Análise do Algoritmo de Grover

Teo Haeser Gallarza

Universidade Federal de Santa Catarina
Centro de Ciências Físicas e Matemáticas
Departamento de Física

Março de 2020

Índice

Algoritmo de Grover

Algoritmo de Grover - Características Iniciais

É um algoritmo de busca quântica criado por Lov Kumar Grover.
Usa apenas $\mathcal{O}(\sqrt{N})$ avaliações, onde o algoritmo de busca clássico é resolvido em $\mathcal{O}(N)$ avaliações. N é o tamanho de entradas do banco de dados.

Algoritmo de Grover - Características Iniciais

- Para o funcionamento do algoritmo é necessário:
  - uma base de dados com N entradas;
  - que tem o valor ω, o qual é o valor buscado;
  - x uma posição do banco de dados;
  - Função oráculo $\begin{cases} O_F |x\rangle = -|x\rangle & \text{para } x = \omega, \text{isto é,} f(x) = 1 \\ O_F |x\rangle = |x\rangle & \text{para } x \neq \omega, \text{isto é,} f(x) = 0 \end{cases}$
  - n qubits, onde $n = \log_2 N$

Circuito

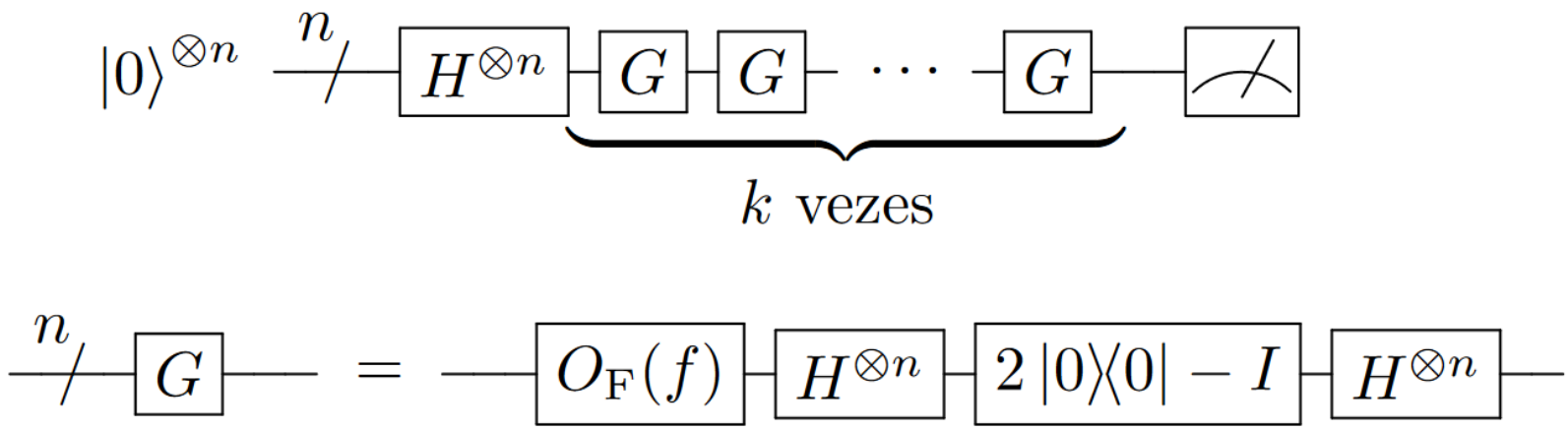


Figure: Notação Compacta Circuito Quântico

Passos do algoritmo

Considerando:

- $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = |+\rangle^{\otimes n}$

Então o operador

- $G = (2|s\rangle\langle s| - I)O_F$

É o operador de Grover

Passos do Algoritmo

Passos:

1. Inicializar o sistema
2. Realizar os próximo passo $\mathcal{O}(\sqrt{N})$ vezes
   1. Aplicar o oráculo de fases
   2. Aplicar o operador de Grover
3. É feita a medição, com uma probabilidade muito alta de ser a respota do problema

Resultado

Com isso é encontrado o vetor que satisfaz a equação do oráculo, onde $f(x) = 1$.
Porém, como determinar essa equação?

O Oráculo

O oráculo é uma implementação de um predicado em que se quer achar uma solução.
Como por exemplo, o problema SAT.

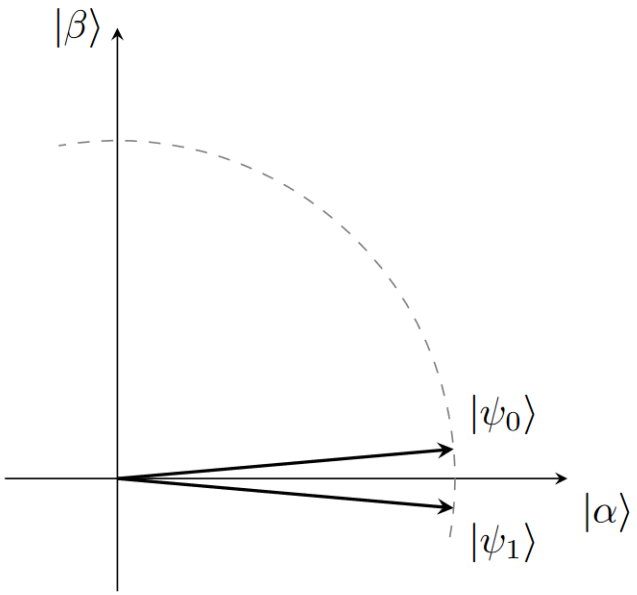
Uraculo de SAT, um exemplo

Vamos utilizar o exemplo de SAT:
Existem 3 inteiros x_1,x_2,x_3 que satisfaz :$x_1^3 + x_2^3 + x_3^3 = 42$?

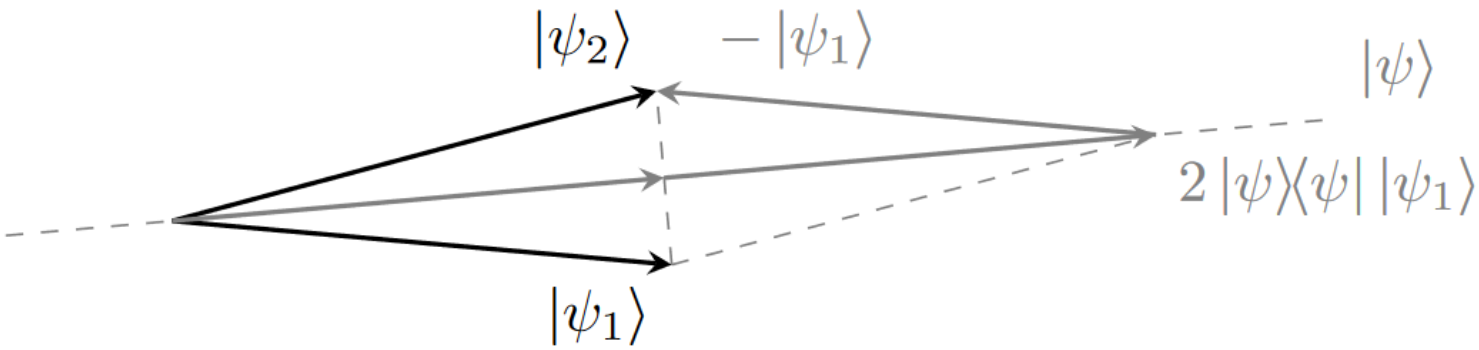
- Deve-se escrever o f com portas NAND e depois converter-las para portas CNOT, para determinar U_f
- Com isso, a combinação dos qubits representam os valores verdadeiros ou falsos para o problema SAT
- E ao se aplicar U_ω e U_s, $\mathcal{O}(\sqrt{N})$ vezes, o resultado medido nos qubits deve ser o estados que satisfaz $f(x) = 1$

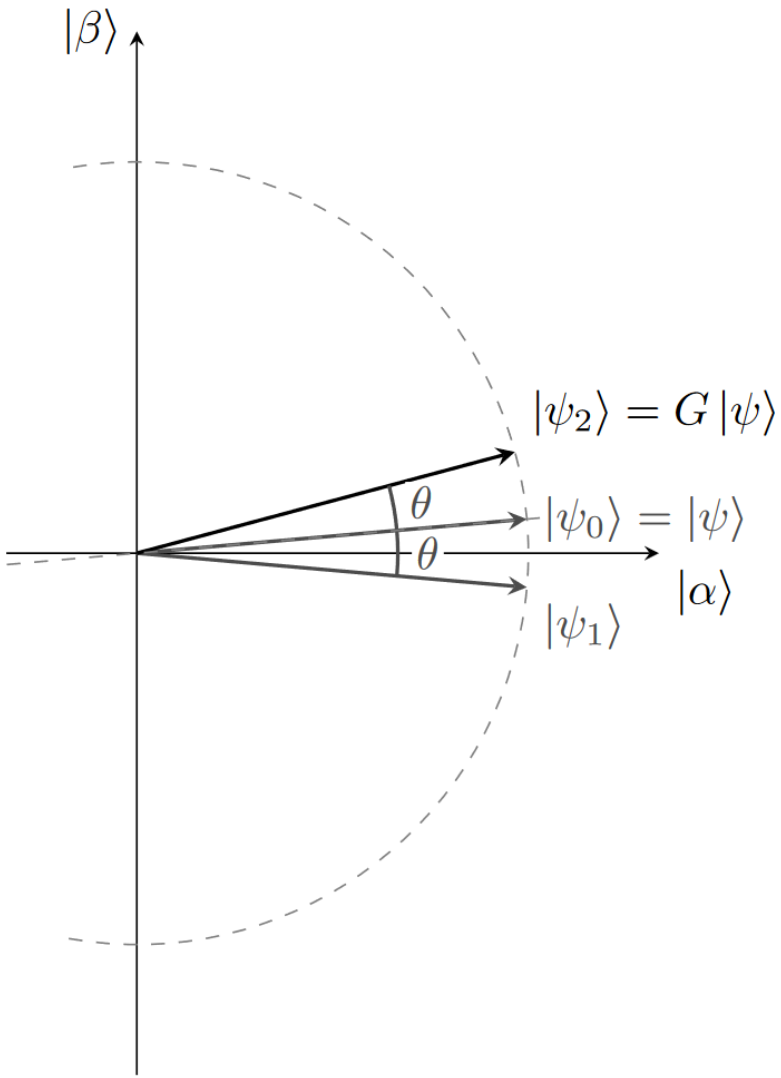
Primeira iteração

$$
\begin{aligned}
|\psi_1\rangle &= O_{\mathrm{F}} |\psi_0\rangle \\
&= O_{\mathrm{F}} \left(\frac{\sqrt{N-1}}{\sqrt{N}} |\alpha\rangle + \frac{1}{\sqrt{N}} |\beta\rangle \right) \quad \text{usando } (\psi) \\
&= \frac{\sqrt{N-1}}{\sqrt{N}} O_{\mathrm{F}} |\alpha\rangle + \frac{1}{\sqrt{N}} O_{\mathrm{F}} |\beta\rangle \\
&= \frac{\sqrt{N-1}}{\sqrt{N}} |\alpha\rangle - \frac{1}{\sqrt{N}} |\beta\rangle \quad \text{usando } (\alpha) \text{ e } (\beta)
\end{aligned}
$$

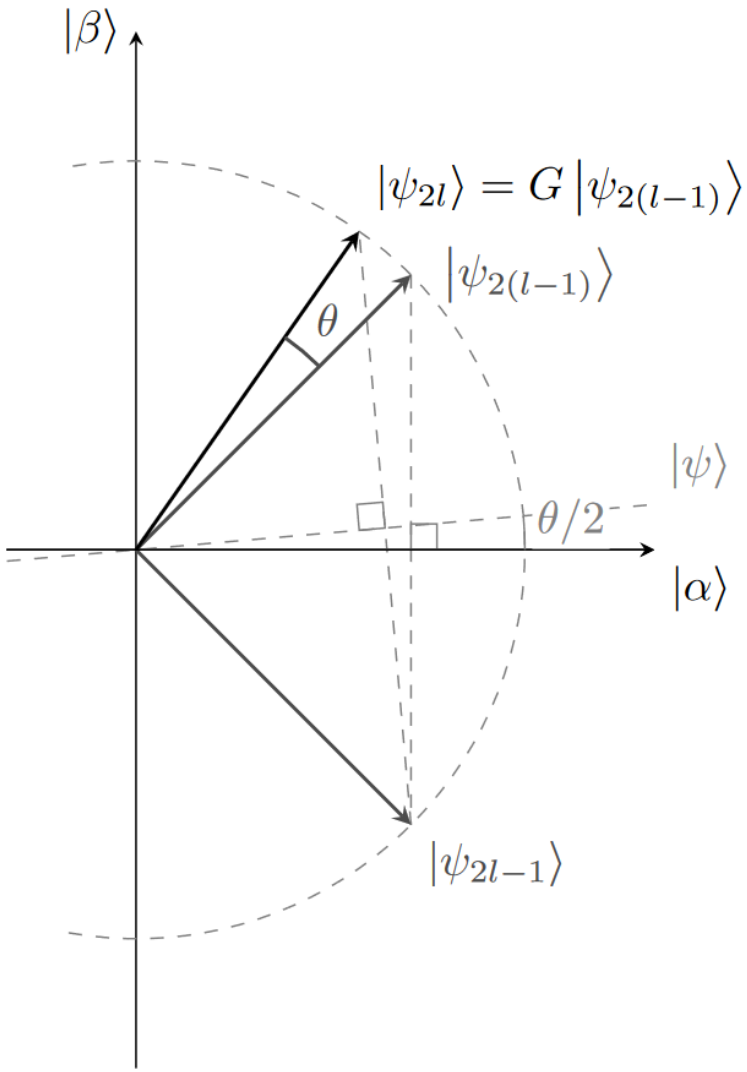


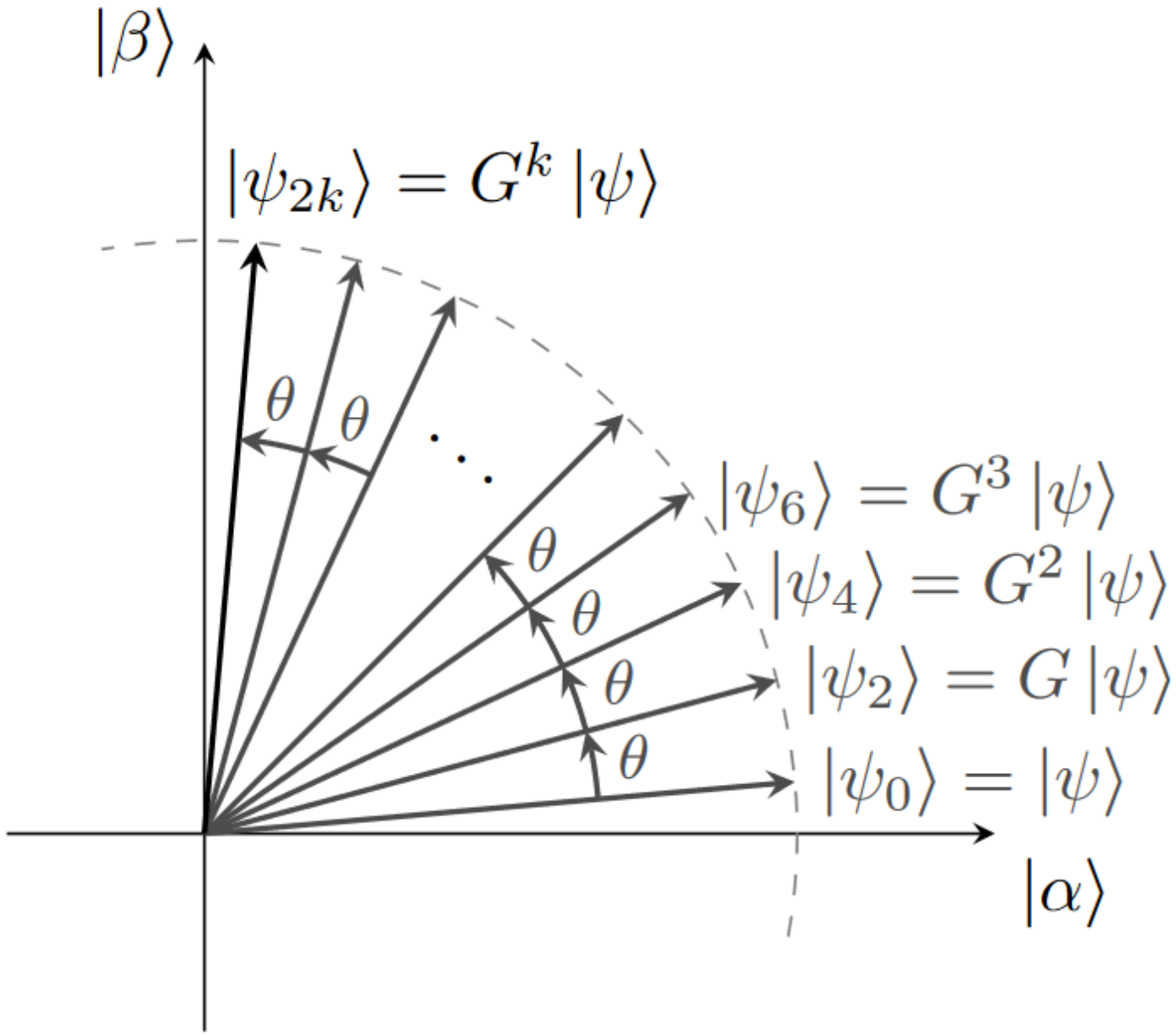
$$\begin{aligned}|\psi_2\rangle &= (2\,|\psi\rangle\langle\psi| - I)\,|\psi_1\rangle \\ &= 2\,|\psi\rangle\langle\psi|\,|\psi_1\rangle - |\psi_1\rangle\end{aligned}$$




$|\beta\rangle$
$|\psi_2\rangle = G\,|\psi\rangle$
θ
$|\psi_0\rangle = |\psi\rangle$
θ
$|\alpha\rangle$
$|\psi_1\rangle$

Visualização Geométrica




$|\beta\rangle$
$|\psi_{2k}\rangle = G^k |\psi\rangle$
θ
θ
θ
θ
θ
$|\psi_6\rangle = G^3 |\psi\rangle$
$|\psi_4\rangle = G^2 |\psi\rangle$
$|\psi_2\rangle = G |\psi\rangle$
$|\psi_0\rangle = |\psi\rangle$
$|\alpha\rangle$

Circuito

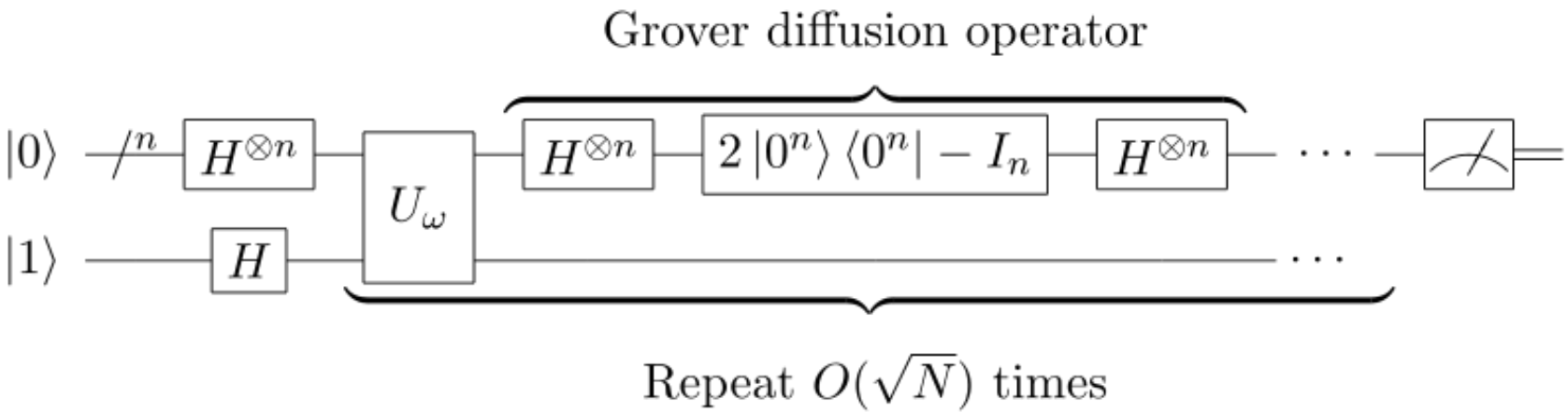
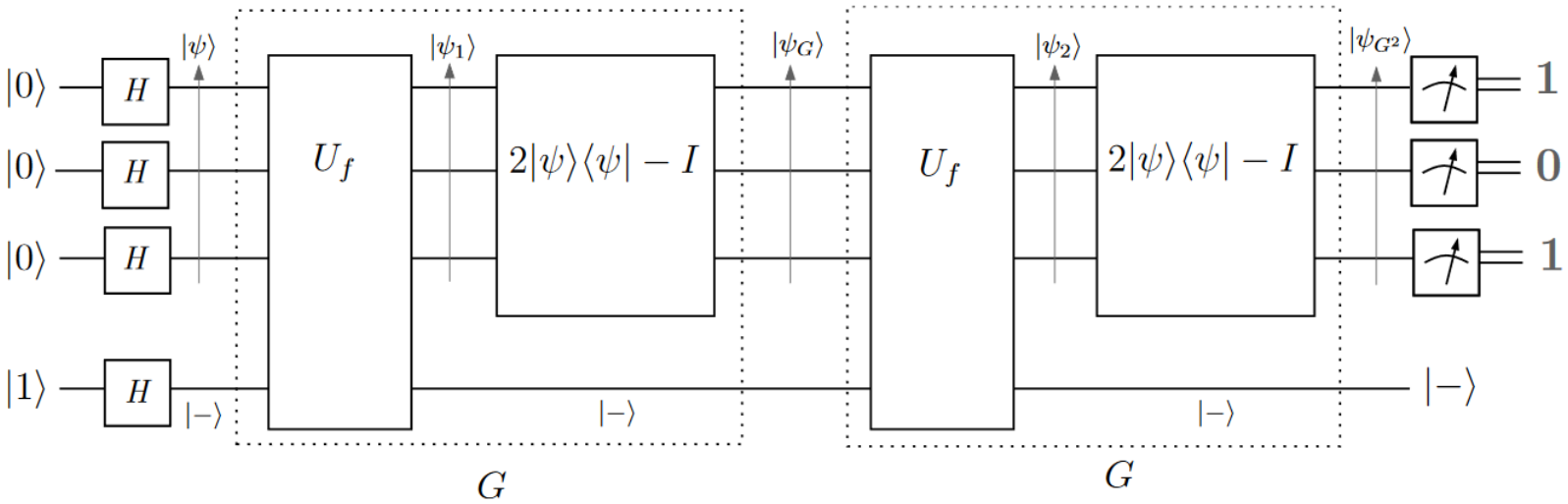


Figure: Circuito Quântico

Exemplo real



Exemplo real

$$
\begin{aligned}
|\psi\rangle &= H|0\rangle \otimes H|0\rangle \otimes H|0\rangle \\
&= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \\
&= \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right).
\end{aligned}
$$

Exemplo real

$$
\begin{aligned}
|\psi_1\rangle|-\rangle &= U_f\left(|\psi\rangle|-\rangle\right) \\
&= \left(\frac{|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle - |5\rangle + |6\rangle + |7\rangle}{\sqrt{8}}\right)|-\rangle.
\end{aligned}
$$

Exemplo real

$$
\begin{aligned}
|\psi_G\rangle &= (2|\psi\rangle\langle\psi| - I)\,|\psi_1\rangle \\
&= (2\langle\psi|\psi_1\rangle)\,|\psi\rangle - |\psi_1\rangle \\
&= \frac{3}{2}|\psi\rangle - |\psi_1\rangle \\
&= \frac{1}{2\sqrt{8}}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |6\rangle + |7\rangle\right) + \frac{5}{2\sqrt{8}}|5\rangle.
\end{aligned}
$$

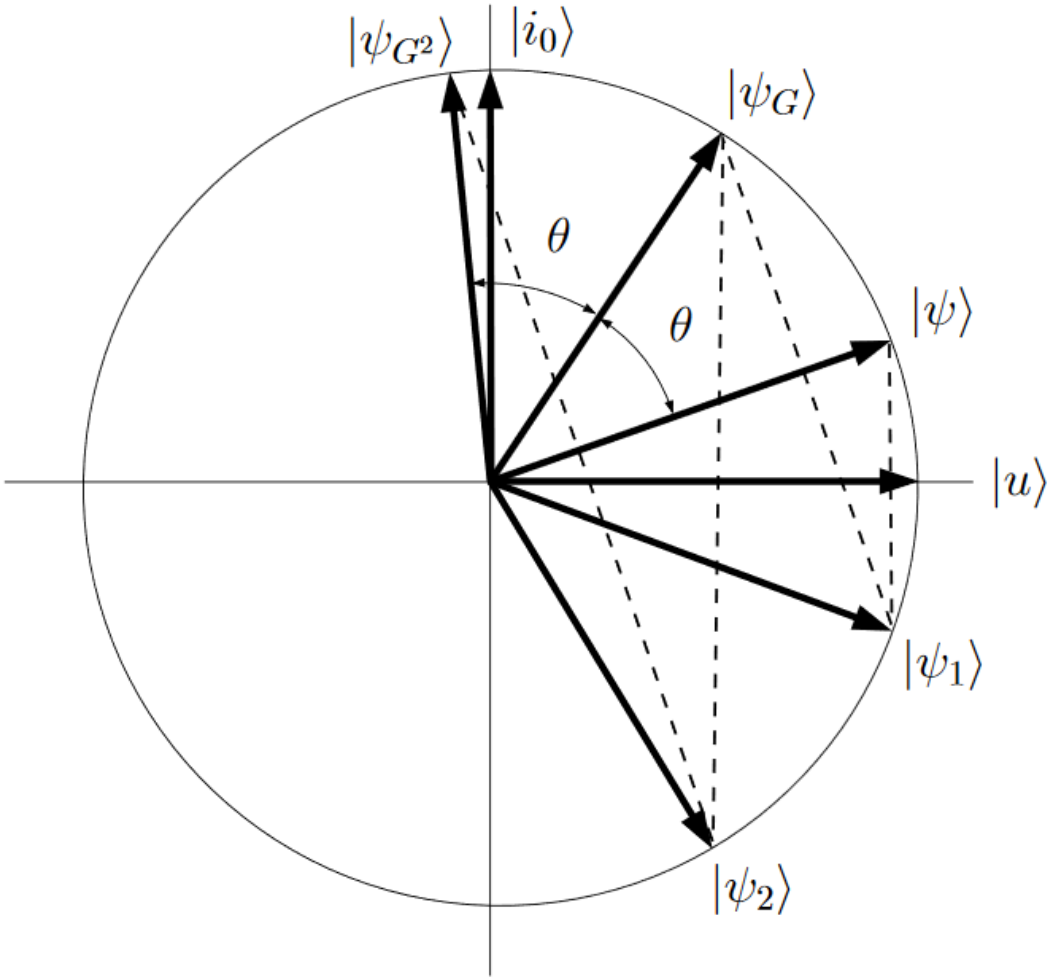
Exemplo real

$$
\begin{aligned}
|\psi_2\rangle|-\rangle &= U_f\left(|\psi_G\rangle|-\rangle\right) \\
&= \left(\frac{1}{2\sqrt{8}}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|6\rangle+|7\rangle\right)-\frac{5}{2\sqrt{8}}|5\rangle\right)|-\rangle.
\end{aligned}
$$

Novamente, o elemento procurado é o único que tem sua amplitude alterada. Aplicando o operador $2|\psi\rangle\langle\psi| - I$ sobre $|\psi_2\rangle$, temos:

$$
\begin{aligned}
|\psi_{G^2}\rangle &= \left(2|\psi\rangle\langle\psi| - I\right)|\psi_2\rangle \\
&= \left(2\langle\psi|\psi_2\rangle\right)|\psi\rangle - |\psi_2\rangle \\
&= \frac{1}{4}|\psi\rangle - |\psi_2\rangle \\
&= \left(\frac{-1}{4\sqrt{8}}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|6\rangle+|7\rangle\right)+\frac{11}{4\sqrt{8}}|5\rangle\right).
\end{aligned}
$$

Exemplo real



Pontos relevantes

Se sabe que o algoritmo de Grover é optimo, no sentido de que, usando o operador G, é necessário utilizá-lo, no mínimo, a quantidade de vezes que o algoritmo usa.
Uma modificação proposta pelo próprio Grover traz uma busca parcial, onde se procura se dado item se encontra dentro de qual bloco.

Outros estudos

Alguns trabalhos já feitos

- Síntese de Circuitos Quânticos usando Projective Simulation (Otto Menegasso)
- QSystem: simulador quântico para Python (Evandro Chagas Ribeiro da Rosa)