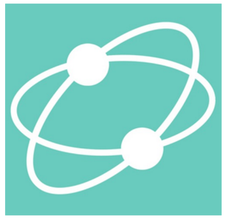
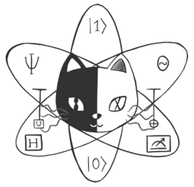
ESCUELA EN ESPAÑOL

QISKIT FALL FEST



Algoritmo de Grover



Dani Guijo

UNIVERSIDAD SIMÓN BOLÍVAR

ESCUELA EN ESPAÑOL

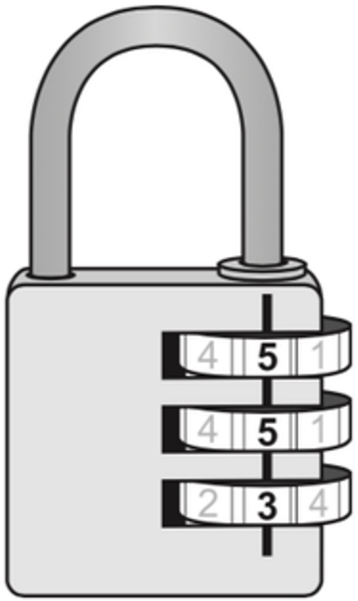
QISKIT FALL FEST

Contenido

- Contexto y Motivación
  - Ejemplo clásico
- Problema de búsqueda de Grover
  - Formulación matemática
- Algoritmo de Grover
  - Oráculo
  - Operador de difusión de Grover
  - Interpretación geométrica
- Discusión y conclusiones

Contexto y Motivación

¿?



000
001
002
003
.
.
.
999

553

Si existen *N* posibles soluciones, necesitaremos una media de *N*/2 intentos

¿Es posible hacerlo más rápido?

Utilizando solamente fuerza bruta, necesitaremos de media **500 intentos** para abrir el candado.

Sin embargo, el algoritmo de Grover nos permite encontrar la combinación correcta en aproximadamente **18 intentos**.

¿¿¿Cómo es eso posible???

Problema de Búsqueda de Grover

Problema de búsqueda de Grover

Dada una función $f : \{0, 1\}^n \rightarrow \{0, 1\}$, donde n es el tamaño en bits de los elementos del espacio de búsqueda (# qubits), y dado $N = 2^n$ el tamaño del espacio de búsqueda, se debe encontrar el único elemento w tal que $f(w)=1$.

- La búsqueda es **no estructurada.**
- Se tiene acceso a un **oráculo**:

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

- O equivalentemente con un qubit ancilla:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

Algoritmo de Grover

Paso 1: Estado de igual superposición

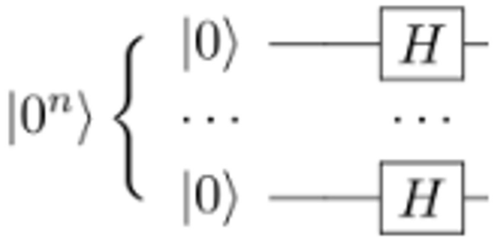
- Todos los estados pueden manifestarse con igual probabilidad:

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

- No es perpendicular al estado solución, pero está en el plano que este genera con:

$$|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle$$

- Se genera con el circuito:



Paso 2: Oráculo

- El operador del oráculo puede escribirse como una reflexión u **operador o de Householder:**

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

- Geométricamente, se interpreta como una reflexión sobre el estado

$$|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle$$

- El circuito de este operador es **desconocido**.

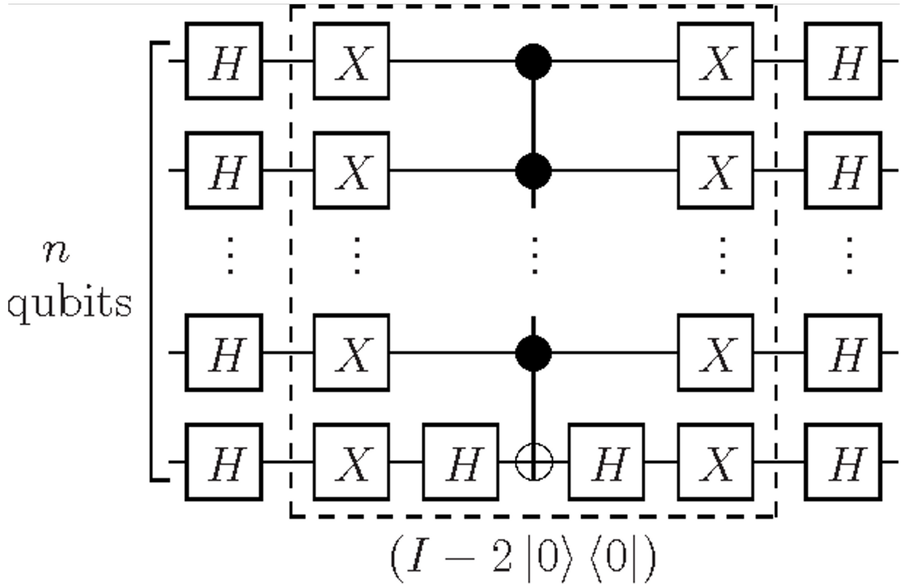
Paso 3: Operador de difusión de Grover

- También puede verse como una reflexión, en este caso sobre el estado de igual superposición:

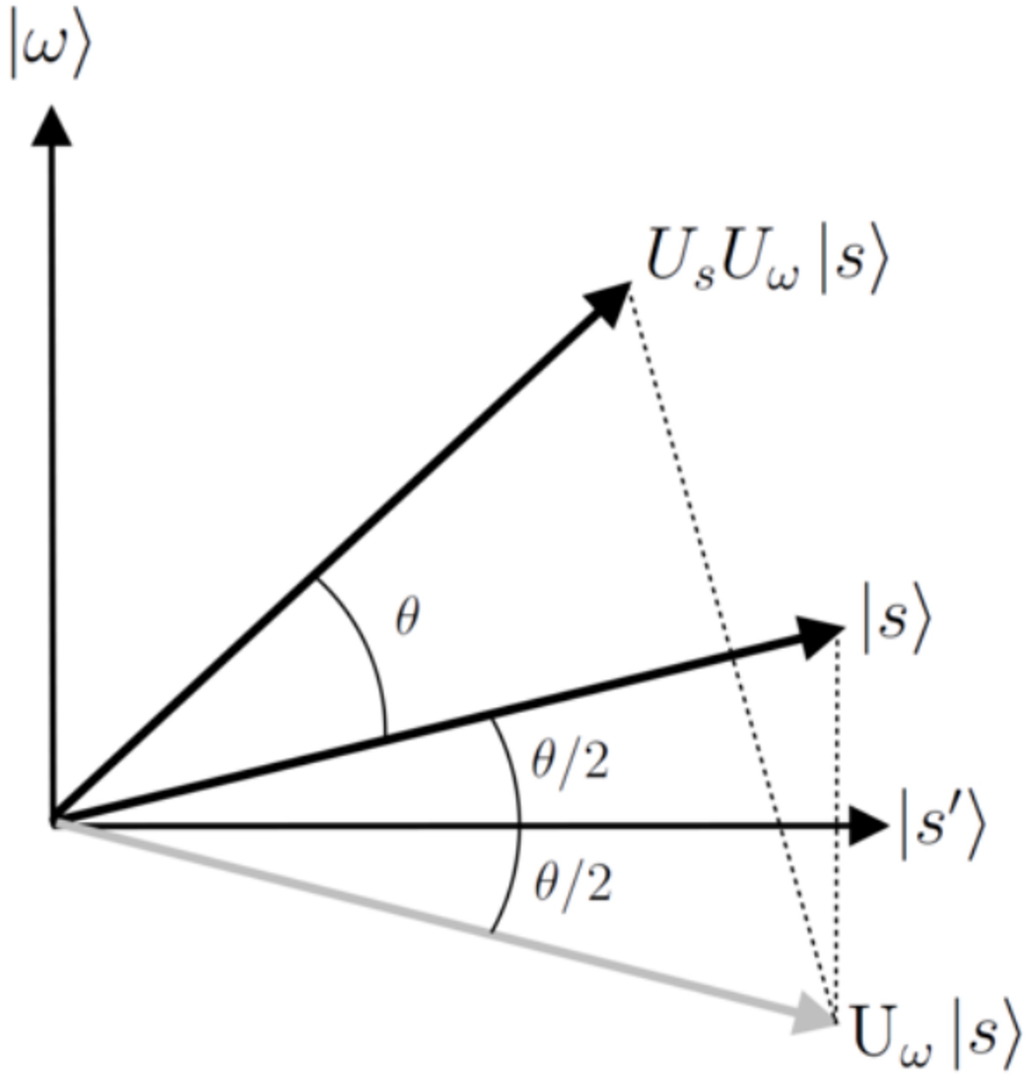
$$U_s = 2|s\rangle\langle s| - I$$

- O equivalentemente:

$$H\,U_0\,H = H(2|0\rangle\langle 0| - I)H$$



Interpretación geométrica

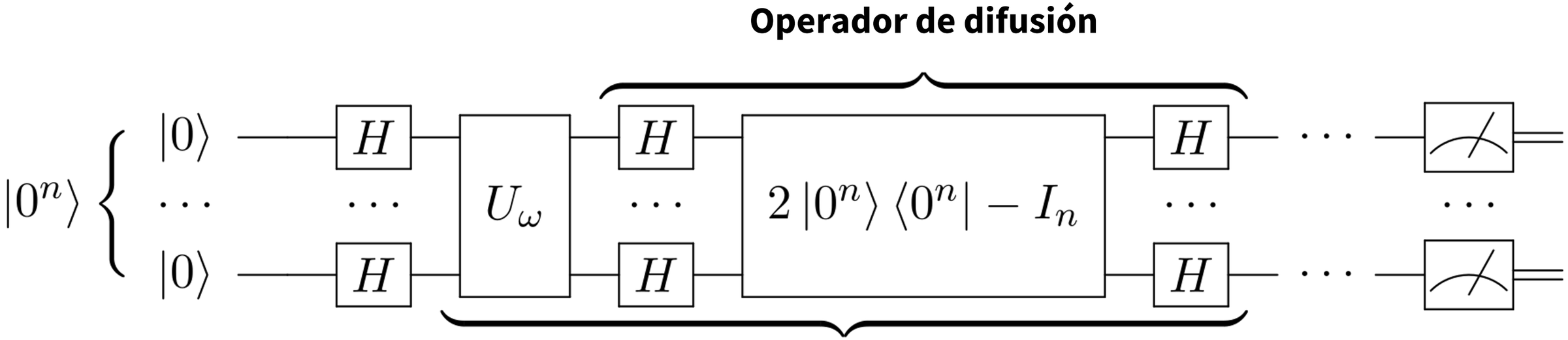


$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}} \Rightarrow \theta = 2\arcsin\frac{1}{\sqrt{N}}$$

$$r(N) = \frac{\pi - \theta}{2\theta} \approx \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$$

$$P(w, N) = \sin^2\left(r(N)\cdot\theta + \frac{\theta}{2}\right)$$

Algoritmo completo



Repetir $\approx \frac{\pi}{4}\sqrt{N}$ **veces**

Conclusiones

Conclusiones

- El algoritmo de Grover **resuelve de forma genérica el problema de búsqueda no estructurada.**

- Lo hace utilizando un número **cuadráticamente menor** de iteraciones que cualquier algoritmo clásico.

- Sin embargo, al igual que los algoritmos clásicos, **escala exponencialmente respecto al tamaño del problema.**

ESCUELA EN ESPAÑOL

QISKIT FALL FEST

QuantumQuipu

GFT
GRUPO DE FÍSICA TEÓRICA
UNMSM

KIPU QUANTUM

IBM

qBraid

¡Gracias por asistir!

JÜLICH
Forschungszentrum

bqb

QWORLD

UNIVERSIDAD SIMÓN BOLÍVAR

CoF
Alumni USB