

## Buscas em Computadores Quânticos: O Algoritmo de Grover

André S. Mota

### Resumo

Estudo sobre algoritmos quânticos de busca, usados em computadores quânticos, que são mais eficientes do que qualquer algoritmo de busca não estruturada conhecido pela computação clássica.

### Palavras-chave:

Quântica, computação, algoritmo de busca

### Introdução

A teoria quântica de informação estuda bits quânticos, os qubits, e maneiras de armazenar, transmitir e processar informação. Um qubit é representado por um vetor ou operador densidade em um espaço de Hilbert complexo de dimensão dois. Neste espaço é possível fazer medições e testes com os qubits, sendo que para cada teste existe um conjunto de operadores de projeção ortogonais associado. Comparativamente, se um bit clássico é 0 ou 1, um qubit é uma superposição de ambos os estados, e assume um deles no momento em que é medido.

Algo muito importante para a ciência da computação são os algoritmos de busca, em que tendo como entrada uma base de dados e um dado que se deseja buscar, o algoritmo realiza a busca neste espaço. Existem diversos algoritmos que cumprem essa tarefa, com suas diferenças em termos de estrutura de dados, de eficiência e execução. Para casos em que o conjunto de dados é não-estruturado, não existe um algoritmo eficiente na computação clássica que resolva este problema. Com o advento da computação quântica, surgiu a possibilidade de realizar este tipo de busca de uma maneira mais eficiente, os chamados algoritmos quânticos de busca.

O mais simples dos algoritmos quânticos que conhecemos chama-se Algoritmo de Grover, que utiliza paralelismo quântico e encontra o dado com alta probabilidade de acerto.

### Resultados e Discussão

Primeiramente, considere um conjunto com  $n$  bits. Uma das vantagens da teoria quântica é a possibilidade de colocar o registrador em uma superposição de todos os possíveis resultados. Matematicamente, podemos representar da seguinte forma:

$$|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

Em seguida, executamos uma instrução de oráculo neste conjunto, que coloca um sinal negativo no elemento procurado,  $w$ , representado por  $f(w) = 1$ , e mantém os outros com seus respectivos sinais positivos, quando

$f(x) = 0$  para  $x$  diferente de  $w$ , como mostrado na expressão a seguir:

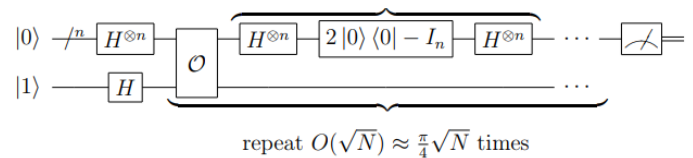
$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$$

Em seguida, aplicamos duas reflexões no conjunto, visando rotacionar o vetor de estado a cada iteração do algoritmo. A iteração deste passo é descrita pela expressão abaixo:

$$[2|\psi\rangle\langle\psi| - I] O$$

Este processo é repetido até que o estado do registrador esteja muito próximo do estado  $w$ .

O tempo total de execução de uma iteração de Grover é  $O(n)$ , devido às aplicações da função oráculo e reflexões. Como o algoritmo aplica rotações, deve-se parar a execução no momento que o vetor de estados está praticamente ortogonal em relação a sua condição inicial.



**Figura 1.** Representação do algoritmo de Grover na forma de circuito quântico.

Feito isso, uma medição neste instante dá o resultado esperado com alta probabilidade de acerto.

### Conclusão

O Algoritmo de Grover executa a busca em um conjunto de dados não-estruturado em tempo raiz de  $N$ . É um ganho considerável relação a todos os algoritmos de busca para este problema na computação clássica. Apesar de ser probabilístico, pode ser usado em casos em que o conjunto de dados é gigantesco e pode-se afirmar com quase certeza de que o resultado obtido é o correto.