QuantumQuipu/

QuantumScholars2023

Autor: Gustavo Valdivia Mera
Institución: University of Houston
Correo: gvaldiviamera@uh.edu (mailto:gvaldiviamera@uh.edu)

Puede consultar la última versión de este notebook en nuestro repositorio (https://github.com/QuantumQuipu/QuantumScholars2023) y los videos de clase en nuestro canal de Youtube (https://www.youtube.com/channel/UCze8vzQLcplutz0nWDNjFCA).

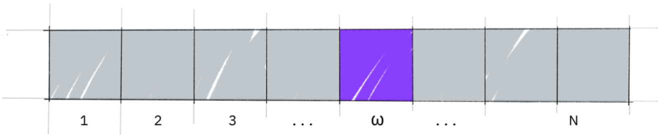
Sesión 5. Algoritmo de Grover

Outline

1. Problema

Supongamos que tenemos una lista de N elementos; tal que, entre ellos existe un grupo de elementos que deseamos encontrar. Para ello, debido a sus atributos (características), estos elementos serán "marcados" con la finalidad de poder ser detectados.

- Por ejemplo: En la siguiente lista de N elementos se ha marcado el objeto ω para su búsqueda: Notamos que es la celda de distinto color.



2. Modelo Computacional con Oráculo

Sea $\omega \in \{0, 1\}^n$

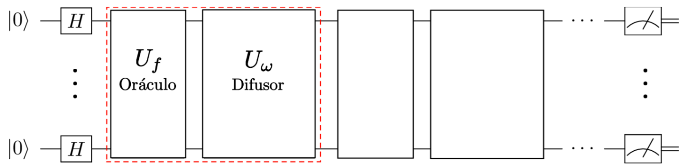
Solución Clásica

En el peor de los casos necesitamos $N = 2^n$ intentos para encontrar la cadena ω (suponiendo que ω es un solo elemento).

Solución Cuántica

Para la solución cuántica requerimos la implementación de dos operadores:

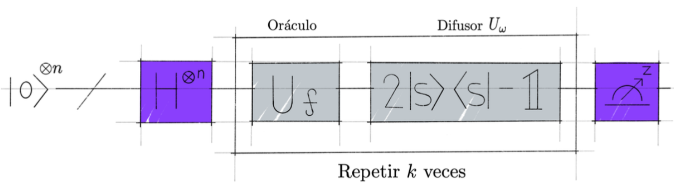
1. Oráculo: Este operador se encarga de marcar los estados deseados.
2. Difusión: Este operador amplifica los estados marcados de tal forma que al final del algoritmo, estos tendrán la mayor probabilidad



3. Algoritmo de Grover

Construimos un circuito de n qubits. Luego:

- Aplicamos la compuerta H a todos los qubits.
- Aplicamos el oráculo U_f y luego el difusor U_ω.
- Repetimos k veces la aplicación de $U_\omega U_f$, y finalmente medimos.



3.1 Análisis

Operador oráculo U_f

Definimos

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle \quad , \quad x \in \{0,1\}^n$$

Tal que

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

o también

$$U_f|x\rangle = \begin{cases} |x\rangle & : x \neq \omega \\ -|x\rangle & : x = \omega \end{cases} \quad , \quad x \in \{0,1\}^n$$

Donde $|\omega\rangle$ representa los estados que deseamos marcar.

Operador difusor U_ω

Definimos

$$U_\omega = 2|s\rangle\langle s| - \mathrm{I}$$

Donde

$$\begin{aligned} |s\rangle &:= H^{\otimes n}|0\rangle^{\otimes n} \\ &= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle \end{aligned}$$

$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n}$

$\langle s| = \langle 0|^{\otimes n}H^{\otimes n}$

$2|s\rangle\langle s| = 2H^{\otimes n}|0\rangle^{\otimes n}\langle 0|^{\otimes n}H^{\otimes n}$

$-HH = -\mathbb{I}$

¿Cómo aplica U_ω en un circuito cuántico?

¿Cómo desaparece ese (-) en el circuito?

$U_\omega U_f|A\rangle$

$$\begin{aligned} U_\omega &= 2|s\rangle\langle s| - \mathrm{I} \\ &\stackrel{!}{=} 2H^{\otimes n}|0\rangle^{\otimes n}\langle 0|^{\otimes n}H^{\otimes n} - H^{\otimes n}H^{\otimes n} \\ &= H^{\otimes n}(2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - \mathrm{I})H^{\otimes n} \\ &= -H^{\otimes n}U_0H^{\otimes n} \end{aligned}$$

$U_0 = \mathbb{I} - 2|0\rangle^{\otimes n}\langle 0|^{\otimes n}$

Donde

$U_0|x\rangle = (\mathbb{I} - 2|0\rangle^n\langle 0|^n)|x\rangle$

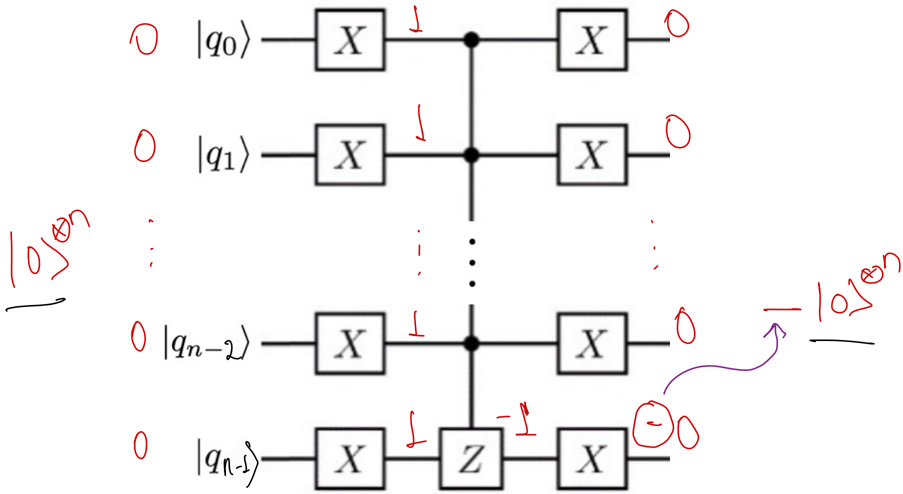
$\stackrel{!}{=} |x\rangle - 2|0\rangle^n\underbrace{\langle 0|^n x\rangle}_{\substack{0:\ x\neq 0^n \\ 1:\ x=0^n}}$

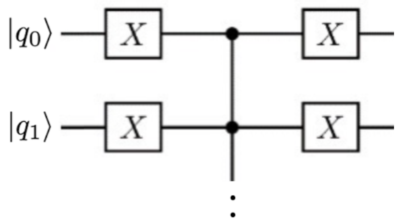
$$U_0|x\rangle = \begin{cases} |x\rangle & : x \neq 0^n \\ -|x\rangle & : x = 0^n \end{cases}$$

Por lo tanto, el operador U_0 se aplicará de la siguiente forma en nuestro circuito

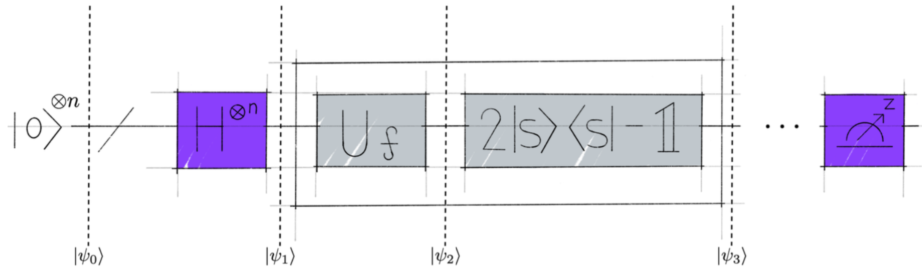
$$U_0|x\rangle = \begin{cases} |x\rangle & : x \neq 0^n \\ -|x\rangle & : x = 0^n \end{cases}$$

$$U_f|x\rangle = \begin{cases} |x\rangle & ; x \neq \omega \\ -|x\rangle & : x = \omega \end{cases}$$





Algoritmo



Tenemos el estado inicial

$$|\psi_0\rangle = |0\rangle^{\otimes n}$$

Luego aplicamos la compuerta H a todos los qubits

$$|\psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n}$$

Sea A el conjunto de los estados (equiprobables) deseados

$$A = \{x \in \{0,1\}^n | f(x) = 1\} \quad \mapsto \quad |A\rangle = \frac{1}{\sqrt{a}}\sum_{x \in A} |x\rangle \quad \text{(Ket de estados deseados)}$$

$$a: \text{ Cantidad de estados deseados}$$

Sea B el conjunto de los estados (equiprobables) no deseados

$$B = \{y \in \{0,1\}^n | f(y) = 0\} \quad \mapsto \quad |B\rangle = \frac{1}{\sqrt{b}}\sum_{y \in B} |y\rangle \quad \text{(Ket de estados no deseados)}$$

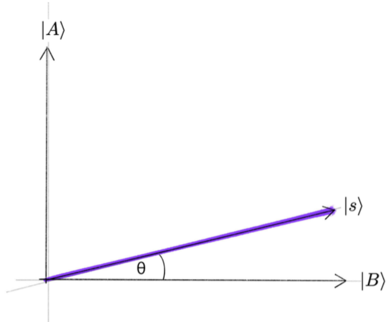
$$b: \text{ Cantidad de estados no deseados}$$

Entonces

$$|\psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n}$$
$$= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$
$$= \frac{1}{\sqrt{2^n}}\sum_{x\in A}|x\rangle + \frac{1}{\sqrt{2^n}}\sum_{y\in B}|y\rangle$$
$$= \sqrt{\frac{a}{2^n}}\left(\overbrace{\frac{1}{\sqrt{a}}\sum_{x\in A}|x\rangle}^{|A\rangle}\right) + \sqrt{\frac{b}{2^n}}\left(\overbrace{\frac{1}{\sqrt{b}}\sum_{y\in B}|y\rangle}^{|B\rangle}\right)$$

$$|S\rangle = H^{\otimes n}|0\rangle^{\otimes n}$$
$$\Rightarrow \underbrace{|\psi_1\rangle}_{=|s\rangle} = \sqrt{\frac{a}{2^n}}|A\rangle + \sqrt{\frac{b}{2^n}}|B\rangle$$

Notamos que $|s\rangle$ se puede visualizar como un vector en el plano dado por los ejes $|B\rangle$ y $|A\rangle$



$$\boxed{|s\rangle = \underbrace{\sqrt{\frac{a}{2^n}}}_{Sen\theta}|A\rangle + \underbrace{\sqrt{\frac{b}{2^n}}}_{Cos\theta}|B\rangle}$$

Entonces

$$|s\rangle = \sin\theta|A\rangle + \cos\theta|B\rangle$$

$$\sin\theta = \sqrt{\frac{a}{2^n}}$$

$$\cos\theta = \sqrt{\frac{b}{2^n}}$$

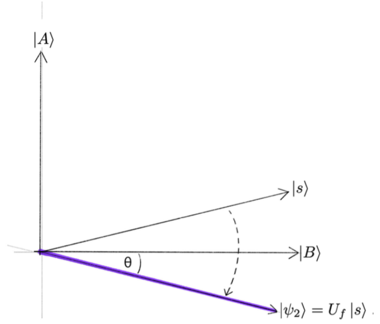
A continuación, aplicamos U_f

$$|\psi_1\rangle = |s\rangle = H^{\otimes n}|0\rangle^{\otimes n}$$

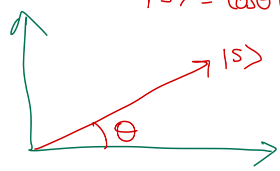
$$|\psi_2\rangle = U_f|s\rangle$$
$$= U_f\left(\sqrt{\frac{a}{2^n}}|A\rangle + \sqrt{\frac{b}{2^n}}|B\rangle\right)$$
$$= \sqrt{\frac{a}{2^n}}U_f|A\rangle + \sqrt{\frac{b}{2^n}}U_f|B\rangle$$
$$= \sqrt{\frac{a}{2^n}}(-1)^{\overbrace{f(A)}^{1}}|A\rangle + \sqrt{\frac{b}{2^n}}(-1)^{\overbrace{f(B)}^{=0}}|B\rangle$$
$$= -\sqrt{\frac{a}{2^n}}|A\rangle + \sqrt{\frac{b}{2^n}}|B\rangle$$

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$
$$f(x) = \begin{cases} 0; & x \text{ no deseado} \\ 1; & x \text{ deseado} \end{cases}$$

Notamos que el oráculo U_f marca los estados deseados ($f(x) = 1,\ \forall x \in A$) haciendo $|A\rangle \to -|A\rangle$. De esta forma, en el plano esto se verá como la reflexión del estado $|s\rangle$ alrededor de $|B\rangle$



$|S\rangle = \cos\theta\,|B\rangle + \text{sen}\,\theta\,|A\rangle$



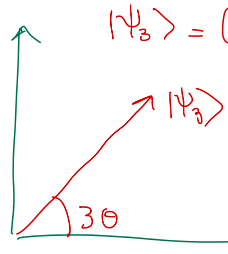
Aplicamos el difusor U_ω

$$|\psi_3\rangle = U_\omega|\psi_2\rangle$$

$|S\rangle = \sqrt{\frac{a}{2^n}}\,|A\rangle + \sqrt{\frac{b}{2^n}}\,|B\rangle$

$$= (2|s\rangle\langle s| - \mathrm{I})\left(-\sqrt{\frac{a}{2^n}}|A\rangle + \sqrt{\frac{b}{2^n}}|B\rangle\right)$$

$|\psi_3\rangle = \cos 3\theta\,|B\rangle + \text{sen}(3\theta)\,|A\rangle$



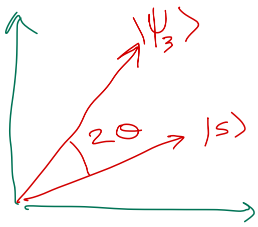
Usando

Llegar a esto

$$|s\rangle\langle s| = \frac{a}{2^n}|A\rangle\langle A| + \frac{b}{2^n}|B\rangle\langle B| + \frac{\sqrt{ab}}{2^n}[|A\rangle\langle B| + |B\rangle\langle A|]$$

Tenemos $\sqrt{\frac{a}{2^n}} = \text{sen}\,\theta$ y $\sqrt{\frac{b}{2^n}}\cos\theta$ Llegar a esto

$$|\psi_3\rangle = \sin 3\theta|A\rangle + \cos 3\theta|B\rangle = U_\omega U_f\,|s\rangle$$



$|\psi_3\rangle = U_\omega U_f\,|S\rangle$

Notamos que el efecto final luego de aplicar el oráculo y el difusor, $U_\omega U_f$, sobre $|s\rangle$,

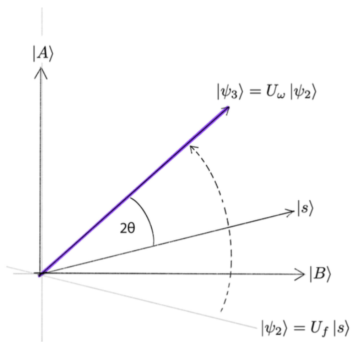
$$|\psi_3\rangle = U_\omega U_f|s\rangle$$

$|s\rangle = \cos\theta\,|B\rangle + \text{sen}\,\theta\,|A\rangle$

es una rotación antihoraria de dicho estado en un ángulp de 2θ

$$\begin{aligned}|\psi_3\rangle &= \sin(2\theta + \theta)|A\rangle + \cos(2\theta + \theta)|B\rangle \\ &= R(2\theta)|s\rangle\end{aligned}$$

Verificar



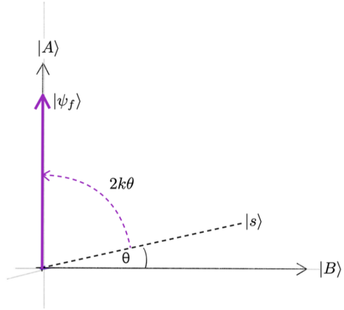
Finalmente, luego de aplicar k veces $U_\omega U_f$ sobre $|s\rangle$, tenemos el estado final $|\psi_f\rangle$

$$|\psi_f\rangle = \underbrace{(U_\omega U_f)(U_\omega U_f)\cdots(U_\omega U_f)}_{k \text{ veces}}|s\rangle$$

El cual será el resultado de la rotación del estado $|s\rangle$ para un ámngulo de $2k\theta$

$$\begin{aligned}|\psi_f\rangle &= R(2k\theta)|s\rangle \\ &= \sin(2k\theta + \theta)|A\rangle + \cos(2k\theta + \theta)|B\rangle\end{aligned}$$

El valor de k será tal que el estado final sea igual al Ket de estados deseados: $|A\rangle$



$$\begin{aligned} |\psi_f\rangle &= \sin(\underbrace{2k\theta + \theta}_{\pi/2})|A\rangle + \cos(\underbrace{2k\theta + \theta}_{\pi/2})|B\rangle \\ &= |A\rangle \end{aligned}$$

Luego (la suposición más sencilla)

$$2k\theta + \theta = \frac{\pi}{2}$$

Tenemos

$$k = \frac{\pi}{4\theta} - \frac{1}{2}$$

Asimismo, sabemos que $\sin\theta = \sqrt{\frac{a}{2^n}}$, entonces para $\sin\theta = \sqrt{\frac{a}{2^n}} \ll 1$ tenemos

$$\theta \approx \sqrt{\frac{a}{2^n}}$$

Finalmente, el número de veces que debemos aplicar $U_\omega U_f$ sobre $|s\rangle$ para maximizar la probabilidad de los estados deseados es

$$k \approx \frac{\pi}{4}\sqrt{\frac{2^n}{a}}$$

Conclusión

1. El algoritmo de Grover representa una contribución importante para la búsqueda cuántica, permitiendo una mejora cuadrática en el tiempo de búsqueda en comparación con la computación clásica.

$$\text{Cuántico: } \sim \sqrt{2^n}$$

$$\text{Clásico: } \sim 2^n$$

2. Sin embargo, su utilidad práctica está limitada por la modesta aceleración en problemas con grandes bases de datos.

5. Recursos útiles

[1] Grover L.K.: A fast quantum mechanical algorithm for database search (https://arxiv.org/abs/quant-ph/9605043),

Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996).

[2] Qiksit: Grover's Algorithm (https://learn.qiskit.org/course/ch-algorithms/grovers-algorithm)

Donaciones

Puedes donar una vez en el siguiente enlace (Ko-Fi) Buy me a coffee

(https://ko-fi.com/rcrdphysics)