Computación Cuántica: El Algoritmo de Grover

Brayan A. Atoccsa Aguilar[1], Walter S. Felipe Gaspar[3], Shigueru E. Nagata Tejada[2] , Ruben Puga Correa[3]

[1]Universidad Nacional San Luis Gonzaga de Ica
[2]Universidad Nacional Mayor de San Marcos
[3]Universidad Nacional de Ingeniería

Abstract

En el presente trabajo se realizo un análisis del algoritmo de Grover, para ello se hicieron los calculos para un determinado caso y se cotejaron con una simulación llevada a cabo en la plataforma **Quantum Experience de IBM.**

1 Introducción

La computación cuántica a pesar de ser un tema que ocupa las labores de los mas avanzados laboratorios de investigación, es una idea que surge hace poco más de tres décadas. Siendo uno de los pioneros David Deutsch quien en 1985 describió el primer modelo para una máquina de Turing cuántica, probando de esa manera que era posible almenos en teoría diseñar una máquina capaz de realizar cálculos complejos. Pero tuvieron que pasar más de diez años antes de que Issac Chuang y su equipo, fabricaran la primera computadora cuántica de 1 qubit.

Adentrándonos en el funcionamiento de una computadora cuántica, se hace imperante mencionar la diferencia fundamental entre esta y una computadora clásica, y nos referimos a su unidad básica de información. En una computadora clásica, la unidad mínima de información es el bit, que puede tomar solo un valor por vez, ya sea 0 ó 1; en contraste, una computadora cuántica posee qubits, los cuales pueden tomar valores distintos simultaneamente, 0 y 1. Siendo más estrictos, los valores en este caso son estados cuánticos, y la capacidad de simultaneidad, hace referencia a la superposición de estados cánticos.

Gracias a esta capacidad inherente de simultaneidad, el poder de cálculo de una computadora cuántica es muy superior al de su contraparte clásica. Pero esta capacidad, provoca un ligero inconveniente, y es que los algoritmos que funcionan tan bien en las computadoras clásicas, fracasan totalmente. Es por ello que se desarrollaron algoritmos especializados, entre los más importantes podemos mencionar:

- Algoritmo de Short
- Algoritmo de Grover
- Algoritmo de Deutsch-Jozsa

Estos algoritmos cuánticos, al igual que los clásicos, se conforman de una serie de pasos, que en este caso son transformaciones unitarias, que son implementadas a través de conpuertas cuánticas simples, que se combinan dando lugar a transformaciones más complejas.

1.1 Compuerta cuántica

Una compuerta cuántica es una transformación unitaria, que se lleva a cabo, ya sea sobre un qubit o sobre un conjunto de ellos, dicha transformación actua sobre los estados cuánticos (qubits) como un operador.

Existen versiones clásicas de algunas compuertas cuánticas, pero en su mayoria, las compuertas cuánticas solo existen en el ámbito de la computación cuántica, ya que exiben comportamientos imposibles de emular clásicamente.

Otra característica de las compuertas cuánticas es que deben ser reversibles, ahora es cierto que se pueden hallar compuertas no reversibles, pero su planteamiento es más complicado y no son tan comunes.

Las compuertas cuánticas de mayor interes para nosotros, son las siguientes:

- Compuerta de Hadamard

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Compuerta Pauli-X (NOT)

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Compuerta NOT controlada

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

1.2 Algoritmo cuántico

Un algoritmo cuántico, es aquel algoritmo que se ejecuta sobre un modelo realista de computación cuántica. Siendo el mas extendido de estos modelos **El modelo de familias uniformes de circuitos cuánticos acíclicos** o modelo de circuitos, para abreviar. Además dicho modelo, posee la característica de ser discreto, es decir que posee un espacio de estados discreto y se ejecuta en pasos discretos de tiempo. Cabe mencionar que existen algoritmos que han sido desarrollados considerando un modelo de computación cuántica continuo en el tiempo.

Muchos algoritmos pueden ser considerados como **cajas negras** u **oraculos**, es decir, que son subrutinas o subcircuitos que implementan alguna operación o función. Dichas funciones u operaciones, son implementadas a traves de compuertas cuanticas, las cuales conforman un circuito.

2 Algoritmo de Grover

El algoritmo fue presentado por Lov K. Grover en 1996, y se define como un algoritmo de busqueda. El cual posee una serie de ventajas al ser comparado con los algoritmos clásicos, tales como:

- La eficiencia del algoritmo está en el orden de $O(\sqrt{N})$, la cual supera a los mejores algoritmos clásicos que poseen una eficiencia del orden de $O(N)$.
- A diferencia de los algoritmos clásicos, no es requisito del algoritmo de Grover, que la lista sobre la cual se va a realizar la búsqueda, se encuentre ordenada de alguna forma específica.

Los pasos que se llevan a cabo en el algoritmo son los siguientes:

- Generación de una superposición de estados uniforme

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

  donde: $N = 2^n$ siendo $\mathbf{n}$ el número de qubits.

- Aplicación de la función U_f (función oráculo).

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

  donde:

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

  siendo x^* el estado buscado.

- Inversión sobre el promedio

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

  donde I es la identidad

podemos representar una iteración del algoritmo como:

$$|\psi_{i+1}\rangle = U_s U_f |\psi_i\rangle$$

Finalmente podemos representar todas las iteraciones del algoritmo, del siguiente modo:

$$|\psi_t\rangle = (U_s U_f)^t |\psi_0\rangle$$

Implementación

El algoritmo de Grover posee la función U_f que es llamada oráculo o caja negra. Como en el presente trabajo, se utilizaron solo 2 qubits, entonces $N = 2^2 = 4$, lo cual indica que se puede implementar de 4 formas distintas la función U_f dependiendo de que estado es el que estemos buscando.

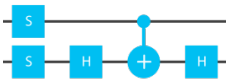

Figura 1: Fuente: Quantum Experience

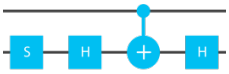

Figura 2: Fuente: Quantum Experience

Figura 3: Fuente: Quantum Experience

Figura 4: Fuente: Quantum Experience

3 Cálculo teórico

Para la realización del cálculo teórico, se consideró la siguiente implementación del algoritmo de Grover:

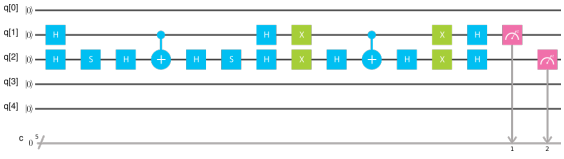

Figura 5: Fuente: Quantum Experience

Iniciamos con :

$$q[1] = 1\,|0\rangle + 0\,|1\rangle \rightarrow |0\rangle$$
$$q[2] = 1\,|0\rangle + 0\,|1\rangle \rightarrow |0\rangle$$

luego aplicamos la compuerta de Hadamard, a cada qubit

$$\begin{aligned} Hq[1] &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} Hq[2] &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \end{aligned}$$

a continuación aplicamos la función U_f implementada como se muestra en la figura 2, obteniendose:

$$q[1] = \frac{1}{\sqrt{2}}(1\,|0\rangle + i\,|1\rangle)$$
$$q[2] = \frac{1}{\sqrt{2}}(1\,|0\rangle - 1\,|1\rangle)$$

luego aplicamos las compuertas de hadamard

$$\begin{aligned} Hq[1] &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1+i \\ 1-i \end{pmatrix} \end{aligned}$$

$$\begin{aligned} Hq[2] &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 0 \\ 2 \end{pmatrix} \end{aligned}$$

Ahora aplicamos la funcion U_s implementada como:

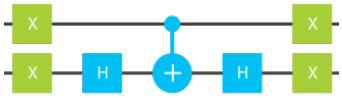

Figura 6: Fuente: Quantum Experience

obtenemos:

$$q[1] = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$$
$$q[2] = \frac{1}{2}\begin{pmatrix} 0 \\ 2 \end{pmatrix}$$

Por último, aplicamos la compuerta de Hadamard a ambos estados, obteniendo

$$\begin{aligned} Hq[1] &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \\ Hq[2] &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 0 \\ 2 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{aligned}$$

4 Resultados

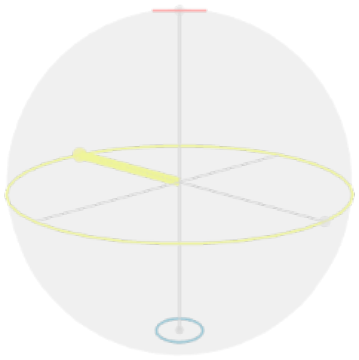

Figura 7: Fuente:Quantum Experience

La figura 7 es la esfera de bloch, que se obtiene al ejecutar la simulación, en la plataforma Quantum Experience, se observa que el estado obtenido es el $|-\rangle$ de la base de hadamard. Para una mejor visulización se tiene la siguiente figura, que es la misma representación, pero se ha rotado la esfera, con el objetivo de que se observe mejor.

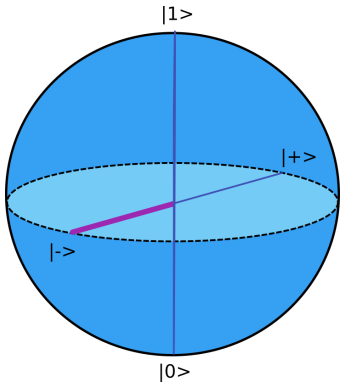

Figura 8: Fuente:Propia

5 Conclusiones

- Para los cálculos teóricos , se utilizó un diseño de U_f, que permitía obtener el estado $|-\rangle$ de la base de hadamard, y al compararlo con lo obtenido en la simulación, se verificó su validez.
- Solo fue necesario realizar una vez el cálculo, ya que por el diseño del algoritmo, el resultado (estado) obtenido siempre será el mismo.
- La plataforma Quantum Experience de IBM, nos fue de mucha ayuda, al permitirnos tener acceso a un computador cuántico real, asi como a sofisticadas simulaciones del mismo.
- Al utilizarse dos qubits la eficiencia del algoritmo es del orden de $O(2)$ comparada con los algoritmos clásicos que poseen una eficiencia, del orden de $O(4)$, aparenta no haber una gran diferencia; pero si se toma en cuenta que los cubits pueden trabajar en simultaneo sobre varios valores, se hace evidente que al tener una lista

de gran tamaño el tiempo de ejecución se reduce significativamente.

Referencias

[1] Barro Ameneiro , *Fronteras de la Computacion*, 2002, cap 5

[2] Eleanor Rieffel and Wolfgang Polak , *Quantum Computing A Gentle Introduction*,The MIT Press Cambridge, Massachusetts London, England, 2011, cap 9

[3] Giuliano Benenti , *Principles of Quantum Computation and Information - Volume II Basic Tools and Special Topics*,World Scientific Publishing Co., 2007, cap 3

[4] Richard J. Lipton, Kenneth W. Regan , *Quantum Algorithms via Linear Algebra A Primer*,The MIT Press, 2014, cap 13

[5] Jaime Coello de Portugal Vazquez , *Diseño y simulación de un procesador cuántico*, Arquitectura y tecnología de computadores, 2014

[6] wikipedia , *Grovers algorithm*, www.en.wikipedia.orgwikiGrover27s_algorithm,