Algoritmo de Grover en búsquedas no ordenadas: la ventaja de la computación cuántica

MACC Matemáticas Aplicadas y Ciencias de la Computación

Semillero de Computación Cuántica

[1]*Diego Felipe Yate Diaz* , [2]*Andrés Leonardo Manrique* ,[3]*Tomás Patiño*, [4]*Nicolás Avilán Vargas*

1 Pregrado MACC, 2 Pregrado MACC, 3 Pregrado MACC, 4 Profesor MACC

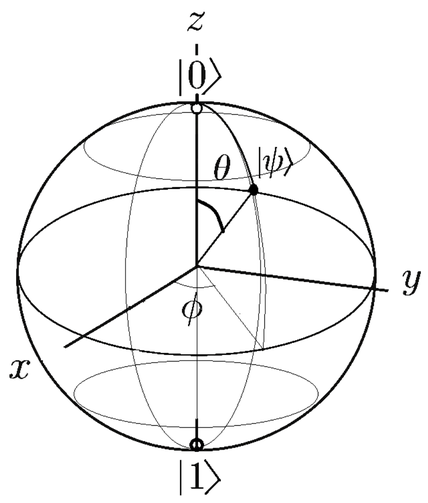
Universidad del Rosario
Escuela de Ciencias e Ingeniería

Introducción

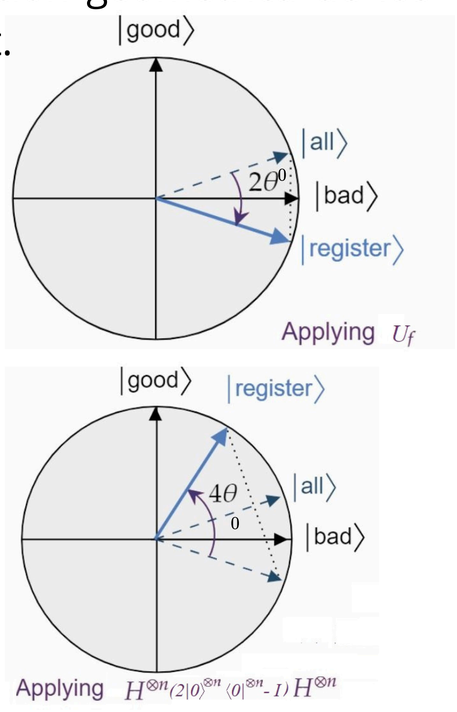
El algoritmo de Grover es un algoritmo cuántico para la búsqueda de datos no ordenados. Emplea la superposición de los qubits y operadores unitarios para reducir la complejidad clásica de búsqueda de $O(N)$ a O($\sqrt{N}$) de encontrar un elemento.

Conceptos clave

- **Computación cuántica:** computación basada en qubits que pueden ser una superposición entre el estado 0 y 1 de un bit.
- **Estado cuántico:** representación del estado de un qubit como un vector unitario en el espacio de Hilbert complejo.
- **Compuerta cuántica:** operador que transforma los estados cuánticos. Se representan con matrices unitarias.
- **Esfera de Bloch**: representación geométrica de los estados cuánticos de un qubit.



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$



Fuente: Learn Microsoft, quantum

Algoritmo de Grover

Inicialización:

- Comienza con n qubits en el estado $|0\rangle^{\otimes n}$, $N = 2^n$.
- Aplica la compuerta de Hadamard para crear una superposición uniforme.

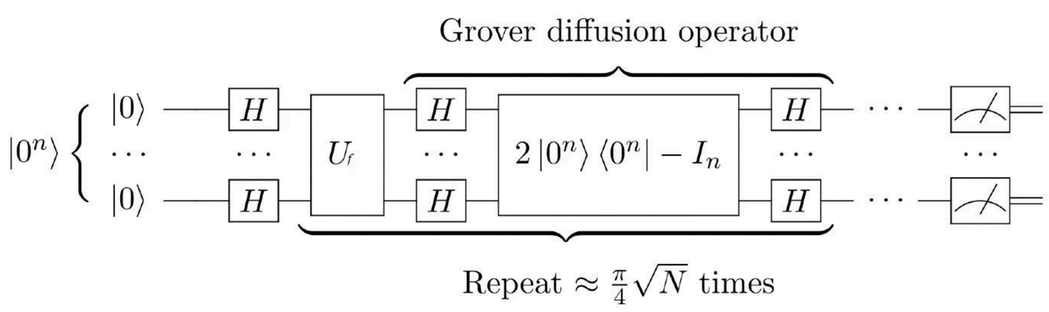
Iteración de Grover:

- **Oráculo:** Se aplica el oráculo U_f que marca el estado solución $|\omega\rangle$, invirtiendo su amplitud.
- **Difusor** (Operador de Inversión alrededor de la Media): Aplica el operador de difusión V.

Medición:

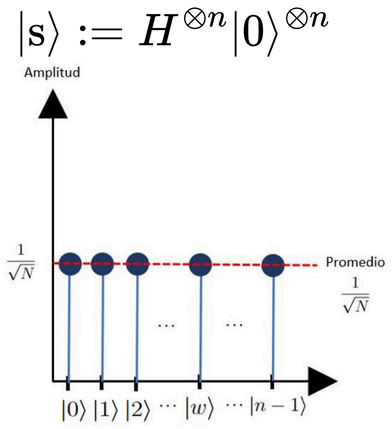
- Mide los n qubits en la base computacional.
- Con alta probabilidad, el resultado de la medición será el estado marcado $|\omega\rangle$, que es la solución a la búsqueda.

Circuito de Grover



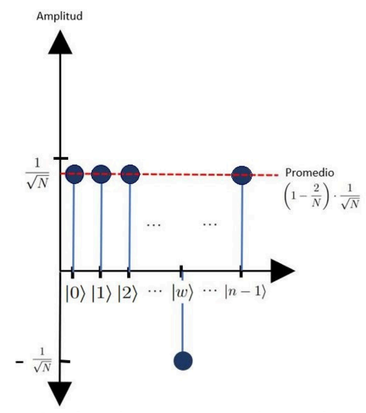
Iteraciones

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



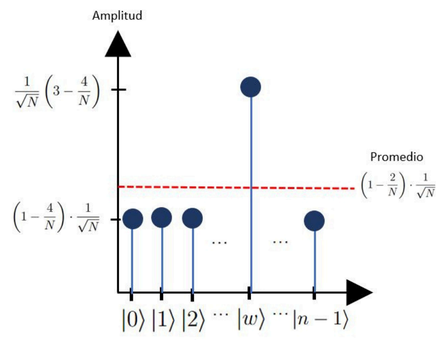
Inicialización del Algoritmo de Grover.

$$U_f|s\rangle = (I - 2|w\rangle\langle w|)|s\rangle$$



Oráculo actuando sobre $|\omega\rangle$.

$$V \cdot U_f \cdot |s\rangle = (2|s\rangle\langle s| - I) \cdot U_f \cdot |s\rangle$$



Reflejar amplitud sobre la amplitud media.

Fuente: Documentación librería qiskit

- Cada iteración de Grover (G) es una rotación de $2\theta_0$ respecto al vector inicial.

$$|\psi_t\rangle = (VU_f)^t|s\rangle = \cos((2t+1)\theta_0)|w^\perp\rangle + \sin((2t+1)\theta_0)|w\rangle$$

- Probabilidad de medir un estado solución $|\langle\omega|s\rangle|^2$

Complejidad Computacional

El algoritmo busca resaltar el estado solución, lo que implica maximizar la amplitud de $|\omega\rangle$.

El ángulo θ_0 después de t iteraciones es:

$$\theta_t = (2t+1)\theta_0 \quad \theta_0 = \arcsin(|\langle s|\omega\rangle|) = \arcsin\left(\frac{1}{\sqrt{N}}\right)$$

Para maximizar la amplitud de $|\omega\rangle$

$$\frac{\pi}{2} = (2t_{\text{optimal}} + 1)\theta_0 \quad (1)$$

Cuando *N* es grande

$$\sin(\theta_0) \approx \theta_0 \quad \theta_0 \approx \frac{1}{\sqrt{N}}$$

Reemplazando en (1)

$$(2t+1)\frac{1}{\sqrt{N}} \approx \frac{\pi}{2}$$

$$t \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2}$$

Obteniendo una cota superior

$$O(\sqrt{N})$$

Experimento

Para N=8 estados, 3 qubits. $\theta_0 = \arcsin(\frac{1}{\sqrt{8}}) \approx 0.36137$**rad**

Iteración (k)	Operador de Grover	Probabilidad
0	$(VU_f)^0$	0.12648
1	$(VU_f)^1$	0.78130
2 (óptima)	$(VU_f)^2$	0.94395
3	$(VU_f)^3$	0.32602

Para N=128 estados, 7 qubits. $\theta_0 = \arcsin(\frac{1}{\sqrt{128}}) \approx 0.0884$**rad**

Iteración (k)	Operador de Grover	Probabilidad
0	$(VU_f)^0$	0.00781
3	$(VU_f)^3$	0.33405
5	$(VU_f)^5$	0.76008
8 (óptima)	$(VU_f)^8$	0.99547
9	$(VU_f)^9$	0.98086

Conclusiones

El algoritmo de grover muestra el poder computacional cuántico revelando complejidades inferiores a los algoritmos de problemas clásicos. Esta ventaja plantea consecuencias en áreas como la ciberseguirad donde debilita la encriptación. Por otro lado, la escalabilidad de la computación cuántica depende del control sobre la frágil información, requiriendo métodos como la correción de errores para proteger la información.

Referencias

- Lov K. Grover. “A fast quantum mechanical algorithm for database search”. En: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. 1996, págs. 212-219. doi: 10.1145/237814.237866.
- Nielsen, M. A., & Chuang, I.L (2010) Quantum Computation and Quantum Information. Cambridge University Press.