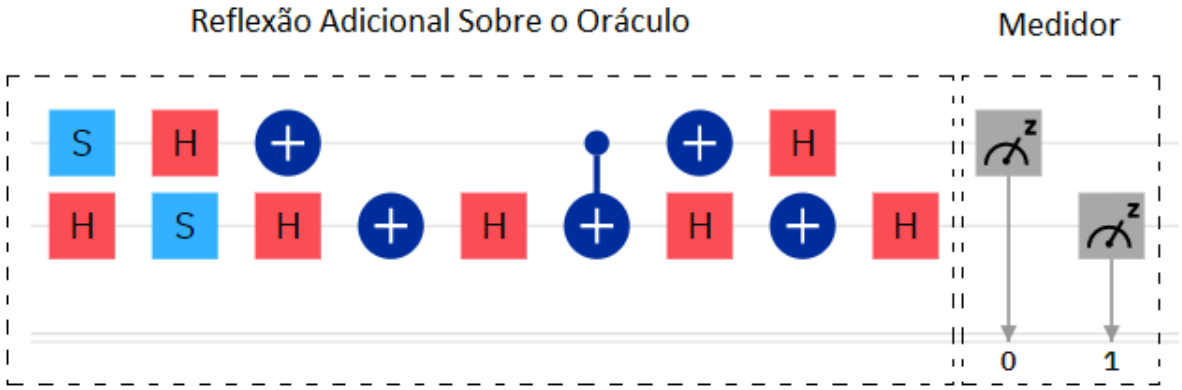
Figura 4: Inicializando o circuito com as superposições $|0\rangle$ e logo em seguida se aplica o Oráculo.



Fonte: Autoria própria.

Em seguida aplica-se o Oráculo (U_f) , 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 mostra a Figura 5.

Figura 5: Reflexão adicional sobre o Oráculo U_s, e por fim o Medidor.

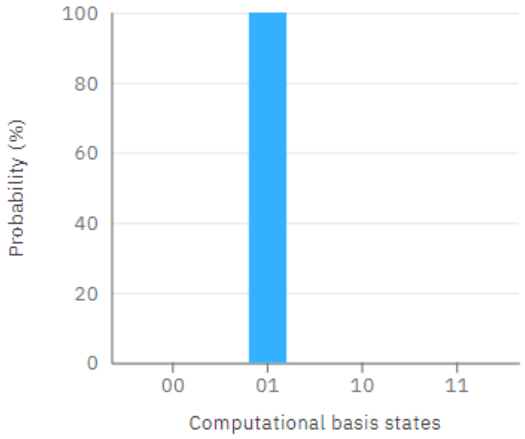


Fonte: Autoria própria.

O resultado na janela de visualização de probabilidade retorna em 100% de probabilidade de ser o valor “01” como resultado. Isso é mostrado na Figura 6. 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 6: Resultado apresentado na janela de visualização da ferramenta Circuit Composer.



Fonte: Autoria própria.

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 um array de dados, e então, utilizando a ideia de que o algoritmo de Grover (G) possui uma iteração média 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.

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: Autoria própria.

A Busca Sequencial é um algoritmo simples e não é utilizado para tratar nenhum tipo de busca 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 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.

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: Autoria própria.

CONSIDERAÇÕES FINAIS

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 possui. Em determinadas aplicações a computação quântica apresenta Em trabalhos futuros pretendemos comparar o algoritmo de Grover com outros algoritmos quânticos. Outra linha para trabalhos futuros é a utilização do algoritmo de Grover para a resolução de problemas de criptografia.

REFERÊNCIAS BIBLIOGRÁFICAS

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

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.

IBM. **IBM Quantum**. 2020. Disponível em: https://quantum-computing.ibm.com/. Acesso em: 31 out. 2020.

IBM. **IBM Quantum Composer Docs:** Grover's algorithm. 2021. Disponível em: https://quantum-computing.ibm.com/composer/docs/iqx/guide/grovers-algorithm. Acesso em: 20 mar. 2021.

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