Universidad Nacional del Altiplano
Facultad de Ingeniería Estadística e Informática

Informe Técnico: Algoritmo de Grover

Docente: Fred Torres Cruz

Estudiante: Eliseo Tarqui Ajahuana

Código: 241077

19 de diciembre de 2024

Enlace del Repositorio

https://github.com/Eliseo-Tarqui/eliseo

Introducción

En computación cuántica, el Algoritmo de Grover es un algoritmo cuántico para la búsqueda en una secuencia no ordenada de datos con N componentes en un tiempo $O(\sqrt{N})$, y con una necesidad adicional de espacio de almacenamiento de $O(\log N)$.

En una búsqueda normal de un dato, si tenemos una secuencia desordenada, se debe realizar una inspección lineal, que necesita un tiempo de $O(N)$. Por lo tanto, el Algoritmo de Grover es una mejora sustancial, evitando además la necesidad de la ordenación previa. La ganancia obtenida es cuadrática, lo que contrasta con otras mejoras de los algoritmos cuánticos que obtienen mejoras de orden exponencial sobre sus contrapartidas clásicas.

Al igual que otros algoritmos de naturaleza cuántica, el Algoritmo de Grover es probabilístico, produciendo la respuesta correcta con una determinada probabilidad de error, que, no obstante, puede hacerse tan baja como se desee mediante iteraciones.

Aplicaciones

Aunque el propósito del algoritmo es, como se ha indicado, la búsqueda en una secuencia, se podría describir de manera más adecuada como la *inversión de una función*. Así, si tenemos la función $y = f(x)$, que puede ser evaluada en un computador cuántico, este algoritmo nos permite calcular el valor de x dado el valor de y.

El Algoritmo de Grover también se puede utilizar para:

- Calcular la media y la mediana de un conjunto de números.
- Resolver algunos problemas de naturaleza NP-completa mediante inspecciones exhaustivas en un espacio de posibles soluciones.

Inicialización

Se considera una secuencia desordenada con N componentes. El algoritmo requiere un espacio de estados N-dimensional H, que puede modelarse con $\log_2 N$ qubits.

Numeremos las entradas de la secuencia con $0, 1, \ldots, N-1$ y seleccionemos un observable Ω, actuando sobre H, con N autovalores distintos conocidos. Cada uno de los autovalores de Ω codifica una de las entradas de la secuencia. Denotaremos los autoestados utilizando la notación bra-ket como:

$$|\psi_k\rangle$$

Y los autovalores correspondientes como:

$$\lambda_k$$

Ahora tomamos un operador unario U_ω, que actúa como una subrutina que compara las diferentes entradas de acuerdo al criterio de búsqueda. Requeriremos U_ω con los siguientes efectos:

$$U_\omega|\omega\rangle = -|\omega\rangle, \quad U_\omega|\psi\rangle = |\psi\rangle \quad \text{si } |\psi\rangle \neq |\omega\rangle.$$

Nuestro objetivo es identificar el autoestado $|\omega\rangle$, o de manera equivalente, el autovalor ω.

Iteraciones del Algoritmo

Los pasos del Algoritmo de Grover son los siguientes:

1. Inicializar el sistema al estado:
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$
2. Realizar $r(N)$ iteraciones, donde $r(N)$ es una función que depende de N.
   a) Aplicar el operador U_ω.
   b) Aplicar el operador de inversión sobre la media.
3. Realizar la medida Ω. La medida corresponderá al valor λ_ω con una alta probabilidad, para un $N \gg 1$. A partir de λ_ω, se puede obtener ω.

Implementación

Supongamos que tenemos una secuencia de 2^n elementos referenciados por su índice x, y disponemos de una función $f(x)$ que nos indica si el valor almacenado en la posición x es el que buscamos:

$$f(x) = \begin{cases} 1 & \text{si } x \text{ es el valor buscado,} \\ 0 & \text{en caso contrario.} \end{cases}$$

Oráculo

A partir de la función $f(x)$, construimos un oráculo con la operación:

$$|x\rangle \to (-1)^{f(x)}|x\rangle.$$

Inversión sobre la Media

La operación de inversión sobre la media puede escribirse como:

$$|\psi\rangle \to 2|\psi\rangle\langle\psi| - I.$$

Iteración de Grover

Una iteración de Grover consiste en:

- Aplicación del oráculo.
- Aplicación de la inversión sobre la media.

Por lo tanto, la iteración completa puede escribirse como:

$$G = (2|\psi\rangle\langle\psi| - I)U_\omega.$$

Conclusiones

El Algoritmo de Grover demuestra el potencial de la computación cuántica para resolver problemas de búsqueda y optimización con una eficiencia superior a los métodos clásicos. Este informe describe las bases teóricas y aplicaciones prácticas del algoritmo, destacando su relevancia en la computación moderna.

Flujograma del Algoritmo de Grover