ALGORITMO QUÂNTICO PARA ENCONTRAR VALORES MÍNIMOS EM UMA MEMÓRIA QUÂNTICA DE ACESSO ALEATÓRIO (QRAM)

Lucas Queiroz Galvão[1]; Anton Simen Albino[1]; Mauro Queiroz Nooblath Neto[1]; João Marcelo Silva Souza[2]
[1] Bolsista de Pesquisa, Desenvolvimento e Inovação (PD&I) Quantum,; lucas.queiroz@fbter.org.br
[2] Centro Universitário SENAI CIMATEC; Salvador - BA; joao.marcelo@fieb.org.br

RESUMO

A busca de valores mínimos em um banco de dados não estruturado é uma tarefa fundamental na Ciência da Computação. Entretanto, o algoritmo determinístico clássico pode encontrar o valor mínimo com uma complexidade de tempo que cresce linearmente com o número de elementos no banco de dados. Neste artigo, apresentamos a proposta de um algoritmo quântico, fundamentado no Algoritmo de Grover, para encontrar o valor mínimo de um banco de dados, que é quadraticamente mais rápido que seus melhores análogos clássicos. Assumimos uma Memória Quântica de Acesso Aleatório (*QRAM*) que armazena valores de um banco de dados e realiza uma busca iterativa baseada em um oráculo, cujo papel é limitar os valores buscados controlando os estados dos qubits mais significativos. Uma análise de complexidade foi realizada para demonstrar a vantagem deste algoritmo quântico sobre seus equivalentes clássicos.

PALAVRAS-CHAVE: Busca de valores mínimos, Quantum RAM, Algoritmo de Grover.

1. INTRODUÇÃO

A Memória de Acesso Aleatório (*Random Access Memory – RAM*) é uma memória volátil usada na computação para armazenar e recuperar informações por meio de bits[1]. Similarmente, o conceito de *Quantum RAM* (QRAM) surge com o mesmo objetivo, mas empregando *quantum bits*, ou simplesmente qubits, para aplicar uma sobreposição de estados, de modo a obter resultados mais eficientes para aplicações computacionais, sejam elas quânticas ou clássicas. Diversos trabalhos discutem o potencial de suas aplicações para otimizar a execução de algoritmos quânticos, incluindo busca quântica em um banco de dados clássico[2] e algoritmos para resolver sistemas lineares[3].

Nesse sentido, esforços têm sido feitos para construir algoritmos quânticos que sejam capazes de acessar uma QRAM de forma otimizada. Isso pode ser feito usando algoritmos de busca quântica para encontrar os valores desejados armazenados em suas células. Um exemplo bem conhecido é o chamado algoritmo de descoberta mínima de Dürr-Hoyer, que emprega o algoritmo de Grover como uma sub-rotina fundamental para encontrar a maior ou menor entrada em uma lista[4]. Várias estratégias sugeridas para busca de valores mínimos foram propostas com base no algoritmo de Dürr-Hoyer, com aplicações em física de altas energias[5] e comunicações não-cabeadas (*wireless*)[6].

Neste trabalho, baseado no conceito central do algoritmo de Durr-Hoyer, aplicamos o Algoritmo de Grover como uma subrotina para desenvolver um algoritmo quântico para identificar o menor valor em um conjunto de dados clássico armazenado em uma QRAM. O algoritmo *Quantum Minimum Search (QMS)* proposto é baseado na mudança iterativa da função oráculo[4], que limita os valores pesquisados controlando os estados dos qubits mais significativos.Na estrutura do presente trabalho, apresentamos a descrição do algoritmo proposto, descrevendo seu circuito e implementação, de modo a abordar um exemplo para encontrar o mínimo em uma lista de quatro valores reais utilizando o algoritmo proposto. Na sequência, analisamos a complexidade do algoritmo QSM em comparação com algoritmos clássicos.

2. METODOLOGIA

Nesta seção, será descrito o método utilizado para obter os resultados, sendo, portanto, a descrição do algoritmo QSM. Para realizar a tarefa de encontrar o menor valor armazenado em uma QRAM, a estratégia adotada é realizar uma busca analisando os bits mais (ou menos, se quisermos o valor máximo) significativos de uma única medição, em que a subrotina especial responsável por essa tarefa é a inversão de fase iterativa, denotada no presente trabalho como operador *P*.

Na Figura 1, é possível visualizar o circuito quântico completo, em que U_x é a representação de uma QRAM, construída a partir de valores armazenados com portas multi-controladas NOT; o operador *P* é alterado iteravitamente analisando os qubits mais significativos na última medição; e *W* é o operador difusor, responsável por aumentar a probabilidade de medição do estado desejado. A ideia chave do algoritmo está

na dinâmica do operador *P*, que marcará os estados desejados. O registro adicional (qubits mais abaixo na Figura 1) é usado para representar o armazenamento de valores clássicos na QRAM e é também onde a busca é feita. Sabe-se que se os qubits mais significativos possuem bits no estado 0, o que significa que, na base decimal, esse número é menor do que se os qubits mais significativos estivessem no estado 1. Com base nesta lógica, o operador *P* pode ser construído através da porta multi-controlada NOT tendo qubits com controle em 0 ou com controle em 1.

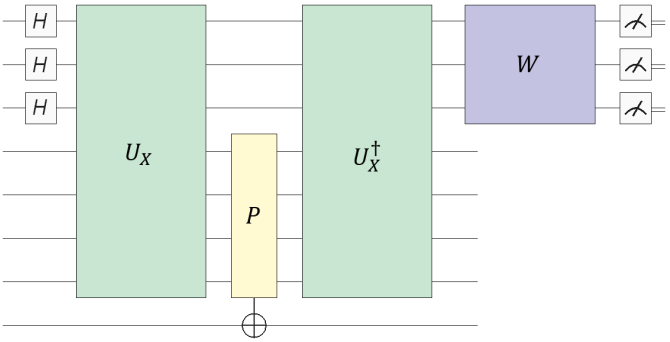

Figura 1 – Circuito do algoritmo QSM, considerando uma QRAM de 4 qubits.

3. RESULTADOS E DISCUSSÃO

Conforme a descrição do algoritmo QSM na seção anterior, o Algoritmo de Grover pode ser usado iterativamente para amplificar estados (índice), que correspondem a valores menores que o último, quadraticamente mais rápido que seus equivalentes clássicos[4]. Por exemplo, supondo o seguinte conjunto de dados $\vec{y} = \{5, 4, 12, 10, 8\}$, as entradas da lista podem ser representadas na base computacional (com quatro qubits) como $\vec{y} = \{|0101>, |0100>, |1100>, |1010>, |1000>\}$.

Se a primeira estimativa (puramente clássica) for, por exemplo, $10 \rightarrow 1010$, é muito improvável que este número seja o mais baixo. Isso pode ser confirmado procurando o número cujo qubit mais significativo é |0>. Assim, uma iteração de Grover com este oráculo marca todos os estados cujo qubit mais significativo está no estado |0>, correspondendo aos prováveis valores mínimos na lista. Depois disso, realizando a busca de Grover naquele qubit mais significativo, os estados $|0100>$ e $|0101>$ terão igual probabilidade de serem medidos. Se obtivermos o estado $|0101>$ após a medição, o próximo passo é procurar valores cujos dois primeiros dígitos binários sejam $|00>$. Esse resultado pode ser visualizado na Figura 2, no histograma à esquerda.

No caso em que $y_i < y_{i+1}$, o processo mostra que o mínimo é $|0101>$ ou um número menor cujos dois primeiros qubits mais significativos também sejam $|01>$, então é necessário buscar valores cujos terceiros qubits mais significativos sejam $|010>$. Neste caso particular, a única tarefa que resta é verificar se $|0100>$ está na QRAM, pois é o menor número possível cujos três qubits mais significativos estão no estado $|010>$. Neste exemplo, o estado $|0100>$ será medido com aproximadamente 100% de probabilidade. O processo é feito iterativamente com o restante dos qubits para encontrar o mínimo $y_{min} = |0100>$com certeza. Esse resultado pode ser visualizado na Figura 2, no histograma à direita.

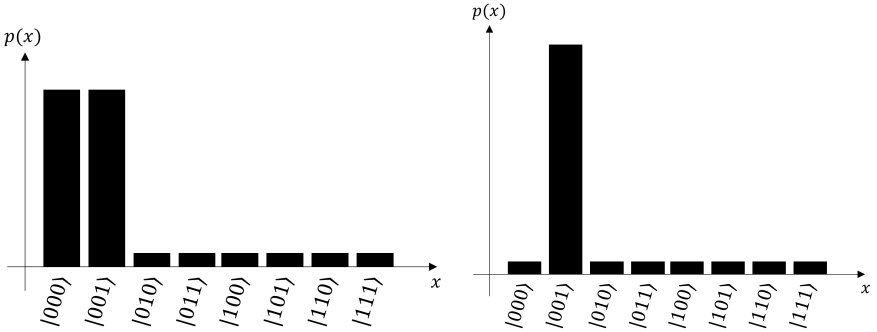

Figura 2 – Histograma com os resultados das iterações.

A fim de comparar o desempenho do QSM com algoritmos clássicos, foi feita uma análise da complexidade de tempo de execução de ambos. Na Figura 3, a sombra entre as linhas representa a faixa de complexidade entre algoritmos clássicos e quânticos. Os limites superior e inferior dos algoritmos clássicos (azul) têm complexidades de tempo de $O(\frac{3}{2}N - 2)$ e $O(N - 1)$. Para o caso do algoritmo quântico (laranja), foram traçados os limites superior e inferior para os casos onde $C_q = 14$ e $c_q = 6$, respectivamente. Nesta lógica, os algoritmos clássicos demonstram uma evolução polinomial, enquanto o QSM demonstra, de fato, uma evolução da ordem da raiz quadrada $O(\sqrt{N})$, representando portanto um crescimento quadrático, conforme discutido anteriormente.

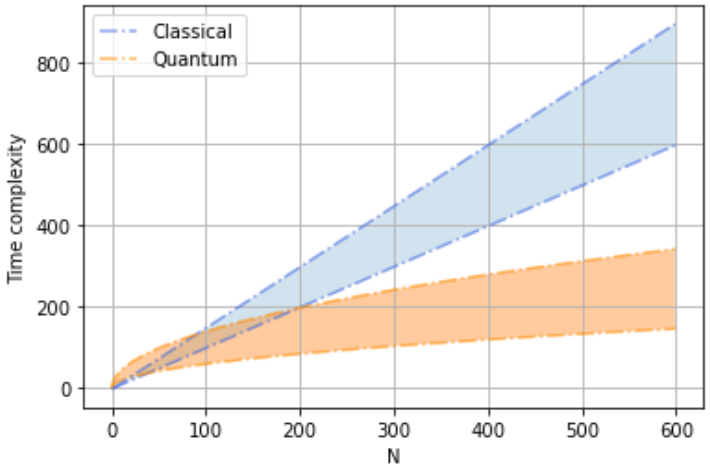

Figura 3 – Complexidade de tempo dos algoritmos clássicos (azul) e do QSM (laranja).

4. CONSIDERAÇÕES FINAIS

A Computação Quântica é amplamente discutida como uma possibilidade de superar a Computação Clássica em uma ampla gama de problemas. O clássico problema de busca mínima é considerado um desses exemplos, especialmente caracterizado pela complexidade linear e conectado a uma ampla variedade de aplicações no domínio da Ciência da Computação. Neste cenário, este trabalho apresentou um algoritmo quântico para encontrar o valor mínimo de um banco de dados que é quadraticamente mais rápido que seus melhores análogos clássicos. O algoritmo é baseado na abordagem de Durr-Hoyer para encontrar um valor mínimo em uma lista não-estruturada através do uso do algoritmo de Grover como uma sub-rotina aplicada a uma QRAM que armazena valores de um banco de dados definido. Este resultado pode servir como um modelo chave para o desenvolvimento de algoritmos quânticos tolerantes a falhas.

5. REFERÊNCIAS

[1] SEDRA, A.; SMITH,K. **Microelectronic Circuits.** Londres: Oxford University Press, 2004.
[2] Di MATTEO, O; GHEORGHIU, V.; MOSCA, M. Fault tolerant resource estimation of quantum random-access memories. **IEEE Transactions on Quantum Engineering**, 2020.
[3] DUAN, B. *et al.*. A survey on HHL algorithm: From theory to application in quantum machine learning. **Physics Letters A**, 2020.
[4] GROVER, L. A Fast Quantum Mechanical Algorithm for Database Search. **Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing**, 1996, 212-219.
[5] LEJARZA, J.; CIERI, L.; RODRIGO, G. Quantum computing for data analysis in high energy physics. **Physical Review D**, 2022.
[6] BOTSINIS, P. *et. al.* Quantum Search Algorithms for Wireless Communications. **IEEE Communications Surveys & Tutorials**, 2018.