

Algoritmo de Grover

SUMÁRIO

01

MOTIVAÇÃO

02

ALGORITMO DE
GROVER

03

CONCLUSÃO

04

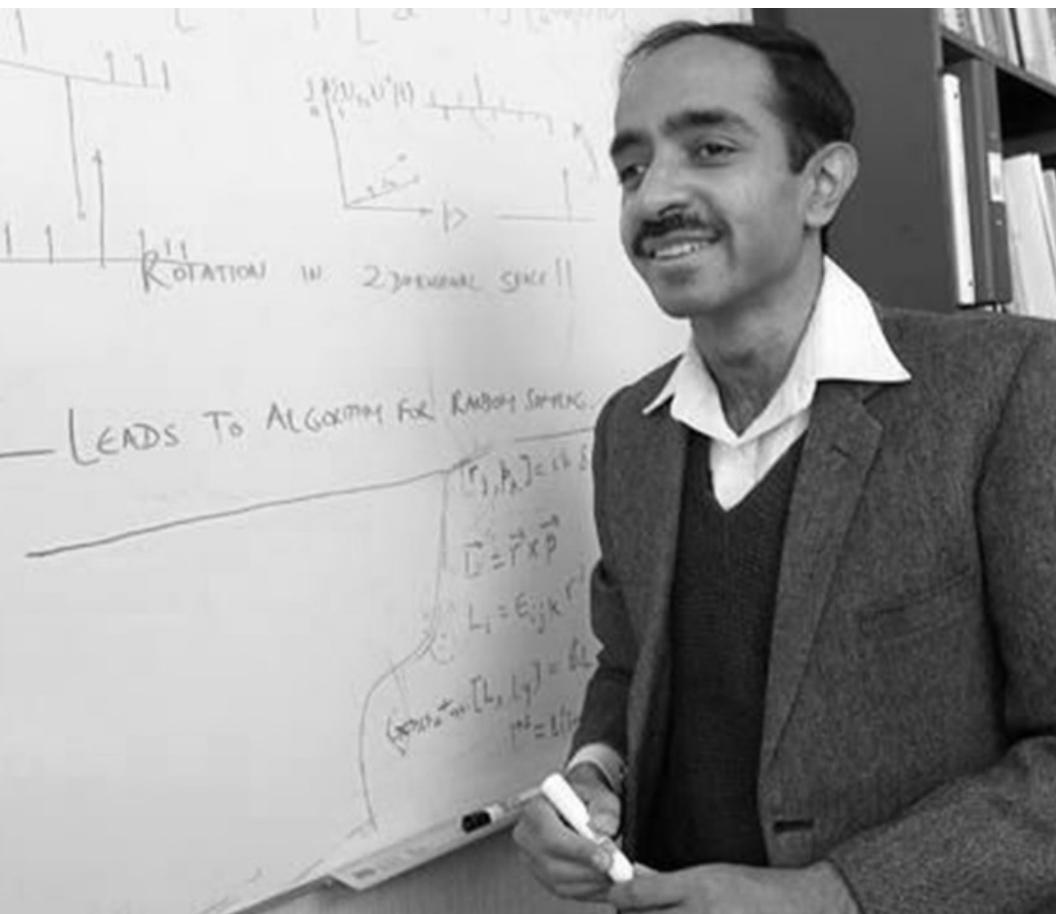
IMPLEMENTAÇÃO
EM QISKit



1

Motivação

Quantum Search Algorithm (QSA)



Algoritmo de Grover

Lov Grover, 1996

<https://medium.com/nerd-for-tech/grovers-algorithm-3ac4616ce23a>

Qual deles é o impostor? - exemplo de busca não-estruturada



<https://medium.com/nerd-for-tech/grovers-algorithm-3ac4616ce23a>



Algoritmo de Grover



Enunciado: Dada uma base de dados não-ordenada com N elementos, encontre um elemento específico.

Algoritmo de Grover

Enunciado: Dada uma base de dados não-ordenada com N elementos, encontre um elemento específico.

Solução Clássica: Testar todos os elementos até encontrar o desejado.

- No pior dos casos, temos que realizar N testes e, na média, $N/2$.
- Complexidade: $O(N)$.

Algoritmo de Grover

Enunciado: Dada uma base de dados não-ordenada com N elementos, encontre um elemento específico.

Solução Clássica: Testar todos os elementos até encontrar o desejado.

- No pior dos casos, temos que realizar N testes e, na média, $N/2$.
- Complexidade: $O(N)$.

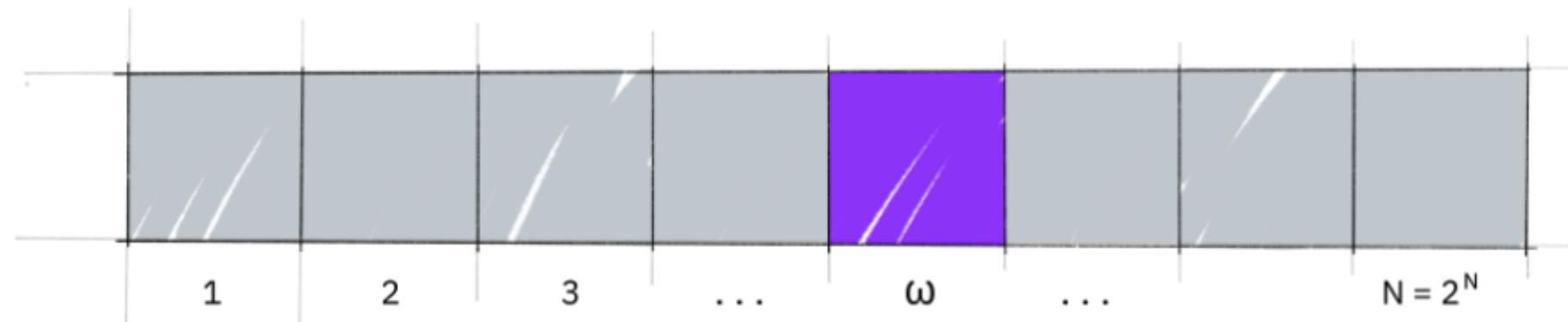
Solução Quântica: Algoritmo de Grover $O(\sqrt{N})$

2

Passo a Passo do Algoritmo de Grover

Definindo oráculo:

- Marcar o estado desejado



$$U_\omega|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq \omega \\ -|x\rangle & \text{if } x = \omega \end{cases}$$

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle$$



$$\begin{aligned} f(x) &= 0 & (x \neq \omega) \\ f(x) &= 1 & (x = \omega) \end{aligned}$$

$$U_\omega = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \leftarrow \omega = 101$$

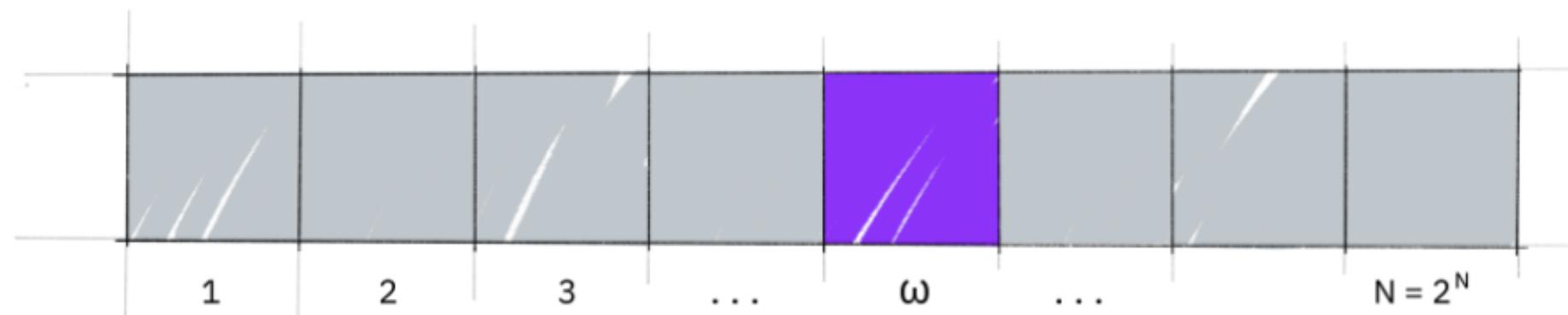
Source: Qiskit Textbook

2

Passo a Passo do Algoritmo de Grover

Definindo oráculo:

- Marcar o estado desejado



$$U_\omega|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq \omega \\ -|x\rangle & \text{if } x = \omega \end{cases}$$

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle$$



$$\begin{aligned} f(x) &= 0 & (x \neq \omega) \\ f(x) &= 1 & (x = \omega) \end{aligned}$$

$$U_\omega = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \leftarrow \omega = 101$$



$$U_\omega = I - 2|\omega\rangle\langle\omega|$$

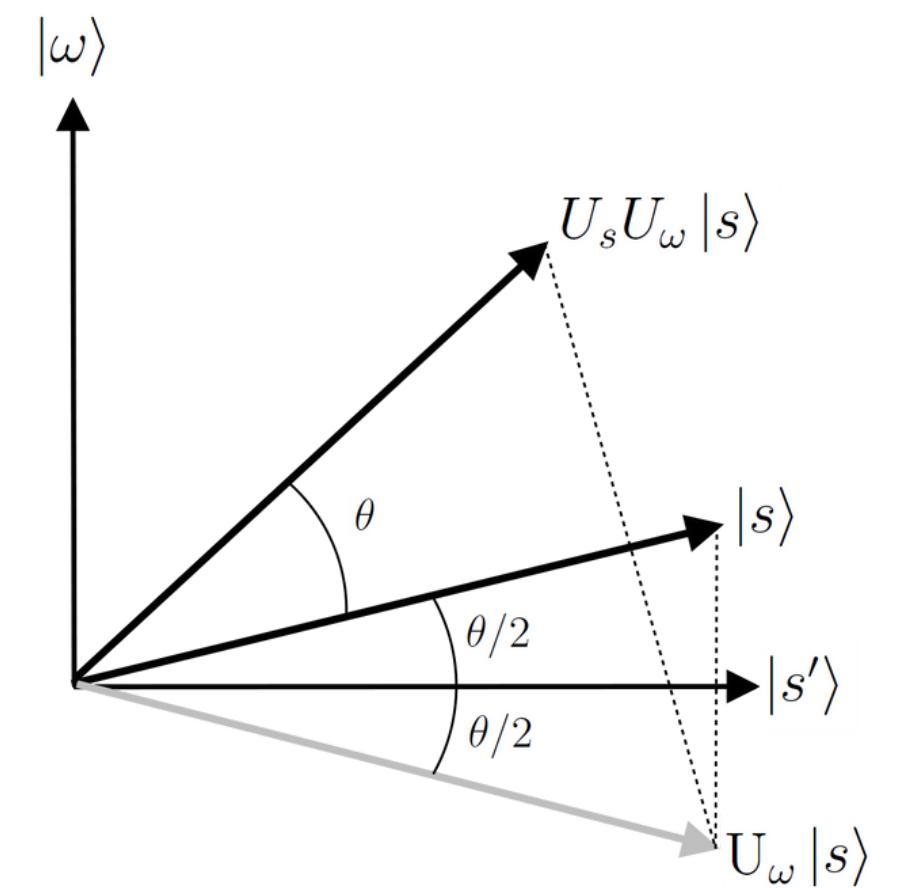
Householder transformation

Source: Qiskit Textbook

- Rotacionar em torno do estado anterior superposto

$$U_s = 2|s\rangle\langle s| - I$$

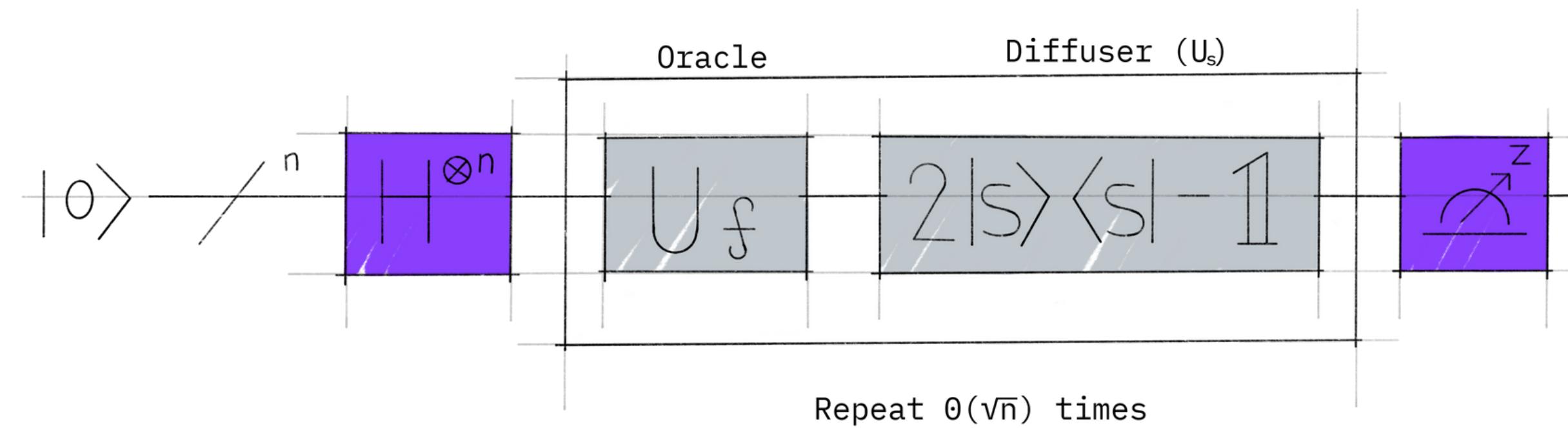
Ao aplicar $U_s U_f$ em cada passo de iteração de Grover gira o vetor de estado por um ângulo $\theta = 2 \arcsin \frac{1}{\sqrt{N}}$



- Medir o estado quântico resultante em base computacional

Source: Wikipedia

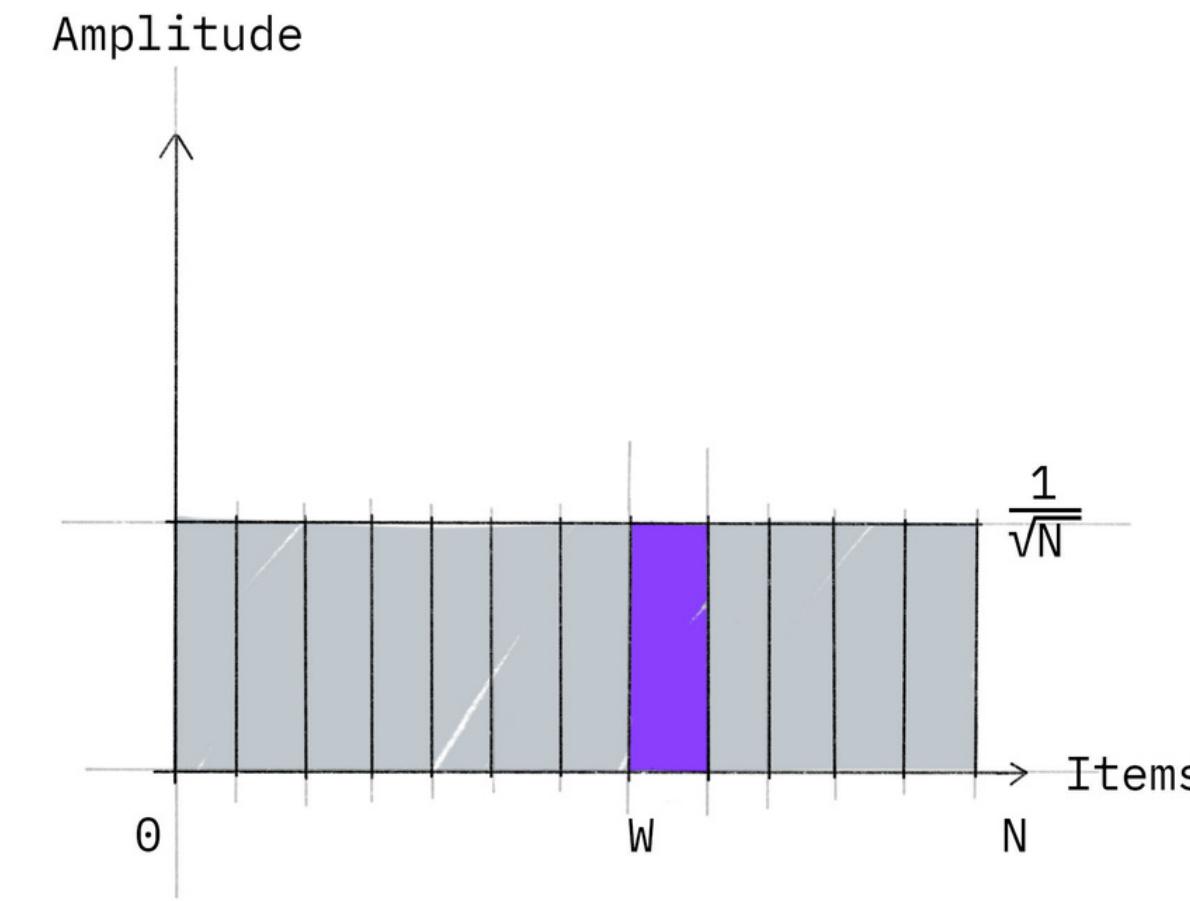
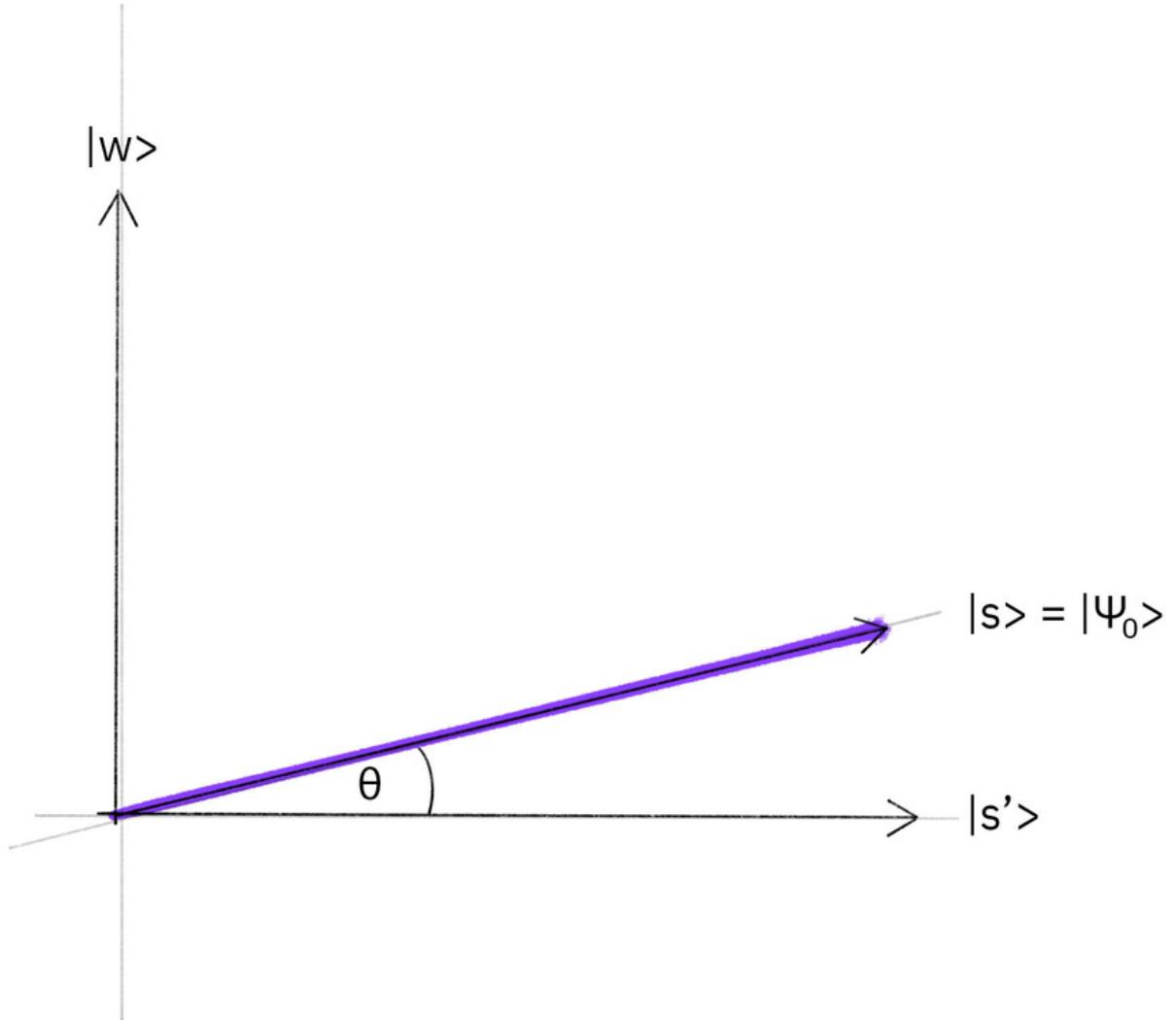
Em outras palavras, temos que construir o seguinte circuito



Source: Qiskit Textbook

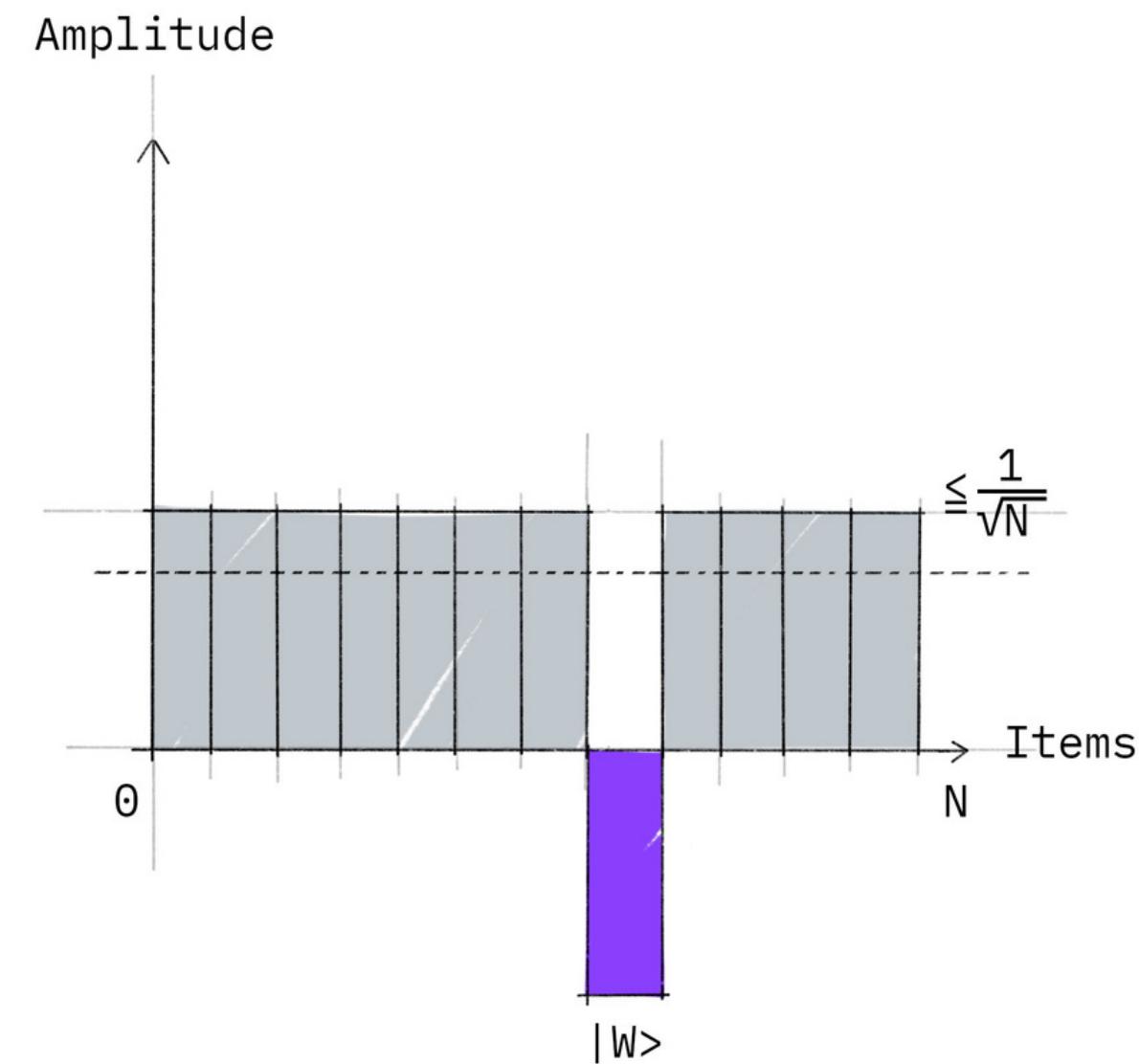
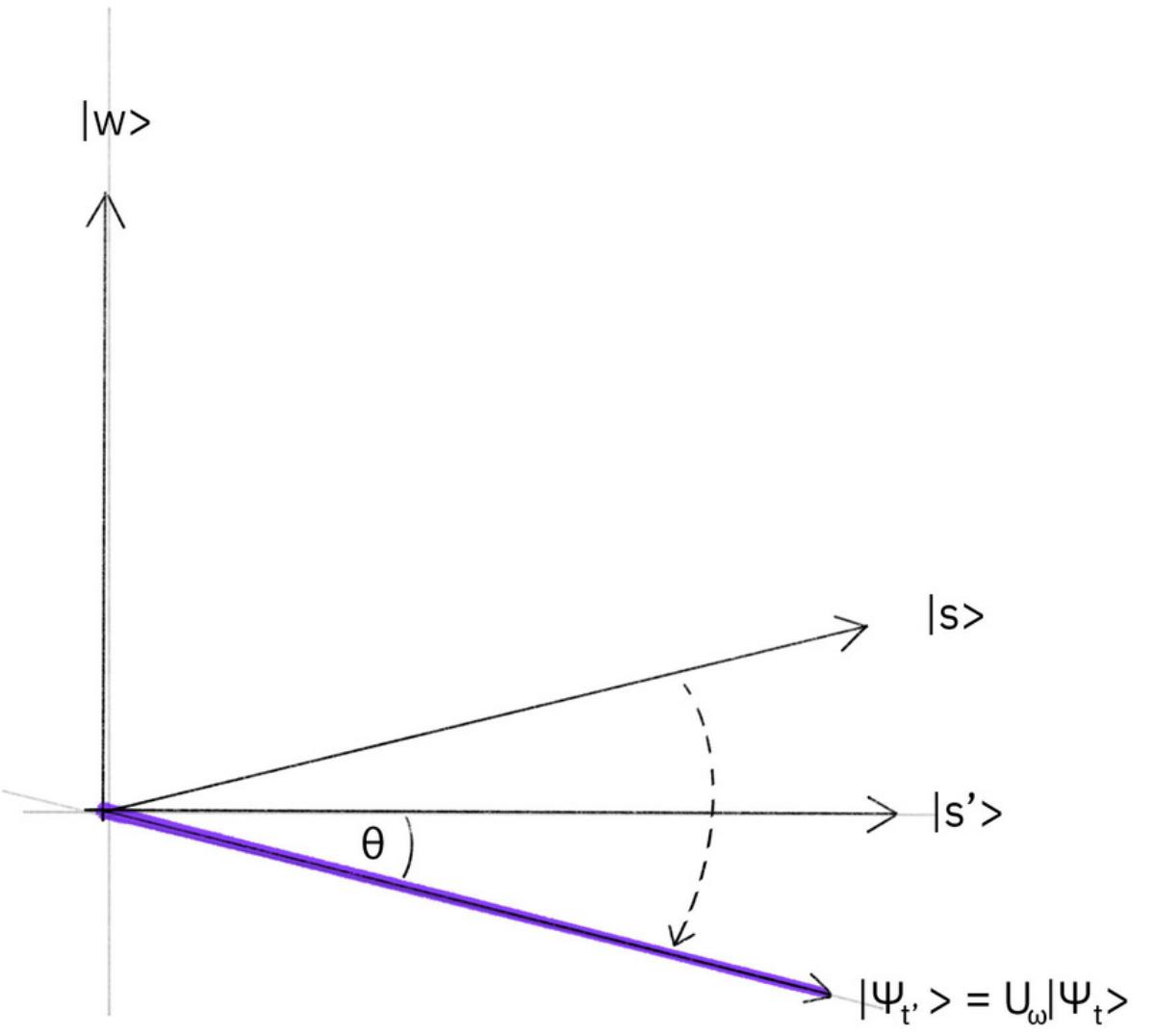
Passo 1: Gerar o estado superposto $|s\rangle$, que é facilmente construído a $|s\rangle = H^{\otimes n}|0\rangle^n$

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



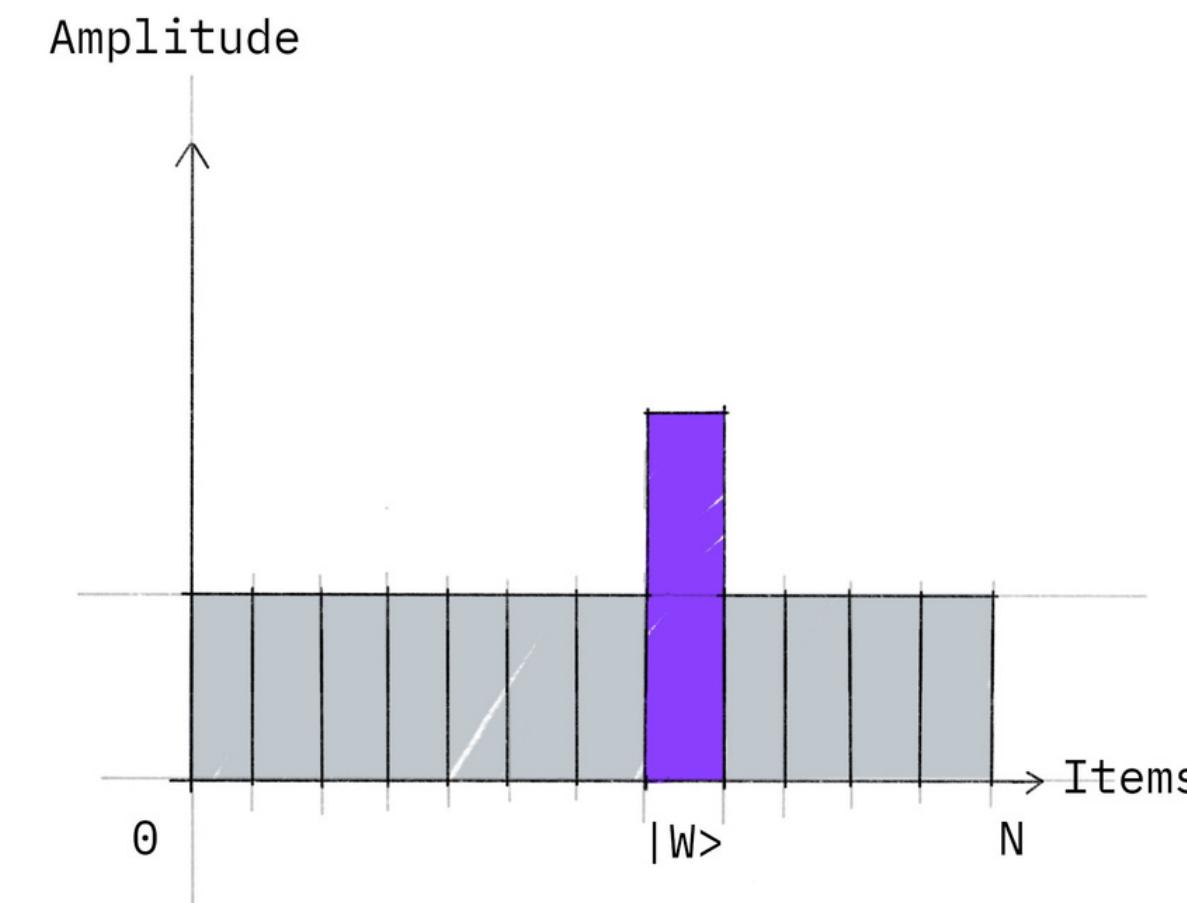
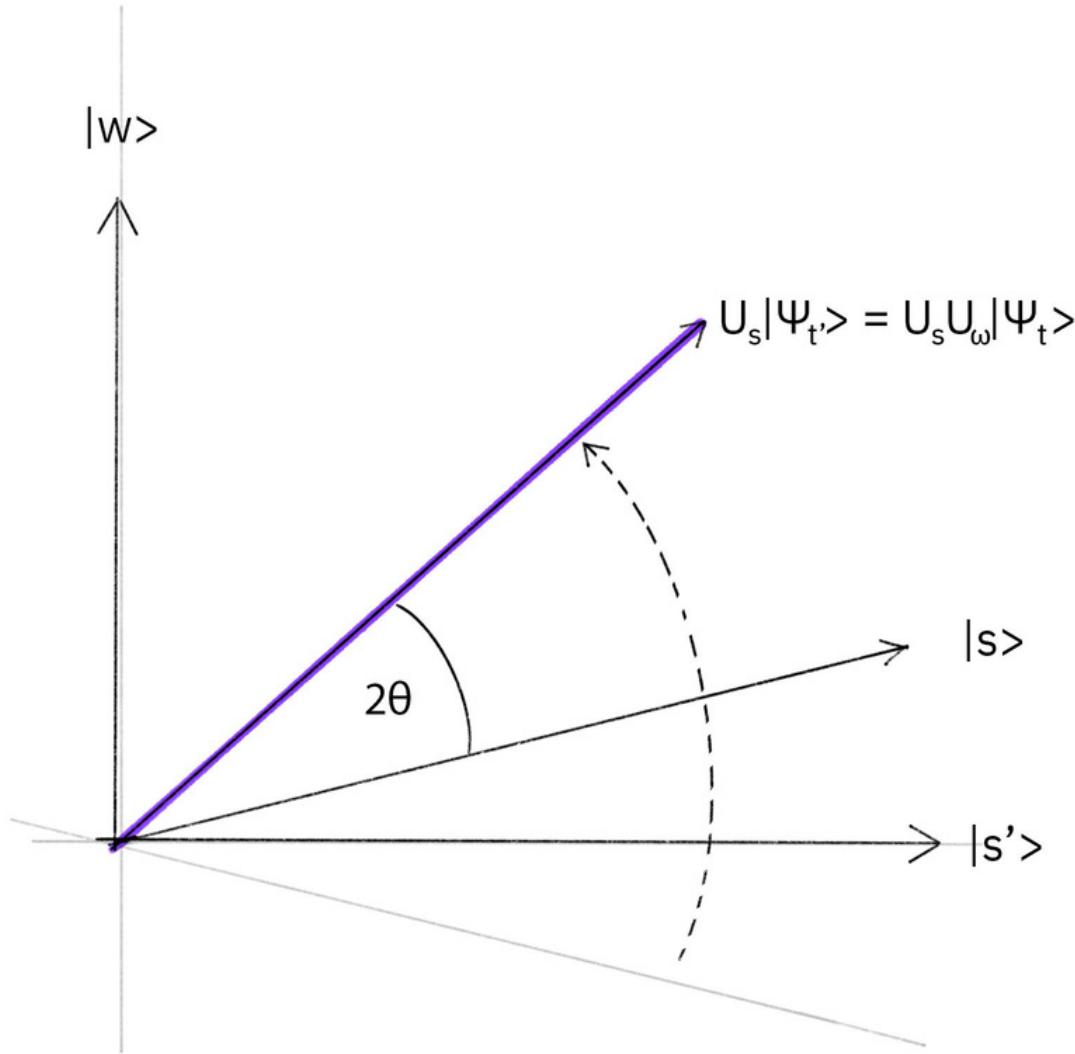
Source: Qiskit Textbook

Passo 2: Aplicamos a reflexão do oráculo U_w no estado $|s\rangle$:



Source: Qiskit Textbook

Passo 3: Agora aplicamos uma reflexão adicional sobre o estado $U_s = 2|s\rangle\langle s| - 1$ atual, i.e., $U_s U_f |s\rangle$



Source: Qiskit Textbook



Continhas...

$$U_\omega |s\rangle = (I - 2|\omega\rangle\langle\omega|)|s\rangle = |s\rangle - 2|\omega\rangle\langle\omega|s\rangle = |s\rangle - 2|\omega\rangle(1/\sqrt{4})$$

$$\begin{aligned} U_s \left(|s\rangle - \frac{2}{\sqrt{4}} |\omega\rangle \right) &= (2|s\rangle\langle s| - I) (|s\rangle - |\omega\rangle) \\ &= 2|s\rangle\langle s|s\rangle - |s\rangle - |s\rangle\langle s|\omega\rangle + |\omega\rangle \\ &= 2|s\rangle - |s\rangle - |s\rangle - |\omega\rangle \\ &= |\omega\rangle \end{aligned}$$



Continhas...

$$\rightarrow U_\omega |s\rangle = (I - 2|\omega\rangle\langle\omega|)|s\rangle = |s\rangle - 2|\omega\rangle\langle\omega|s\rangle = |s\rangle - 2|\omega\rangle(1/\sqrt{4})$$
$$U_s \left(|s\rangle - \frac{2}{\sqrt{4}} |\omega\rangle \right) = (2|s\rangle\langle s| - I) (|s\rangle - |\omega\rangle)$$
$$= 2|s\rangle\langle s|s\rangle - |s\rangle - |s\rangle\langle s|\omega\rangle + |\omega\rangle$$
$$= 2|s\rangle - |s\rangle - |s\rangle - |\omega\rangle$$
$$= |\omega\rangle$$



Continhas...

$$\rightarrow U_\omega |s\rangle = (I - 2|\omega\rangle\langle\omega|)|s\rangle = |s\rangle - 2|\omega\rangle\langle\omega|s\rangle = |s\rangle - 2|\omega\rangle(1/\sqrt{4})$$

$$\begin{aligned}\rightarrow U_s \left(|s\rangle - \frac{2}{\sqrt{4}} |\omega\rangle \right) &= (2|s\rangle\langle s| - I) (|s\rangle - |\omega\rangle) \\ &= 2|s\rangle\langle s|s\rangle - |s\rangle - |s\rangle\langle s|\omega\rangle + |\omega\rangle \\ &= 2|s\rangle - |s\rangle - |s\rangle - |\omega\rangle \\ &= |\omega\rangle\end{aligned}$$

3

Recap

O Algoritmo de Grover é um algoritmo quântico que realiza buscas não estruturadas em bancos de dados.

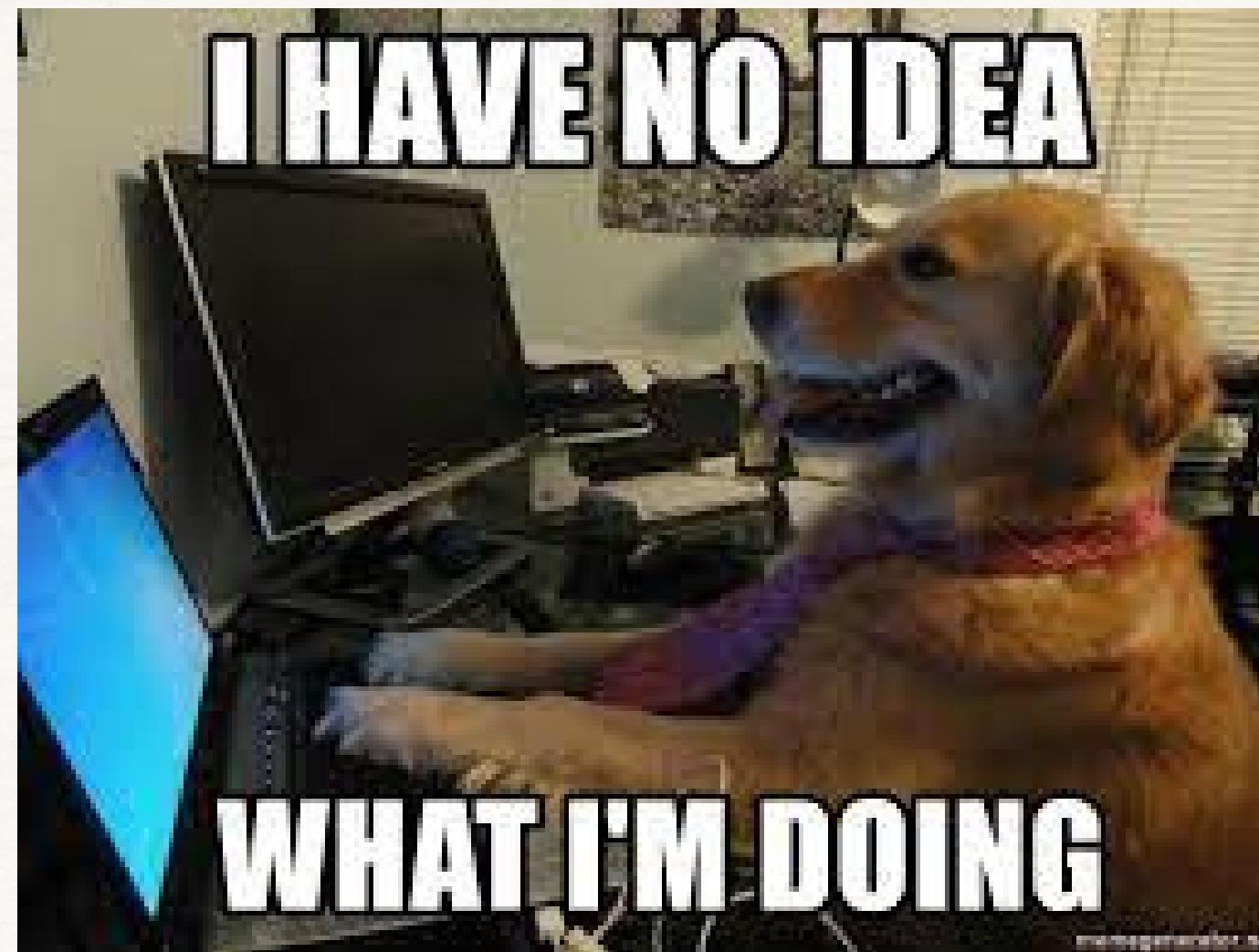
Você pode usá-lo para melhorar quadraticamente o tempo de execução de outros algoritmos, usando um hack chamado amplificação de amplitude.

A amplificação da amplitude aumenta a probabilidade de encontrar um item único w entre uma lista de itens N , através de reflexões de oráculo ao estado superposto

Extras: Criptografia

4

Implementação em Qiskit



OBRIGADO!

Perguntas?



ooo