# O Algoritmo de Grover

RODRIGO FEDRIZZI DILLENBURG, ENGENHARIA FÍSICA – UFRGS
SANDRA DENISE PRADO (orientadora)

O Agoritmo de Grover é uma versão quântica do algoritmo de busca, que usa o fenômeno de paralelismo quântico para buscar soluções para o problema de busca. Ele apresenta uma melhoria quadrática em relação ao algoritmo clássico. Este trabalho se dedica a explicar seu funcionamento.

## Considerações Iniciais

Os gates quânticos utilizados neste algoritmo são o Hadamard e o Pauli X. Suas representações matriciais estão apresentadas abaixo

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

## O Algoritmo:

A apresentação do algoritmo que será feita a seguir considera um espaço com N elementos e M soluções. Por conveniência, toma-se N=2^n, onde n é o número de qubits em cada estado. O algoritmo faz uso de um registro de n qubits onde são processados os elementos do espaço de busca e um registro para uso do oráculo, um conceito que será explicado a seguir.

O computador é posto inicialmente no estado $|\mathbf{0}\rangle^{\otimes n}$, que é equivalente ao estado $|0 \ldots 0\rangle$.
Aplica-se o gate Hadamard ao estado, resultando no novo estado .

$$|\psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle$$

## A Iteração de Grover

A próxima etapa do algoritmo são múltiplas aplicações do processo chamado Iteração de Grover. Por ser um processo bastante complicado, seus detalhes serão omitidos no poster. A fórmula final da aplicação de uma Iteração de Grover é:

$$G = (2|\psi\rangle\langle\psi| - I)O$$

$|\psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle$ , I é o operador Identidade e O é o oráculo, um elemento de um circuito quântico capaz de reconhecer soluções para o problema e alterar a fase do estado quando as encontra. No Algoritmo de Grover o oráculo é aplicado a um estado de superposição perfeita e esse é o segredo do seu sucesso. Um oráculo aplicado a bits clássicos é equivalente ao algoritmo clássico de busca.

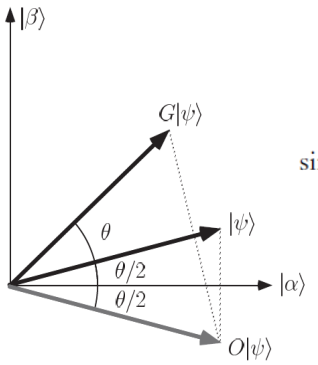
Mas, quantas vezes deve-se aplicar a Iteração de Grover? Para resolver este problema, é útil ter um visualização geométrica da ação da Iteração de Grover num estado. Usando o processo de Graham-Schmidt é possível construir uma base ortogonal para representar o estado em questão na forma

$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x{}'' |x\rangle$ $\sum_x{}''$ = soma dos x que são solução

$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x{}' |x\rangle .$ $\sum_x{}'$ = soma dos x que não são solução

Nesta base, o estado será $|\psi\rangle = \sqrt{(N-M)/N}|\alpha\rangle + \sqrt{M/N}|\beta\rangle$

A ação da Iteração de Grover sobre o estado representado na base alpha-beta pode ser representada como uma rotação




$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}$$

Rotacionar o estado sobre o ângulo $\arccos\sqrt{M/N}$ o leva ao estado beta, que é o estado das soluções do problema. No entanto, este ângulo é, na maioria das vezes, um número não inteiro. Considerando CI(x) como o inteiro mais próximo de x, O número de aplicações da Iteração de Grover deve ser

$$\mathrm{CI}\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$$

## Medição

Após as aplicações da Iteração de Grover, a medição do estado dará a resposta correta com probabilidade bastante alta. Apesar de o algoritmo não ter probabilidade 100% de sucesso, ela é bem próxima disso, então repetir o processo algumas vezes deve fornecer a resposta correta.

Com algumas contas que serão omitidas, é possível mostrar que o número de Iterações de Grover e, consequentemente, consultas ao oráculo feitas pelo Algoritmo de Grover é no máximo $(\sqrt{N/M})$, enquanto que no algoritmo clássico, esse número é $(N/M)$. Ou seja, o Algoritmo de Grover representa uma otimização quadrática em relação ao algoritmo clássico.

Imagens retiradas de: *Michael A. Nielsen, Isaac L. Chuan – Quantum Computation and Quantum Information, Cambridge.*

Instituto de Física