ESCUELA COLOMBIANA DE INGENIERIA JULIO GARAVITO

PROGRAMA DE INGENIERIA DE SISTEMAS

PROYECTO DE GRADO

COMPUTACIÓN CUÁNTICA:

IMPLEMENTACIÓN DE ALGORITMOS DE SHOR Y GROVER EN EL COMPUTADOR CUÁNTICO DE IBM

Autor:

Cesar Augusto Vega Fernández

Johan Sebastián Ramírez Celis

Director:

Luis Daniel Benavides Navarro

Bogotá D.C 2017

Resumen

Este proyecto estudia el estado del arte en computación cuántica, explorar a profundidad los algoritmos de Grove y Shor, y realizar implementaciones y extensiones de dichos algoritmos en el computador cuántico de IBM.

Las contribuciones concretas de este proyecto son primero material didáctico para la enseñanza de Computación Cuántica, segundo Documento que describe el estado del arte, y los algoritmos de Grover y Shor, y por último las implementaciones de los algoritmos en la máquina de IBM.

Abstract

This project studies the state of the art in quantum computing, it explores in depth the algorithms of Grove and Shor, and performs the implementations and extensions of those algorithms in the IBM quantum computer.

The concrete contributions of this project are: first didactic material related to quantum computing, second a document that describes the state of the art, and the algorithms of Grover and Shor, and finally the implementations of the algorithms in the IBM machine.

Contenido

1 **Introducción**.

Computación cuántica nace como una alternativa al paradigma computacional actual basado en máquinas de Turing y de Von-Neumann, este nuevo paradigma pretende dar fin a los problemas no tratables llamados así debido a la gran cantidad de operaciones que son necesarias para encontrar una solución además se pretende mejorar los modelos que dependan de una gran cantidad de variables, para esto se hace uso de algunas propiedades de la física cuántica las cuales detallaremos más adelante, gracias a estas podemos hacer más operaciones en una misma unidad de tiempo disminuyendo radicalmente los tiempos de respuesta (Yanofsky & Manucci, 2008).

Esto tendría potenciales aplicaciones en la medicina, la física, la química, Big data, entre otros. Por ejemplo, probar el efecto que tiene un nuevo fármaco sin la necesidad de usar sujetos de prueba, podríamos simplemente correr una simulación donde se tengan en cuenta varios tipos de pacientes donde la diferencia entre paciente y paciente está dada por las variables que nos interesa estudiar.

Actualmente hay una gran cantidad de personas y empresas que están trabajando en computación cuántica por lo que ya existe una gran cantidad de material al respecto.

Lo que se pretende con este proyecto es estudiar el estado del arte en computación cuántica, explorar a profundidad los algoritmos de Grove y Shor, y realizar implementaciones y extensiones de dichos algoritmos en el computador cuántico de IBM.

Las contribuciones de este proyecto son primero material didáctico para la enseñanza de Computación cuántica, segundo Documento que describe el estado del arte, los algoritmos de Grover y Shor y por último implementaciones de los algoritmos en la máquina de IBM.

El documento contiene primero un marco teórico con las convenciones y una breve conceptualización de algunos términos de gran importancia para el entendimiento de la computación cuántica como lo son número complejos, operaciones con números complejos, espacios vectoriales complejos, propiedades de los espacios vectoriales complejos, teoría cuántica básica, entre otros. Además, se desarrollan temas como computación donde se explican los elementos necesarios para hacer cómputos usando una maquina cuántica, algoritmos cuánticos donde se describe cual es el objetivo y cómo funcionan los algoritmos de Grove y Shor, conclusiones y logros del proyecto, por último, la bibliografía que fue usada a lo largo del proyecto.

2 Marco teórico

2.1 Convenciones

$$V, W, X = hace\ referencia\ aun\ espacio\ vectorial\ complejo.$$

$$V_i, W_i, V_i = Hace\ referencia\ a\ i-ésimo\ elemento\ del\ espacio\ vectorial$$

$$c, c_i, = Hace\ referencia\ a\ un\ numero\ complejo.$$

2.2 Números complejos

Los números complejos nacen como como respuesta a la ecuación 1, se construyó toda una teoría matemática sobre los números complejos, estos no fueron formalmente usados sino hasta que salió la introducción de análisis de Fourier y ondas donde en su investigación uso números complejos, este fue un importante paso para usar números complejos en la teoría cuántica pues la mecánica cuántica está basada en gran parte en la mecánica de ondas.

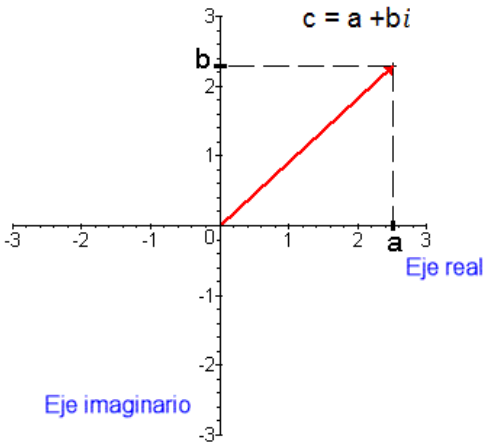
$$x^2 = -1, i = \sqrt{-1}$$

ecuación 1

Lo primero que debemos saber es que un número complejo es que se expresa de la forma (ecuación2), Donde a y b son números que pertenecen a los números reales.

$$c = a + b \times i = a + bi = (a, bi)$$

ecuación 2



Gráfica 1 - Representación de un número complejo como un vector

ya que los números complejos se pueden expresar y ver como un vector este también posee la propiedad de los vectores modulo o magnitud donde

$$|c| = |a + bi| = +\sqrt{a^2 + b^2}$$

ecuación 4

$$|c|^2 = a^2 + b^2$$

ecuación 5

$$|c_1||c_2| = |c_1 \times c_2|$$

ecuación 6

$$|c_1 + c_2| \leq |c_1| + |c_2|$$

ecuación 7

Los números complejos se pueden expresar como coordenadas polares $\rho\ es\ modulo\ del\ vector$ y $\theta\ es\ el\ angulo\ con\ el\ eje\ de\ los\ reales$

$$a = \rho \cos\theta$$

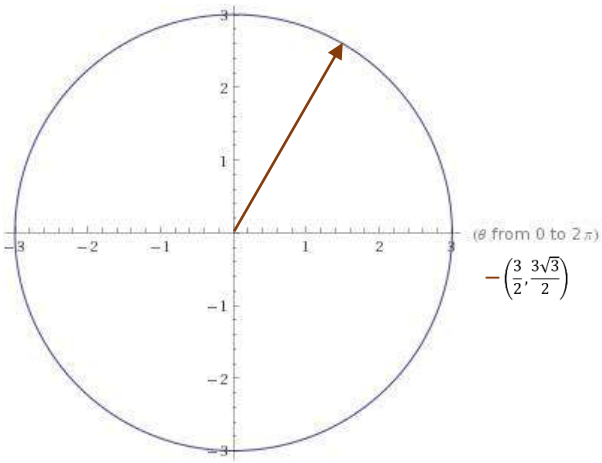
ecuación 8

$$b = \rho \sin\theta$$

ecuación 9

$$c = \rho\cos(\theta) + \rho\sin(\theta)\, i$$

ecuación 10



Gráfica 2 - Pasar de coordenadas polares a un vector complejo

Los números complejos poseen la propiedad de ser cerrados en la suma, resta,

multiplicación y división es decir que al aplicar cualquiera de estas operaciones en dos números complejos el resultado será un numero complejo (ecuación 3):

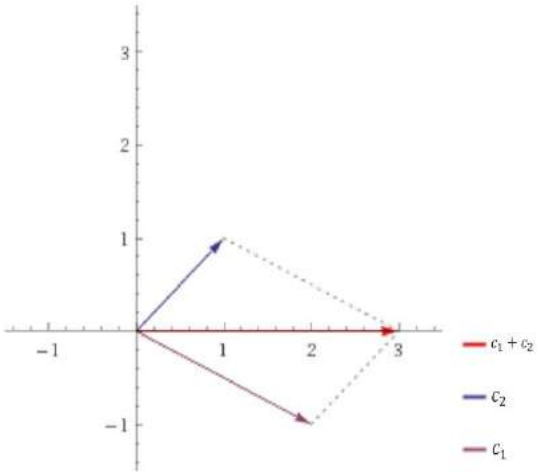
$$a \cdot b = s\,, \qquad a, b, s \in \mathbb{C}$$

ecuación 11

la suma se define como:

$$c_1 + c_2 = (a_1 + b_1 i) + (a_2 + b_2 i)$$
$$= (a_1 + a_2, (b_1 + b_2) i)$$

ecuación 12

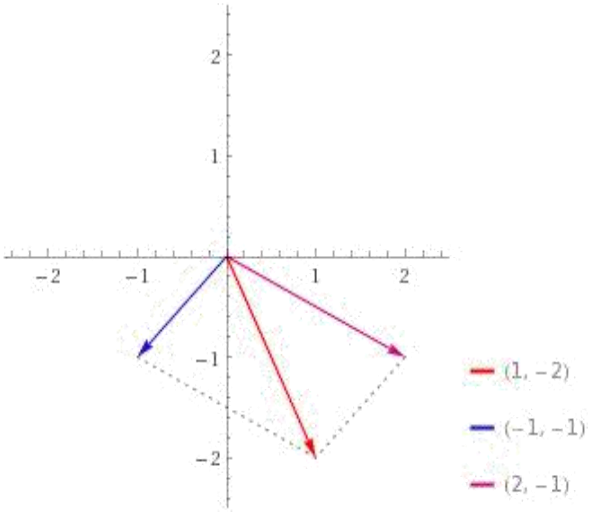


Gráfica 3 - la suma de vectores c_1 y c_2

la resta se define como:

$$c_1 - c_2 = (a_1 + b_1 i) - (a_2 + b_2 i)$$
$$= (a_1 - a_2, (b_1 - b_2) i)$$

ecuación 13



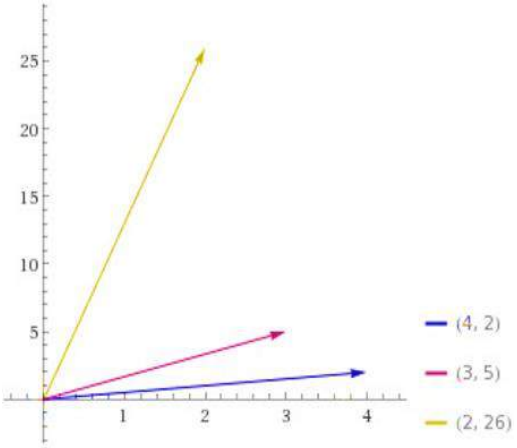
Gráfica 4 - Resta de vectores c_1 y c_2

La multiplicación se define como:

$$c_1 \times c_2 = (a_1 + b_1 i) \times (a_2 + b_2 i)$$

$$= (a_1 a_2 - b_1 b_2, (a_1 b_2 + a_2 b_1) i)$$

ecuación 14



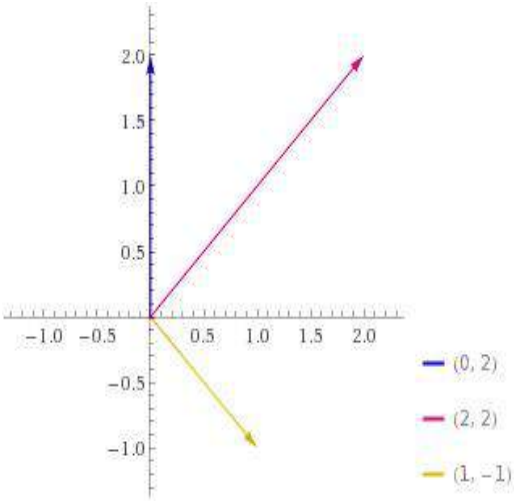
Gráfica 5 - la multiplicación de vectores c_1 y c_2

La división se define como:

$$\frac{c_1}{c_2} = \frac{a_1 + b_1 i}{a_2 + b_2 i}$$

$$= \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} + \frac{a_2 b_1 - a_1 b_2}{a_2^2 + b_2^2} i$$

ecuación 15



Gráfica 6 - la división de c_1, c_2

la suma es conmutativa

$$c_{1+}c_2 = c_2 + c_1$$

ecuación 16

la suma y la multiplicación son asociativas

$$(c_1 + c_2) + c_3 = c_1 + (c_2 + c_3)$$

ecuación 17

$$(c_1 \times c_2) \times c_3 = c_1 \times (c_2 \times c_3)$$

ecuación 18

la suma, la resta y la multiplicación tienen identidad

$$c_1 \pm 0 = c_1$$

ecuación 19

$$c_1 \times 1 = c_1$$

ecuación 20

La multiplicación distribuye sobre la suma

$$c_1 \times (c_2 + c_3) = (c_1 \times c_2) + (c_1 \times c_3)$$

ecuación 21

Además de estas operaciones para los números complejos está definida la conjugada

$$\bar{c} = a - (bi)$$

ecuación 22

$$\bar{c_1} + \bar{c_2} = \overline{c_1 + c_2}$$

ecuación 23

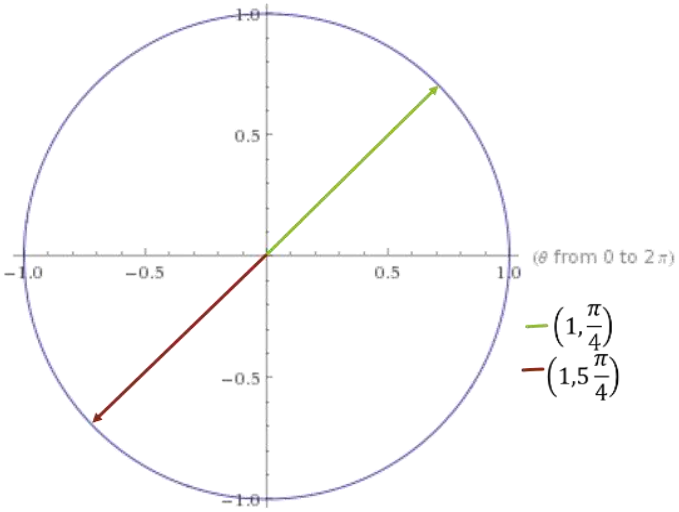
$$\bar{c_1} \times \bar{c_2} = \overline{c_1 \times c_2}$$

ecuación 24

Existen dos tipos de potencia, la primera es la potencia no fraccionada donde se obtiene un incremento o reducción del vector que representa un numero complejo

$$c^n = (p^n, n\theta\ )$$

ecuación 25



Gráfica 7 - potencias n

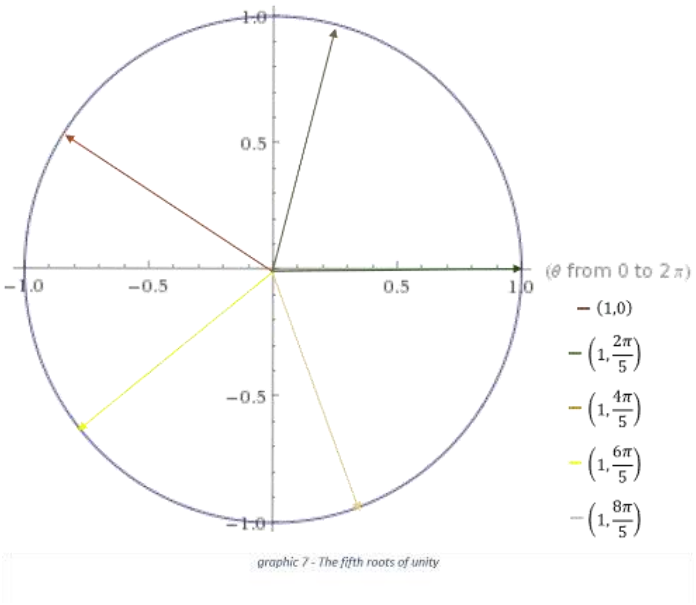
la segunda es la potencia fraccionada, esta tiene múltiples respuestas ya que la potencia fraccionada divide la circunferencia en n partes.

$$c^{\frac{1}{n}} = \left(p^{\frac{1}{n}}, \frac{1}{n}\theta\ \right)$$

ecuación 26

$$c^{\frac{1}{n}} = \left(\sqrt[n]{\rho}, \frac{1}{n}(\theta + k2\pi)\right)$$

ecuación 27



Gráfica 8 - potencias n fraccionadas

la representación de los polinomios

$$P(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0.$$

ecuación 28

Donde $P(x)$ es una trasformación de la forma.

$$P(x): \mathbb{C} \longrightarrow \mathbb{C}$$

ecuación 29

2.3 Espacios vectoriales complejos

2.3.1 Definiciones y ejemplos

Los números complejos cumplen las siete propiedades para ser llamado un espacio.

1. La suma es conmutativa y asociativa.
2. La suma tiene un elemento identidad (0, 0).
3. La multiplicación es conmutativa y asociativa.
4. La multiplicación tiene un elemento identidad (1, 0).
5. La multiplicación distribuye con respecto a la suma.
6. La resta está definida para todos los números complejos.
7. No se puede dividir por cero (0, 0).

Al ser un espacio también podemos ubicar el número dentro de un plano, hallar la magnitud del vector que hace con (0, 0), hacer transformación a coordenadas polares, usar trigonometría, entre otros.

Usando un conjunto de números de complejos se pueden definir un espacio vectorial.

$$\mathbb{C}^n = \mathbb{C}_1 \times \mathbb{C}_2 \times \mathbb{C}_3 \times \cdots \times \mathbb{C}_n$$

ecuación 30

$$\begin{bmatrix} \mathrm{A} + \mathrm{B}i \\ \mathrm{C} + \mathrm{D}i \\ \vdots \\ \mathrm{G} + \mathrm{H}i \\ \mathrm{E} + \mathrm{F}i \end{bmatrix}$$

ecuación 31

2.3.2 Base y dimensión

Una combinación lineal es la forma de expresar un vector como la sumatoria de la multiplicación de elementos pares relacionados entre sí (ecuación 34).

$$X = \{X_0, X_1, \cdots, X_{n-1}\}$$

ecuación 32

$$W = \{W_0, W_1, \cdots, W_{n-1}\}$$

ecuación 33

$$V = X_0W_0 + X_1W_1, \cdots, X_{n-1}W_{n-1} = \sum_{i=0}^{n-1} X_iW_i$$

ecuación 34

un conjunto de espacios vectoriales es llamado independiente si:

$$0 = c_0 * V_0 + c_1 * V_1 + \cdots + c_{n-1} * V_{n-1}$$

ecuación 35

Una base es un conjunto $\mathcal{B} = \{V_0, V_1, \cdots, V_{n-1}\} \subseteq \mathbb{V}$ de un espacio vectorial, si todo elemento del espacio vectorial se puede escribir en términos (combinación lineal) de los elementos de la base, además los elementos de la base forman un sistema linealmente independiente.

La dimensión de un espacio vectorial complejo es el número de elementos en la base (cardinal del conjunto).

2.3.3 Operaciones básicas

Al igual que en algebra lineal poseen operaciones como suma, resta, multiplicación, multiplicación por un escalar real, multiplicación por un escalar complejo, transpuesta, conjugado, adjunta, producto interno, producto tensor, Además de estas operaciones hay que tener en cuenta conceptos como bases de un espacio vectorial, dimensiones de un espacio vectorial, matrices unitarias, matrices hermitiana y espacios de Hilbert, probabilidad con números complejos,

A continuación, vamos a explicar cada una de las operaciones y de los conceptos mencionados anteriormente.

La suma y la resta de espacios vectoriales se operan de la misma manera, se suma o se restan los elementos correspondientes, por lo que hay que tener en cuenta que los espacios deben contar con las mismas dimensiones, estas operaciones respetan el elemento identidad.

$$(V + 0 = V + 0 + V)\ ,\ (V - 0 = V = 0 - V)$$

ecuación 36

Además, cada vector tiene un inverso o un negativo y Como podemos ver en la figura 8, la resta se puede expresar como una suma.

$$(V - V = 0),(V + (-V) = 0)$$

ecuación 37

La multiplicación por un escalar consiste en multiplicar una entrada que puede ser un numero complejo con cada uno de los elementos que componen el espacio vectorial complejo.

$$c \cdot \begin{bmatrix} V_0 \\ V_1 \\ \vdots \\ V_{n-1} \end{bmatrix} = \begin{bmatrix} c \times V_0 \\ c \times V_1 \\ \vdots \\ c \times V_{n-1} \end{bmatrix}$$

ecuación 38

Estos poseen las siguientes propiedades

- $1 \cdot V = V$
- $c_1 \cdot (c \cdot V) = (c_1 \times c_2) \cdot V$
- $c_1 \cdot (V + W) = (c_1 \cdot V) + (c_1 \cdot W)$
- $(c_1 + c_2) \cdot V = (c_1 \cdot V) + (c_2 \cdot V)$

La transpuesta se denota con la letra t en mayúscula (T) como superíndice (V^T) y se define como:

$$V^T[j,k] = V[K,J].$$

ecuación 39

$$\begin{bmatrix} \mathrm{V}_0 \\ V_1 \\ \vdots \\ V_{n-1} \end{bmatrix}^T = [V_0, V_1, \dots, V_{n-1}]$$

ecuación 40

Posee las siguientes propiedades

- $(V^T)^T = V$
- $(V + W)^T = V^T + W^T$
- $(c_1 \cdot V)^T = c_1 \cdot V^T$

la conjugada se denota con usando línea sobre el nombre del espacio ($\bar{V}$), consiste en aplicar el conjugado (cambiar el signo de la parte imaginaria del número complejo) a cada uno de los elementos del espacio.

$$\bar{V} = \begin{bmatrix} \bar{V}_0 \\ \bar{V}_1 \\ \vdots \\ \overline{V_{n-1}} \end{bmatrix}$$

ecuación 41

Posee las siguientes propiedades

- $\bar{\bar{V}} = V$
- $\overline{(V + W)} = \bar{V} + \bar{W}$
- $\overline{c \cdot V} = \bar{c} \cdot \bar{V}$

La adjunta se denota con una cruz (†) en superíndice ($V^{\dagger}$) y se define como la combinación de las dos operaciones anteriormente mencionadas (la transpuesta y la conjugada), no importa cuál de las dos operaciones de realice primero.

$$\mathrm{V}^{\dagger} = (\bar{V})^{T} = \overline{(V^{T})}\ , V^{\dagger}[j,k] = \overline{V[K,J]}.$$

ecuación 42

Posee las siguientes propiedades

- $(V^{\dagger})^{\dagger} = V$
- $(V + W)^{\dagger} = V^{\dagger} + W^{\dagger}$
- $(c_1 \cdot V)^{\dagger} = c_1 \cdot V^{\dagger}$

La multiplicación entre dos espacios se comporta de la misma manera que en el álgebra lineal,

$$V^{m\times n} \star W^{n\times p} \rightarrow X^{m\times p}$$

ecuación 43

Como podemos ver en la figura 15 las columnas del primer espacio deben corresponder con las filas del segundo espacio, generando un tercer espacio que tienen las filas del primer espacio y las columnas del segundo espacio.

Se define como la sumatoria de la multiplicación de los elementos y una columna h (ecuación 45).

$$V^{m\times n}, W^{n\times p}$$

ecuación 44

$$(V \star W)[j,k] = \sum_{h=0}^{n-1} (V[j,h] \times W[h,k])$$

ecuación 45

Posee las siguientes propiedades

$$I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

ecuación 46

- $(V \star W) \star X = V \star (W \star X)$
- $I_n \star V = V = V \star I_n$
- $V \star (W + X) = (V \star W) + (V \star X)$

  $(V + W) \star X = (V \star X) + (W \star X)$
- $(V \star W)^T = W^T \star V^T$

- $\overline{(V \star W)} = \bar{V} \star \bar{W}$
- $(V \star W)^{\dagger} = W^{\dagger} \star V^{\dagger}$

2.3.4 Producto interno

El producto interno sobre es una trasformación que va desde los espacios vectoriales complejos a los números complejos

$$\langle V, W \rangle \longrightarrow c$$

ecuación 47

Que se define como la suma de los productos de los elementos correspondientes:

$$\langle V, W \rangle = V * W = \sum_{j=0}^{n} V_j \, W_J$$

ecuación 48

Se usa para saber si el Producto interno es cero, lo que implica que los espacios son ortogonales

2.3.5 Valores propios y Vectores propios

Dado un espacio vectorial V y una transformación $T: V \to V$, donde λ es un escalar diferente de cero ($\lambda \neq 0$) tal que:

$$T(V) = \lambda W$$

ecuación 49

Se dice que λ es un valor propio de V y W es llamado un vector propio de V, el conjunto de

los vectores propios de V forman un subespacio que es llamado espacio propio.

2.3.6 Matrices unitarias y Hermitiana

Matriz Identidad

$$I_n = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix}$$

ecuación 50

Matriz simétrica es una matriz si

$$A^T = A$$

ecuación 51

Una matriz n x n es llamada Hermitiana si:

$$A^\dagger = A$$

$$A^\dagger[j,k] = \overline{A[k,j]}$$

ecuación 52

Una matriz n x n es llamada Unitaria si

$$A^\dagger \star A = A \star A^\dagger = I_n$$

ecuación 53

2.3.7 Producto Tensor

Está definido como $(A \otimes B)$

$$\begin{bmatrix} x \\ y \end{bmatrix} \otimes \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} xa \\ xb \\ xc \\ ya \\ yb \\ yc \end{bmatrix}$$

ecuación 54

Posee las siguientes propiedades

- $A \otimes (B \otimes C) = (A \otimes B) \otimes C$
- $(A \otimes B)^{\dagger} = A^{\dagger} \otimes B^{\dagger}$
- $(A \star A') \otimes (B \star B') = (A \otimes B) \star (A' \otimes B')$

2.4 Teoría cuántica Básica

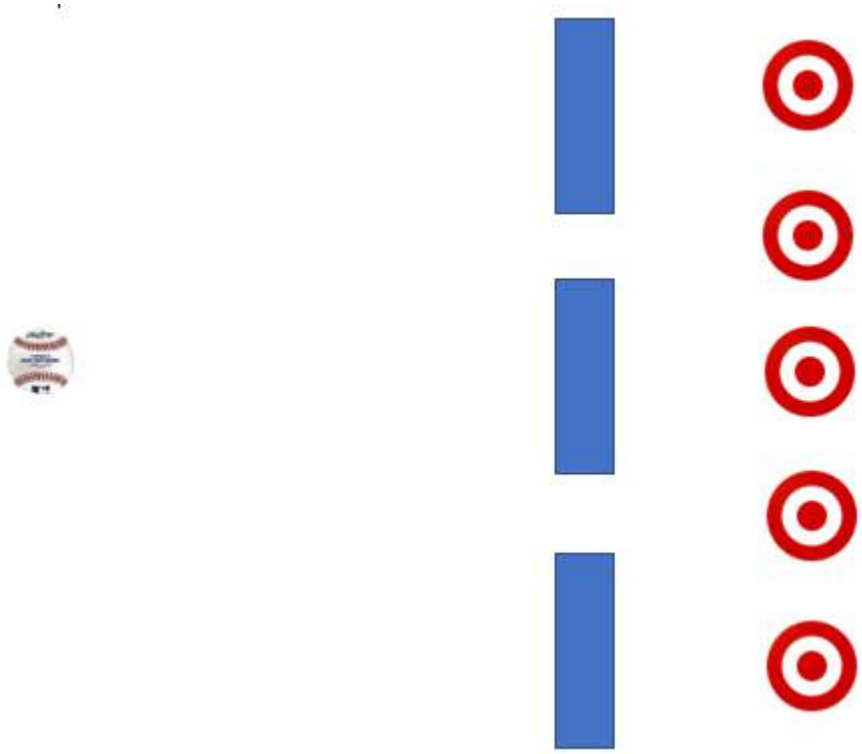
La física ha jugado un rol trascendental en todos los diferentes inventos del hombre y los computadores no han sido la excepción, su nivel de desarrollo va a la mano con los descubrimientos y adelantos tecnológicos, aunque estos dispositivos en la actualidad tienden a ser más pequeños con mayor capacidad, todavía siguen siendo insuficientes, primero porque estamos llegando a los límites de la arquitectura basada en transistores (uno y ceros) y segundo es no están diseñadas para las necesidades de cómputo que exigen problemas con manejo de muchas variables, como por ejemplo el modelamiento de fármacos, enfermedades actuando en el cuerpo humano e incluso como actúa una simple molécula cafeína en nuestro organismo.

En 1982, el nobel de física Richard Feynman reto a la comunidad científica para la creación de un computador que se basará en mecánica cuántica aprovechando las propiedades ya conocidas en ese entonces dadas las investigaciones llevadas por varios científicos de la época como Albert Einstein, este reto fue argumentado por la idea de que solo la física cuántica puede simular correcta y eficiente los procesos cuánticos que se producen en la naturaleza.

Las dos propiedades más importantes en las que se basa un computador cuántico es la superposición y el entrelazamiento cuántico. Un computador cuántico realiza sus operaciones con bit cuánticos, como bien sabemos un computador clásico realiza operación

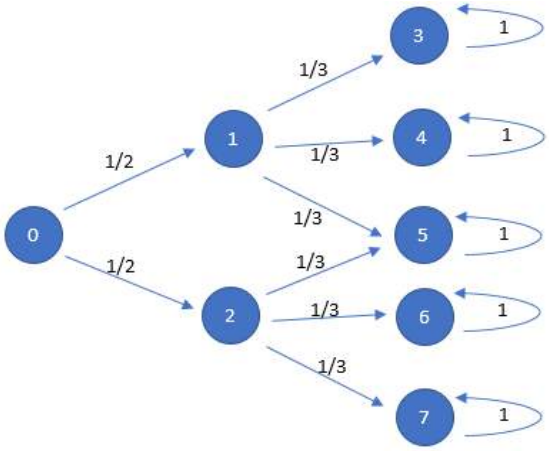
en bits, es decir manipulación de voltajes los cuales los podemos traducir como 0 o 1, por lo cual un bit puede tener dos estados distinguibles, ahora bien, un bit cuántico también puede tener un estado de 0, 1 o los dos estados simultáneamente, los cuales se representan como $\{|0\rangle, |1\rangle, |0\rangle + |1\rangle\}$ respectivamente. En 1937, Erwin Schrödinger por medio de su experimento explica la diferencia entre interacción y medida en el campo de la mecánica cuántica, en la paradoja del gato de Schrödinger, el cual consiste en imaginar un gato dentro de una caja la cual posee un dispositivo que tiene una ampolleta de vidrio que contiene veneno, un martillo y un detector de partícula alfa, al lado de este detector se encuentra un átomo radiactivo el cual tiene un 50% de posibilidad de generar o no una partícula alfa cada cierto tiempo, la cual si se llega a generar la partícula después de un tiempo el detector se acciona dejando caer el martillo sobre la ampolleta, rompiéndola y dejando salir el veneno, como resultado de esta interacción, en el interior de la caja, puede que el gato esté vivo o muerto. Por lo cual si intentamos describir lo que ocurre dentro de la caja usando las leyes de la mecánica cuántica, como resultado obtenemos una función extremadamente compleja, la cual nos deja como resultado de la superposición de dos estados donde el gato a la vez estaría vivo y muerto.

Como ya vimos anteriormente, los estados cuánticos se pueden representar como un sistema probabilístico, donde cada posible estado tiene una probabilidad de existir. Un ejemplo de un sistema probabilístico es pensar que contamos con una máquina que lanza pelotas de béisbol, la cual está configurada para que pueda lanzar las pelotas a través de dos aberturas en una pared. Supongamos que tenemos 5 blancos de tiro detrás de la pared como vemos en la ilustración 1.



Gráfica 9 – Ejemplo de doble ranura

Ahora supongamos que lanzamos una pelota, como se mencionó anteriormente la pelota tiene una probabilidad de un 50 % de pasar por alguna de las dos ranuras. Cuando la pelota intenta pasar por las ranura supongamos que rebota en alguna de las paredes internas y cae en alguno de los targets, como vemos en la figura 2, podemos representar la probabilidad en cada uno de los puntos de los posibles estados donde estará la pelota, dado esto la pelota al pasar por alguno de estas ranuras podría caer en alguno de los 3 target al frente de él por lo que sería un 1/3 la probabilidad de caer en alguno, en los puntos 3,4,5,6 y 7 la probabilidad es 1, ya que es la probabilidad de llegar a ese mismo punto.



Gráfica 10 - Ejemplo doble ranura probabilístico

Para representar estas probabilidades se hace uso de una matriz (figura 3).

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

ecuación 55

Una vez hemos construido la matriz podemos generalizar las probabilidades para cualquier intento multiplicando la matriz por sí misma el número de intentos, es decir si queremos ver qué pasa luego de dos intentos (ecuación 55).

$$B^2 = B \star B$$

ecuación 56

$$B^2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{6} & \frac{1}{3} & 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{1}{6} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 \\ \frac{1}{6} & 0 & \frac{1}{3} & 0 & 0 & 0 & 1 & 0 \\ \frac{1}{6} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

ecuación 57

Ahora debemos determinar el estado inicial, para esto usamos una matriz de una sola dimensión, por ejemplo (ecuación 56)

$$X = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

ecuación 58

Luego de esto multiplicamos la matriz por el estado inicial.

$$B^2 \star X = \left[0, 0, 0, \frac{1}{6}, \frac{1}{6}, \frac{1}{3}, \frac{1}{6}, \frac{1}{6}\right]^T.$$

ecuación 59

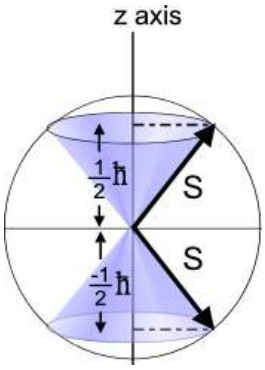
2.5 Estados

Ahora bien, así como observamos los posibles estados que puede tener una partícula observada en normalmente, en el mundo cuántico podemos tener múltiples estados al mismo tiempo, por lo cual para explicar un poco mejor esto nos remitimos a la paradoja de Schrödinger como se mencionó anteriormente, el cual busca tener una expresión matemática a la superposición de estados cuánticos $\{|0\rangle, |1\rangle, |0\rangle + |1\rangle\}$. Estos estados cuánticos describen los valores que puede tomar un sistema se pueden expresar en la esfera de Bloch y con números complejos, su tamaño depende de la cantidad de estos estados, matemáticamente se describen como un vector de estados $|\psi\rangle = [4 + 3i, 7{,}8 - i, 15 + 3i, 1{,}2 + 10i, 10]$, estos estados tienen una probabilidad de pasar de un valor a otro, o de estar en solo uno de estos estados, por lo anterior matemáticamente se expresa como la normal del estado al cuadrado, sobre la norma de todos los posibles estados.

$$p(x_i) = \frac{|x_i|^{\mathbf{2}}}{||\psi\rangle|}, x_i \in |\psi\rangle$$

ecuación 60

Gracias al Experimento de Stern y Gerlach donde lograron demostrar la deflexión de partículas o Spin, la cual consiste en que una partícula puede tener una carga positiva y negativa de la misma magnitud al mismo tiempo, esta es la base de la superposición de estados cuánticos.



Gráfica 11 - Spin

Matemáticamente es expresado como $|\psi\rangle = c_0|\downarrow\rangle + c_1|\uparrow\rangle$ donde el estado que me define la carga negativa ($|\downarrow\rangle$) tiene una magnitud expresada en números complejos (c_0) y al igual con la carga positiva ($|\uparrow\rangle$) tiene una magnitud definida como c_1 y por superposición de estos dos estados los sumamos. Esta magnitud o longitud se puede calcular $|\psi\rangle = \sqrt{{c_0}^2 + {c_1}^2}$ y al igual se puede calcular la probabilidad de ser un estado es especifico utilizando la magnitud de los estados de esta partícula $p(\uparrow) = \frac{c_1}{\text{longitud } |\psi\rangle}$.

ecuación 61

2.6 Observables

La mecánica cuántica describe el estado instantáneo de un sistema representado con estados cuánticos definidos con una distribución de probabilidad de todas las propiedades medibles u observables, Los observables se representan por Ω y se operan matemáticamente con matrices hermitiana, estos observables son:

- Energía
- Posición

- Momento o momentum
- Momento angular

Al tener una probabilidad, la mecánica cuántica no asigna valores definidos a los observables, por el contrario, lo hace prediciendo sobre sus distribuciones de probabilidad, por lo cual se representan con una operación hermitiana y como ya vimos anteriormente podemos realizar diferentes tipos de operaciones, como la suma, multiplicación, conmutarlas entre otras.

Por ejemplo, para la representación de la posición especifica en el sistema cuántico, está dada por la multiplicación del estado por la posición.

$$P(|\psi\rangle) = x_i|\psi\rangle$$

ecuación 62

$$P(|\psi\rangle) = P\left(\sum c_i|x_i\rangle\right) = \sum x_i c_i|x_i\rangle$$

ecuación 63

En otras palabras, P es simplemente la diagonal de una matriz donde x_i son las coordenadas. Por lo tanto, P es una matriz hermitiana, donde los valores propios son los valores de x_i.

$$P = \begin{bmatrix} x_0 & 0 & \dots & 0 \\ 0 & x_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x_{n-1} \end{bmatrix}$$

ecuación 64

Como ya sabemos el momentum, clásicamente está definido como el impulso que lleva una masa, para representarlo cuánticamente tenemos que hacer un modelo discreto, definido así:

$$M(|\psi\rangle) = -i * h * \frac{|\psi(x+\delta x)\rangle - |\psi(x)\rangle}{\delta x}$$

ecuación 65

En otras palabras, el momentum, es una constante $-i * h$ (h es una constante universal de la mecánica cuántica, es conocida como la contante de Planck) y el cambio de un punto a otro en los estados cuánticos (δx).

Como mencionamos anteriormente, los estados cuánticos pueden tener una dirección y giros, definidos como Spin. Para representar cada una de las tres posibles direcciones en las que podemos ubicar una partícula (Plano x, y, y z).

$$S_z = \frac{h}{2}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \quad S_y = \frac{h}{2}\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \quad S_x = \frac{h}{2}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

ecuación 66

Cada uno de los tres operadores de giro viene equipado con una base ortonormal, S_z, S_x tiene bases propias $\{|\leftarrow\rangle, |\rightarrow\rangle\}$, o izquierda y derecha, y S_y tiene $\{|\swarrow\rangle, |\nearrow\rangle\}$.

2.7 Medidas

Una actividad importante que se puede hacer sobre los estados observables es poder medirlos. Como ya sabemos a un observable solo podemos asumirle un valor propio como el resultado de la observación, y, si definimos también un tiempo con el que vamos a tomar una medición, cuando hacemos este proceso y obtenemos un valor propio del observable es llamado λ. En otras palabras, sea **Ω** un observable y $|\psi\rangle$ un estado, si el resultado de medir **Ω** es el valor propio λ, el estado después de la medición siempre será un vector propio de λ, estos muy importante ya que, si conocemos con certeza que valor tenemos, es posible predecir su comportamiento y algo que se debe tener en cuenta es que cuando medimos

varios observables, el orden de las medidas importa.

2.8 Dinámica y ensamblaje de sistemas cuánticos

Algo sumamente importante es la posibilidad de trabajar con sistemas cuánticos que involucran a más de una partícula que son independientes entre sí, la formulación matemática sería el producto cruz entre los sistemas:

$$\mathbb{v}_0 \otimes \mathbb{v}_1 \otimes \ldots \otimes \mathbb{v}_k$$

ecuación 67

Ahora vamos a generalizar el conjunto de estados de la siguiente manera.

$$|\psi\rangle = C_{0,0}|x_0\rangle \otimes |y_0\rangle + \cdots + C_{i,l}|x_i\rangle \otimes |y_l\rangle + \ldots + C_{n-1,m-1}|x_{n-1}\rangle \otimes |y_{m-1}\rangle$$

ecuación 68

Donde $C_{i,l}$ es la amplitud en x_i y a y_l como lo hemos venido representando en ejemplos pasados.

La probabilidad de encontrar la partícula en x_i y y_l, es igual que cuando trabajamos con un solo sistemas, por lo cual está dada por:

$$\mathrm{p}(x_i, y_l) = \frac{\left|C_{i,l}\right|^2}{||\psi\rangle|}$$

ecuación 69

3 Computación

3.1 Qubit

Es un objeto matemático, con unas ciertas propiedades:

La primera propiedad es que Puede representar diferentes estados.

Al igual que el bit tiene estados de 0 y 1, que se representan como $|0\rangle\, y\, |1\rangle$ estos son llamados estados base. A diferencia de los bits, los Qubits tienen otros estados que se representan como una combinación lineal de los estados bases.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

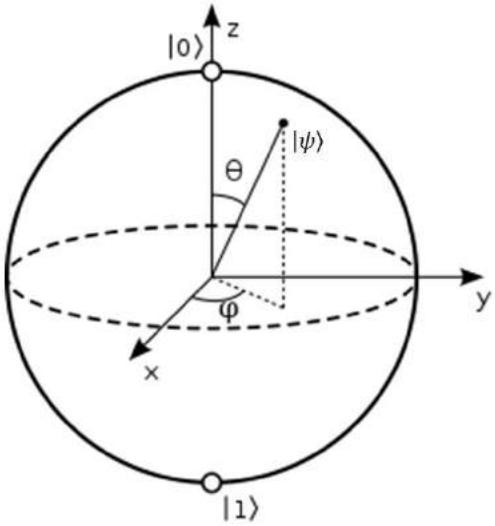
ecuación 70

Donde $\alpha\, y\, \beta$ son números completos y se dice que el Qubit está en superposición de sus estados base. La segunda propiedad es que al medir el valor del estado actual del Qubit siempre se obtiene $|0\rangle\, o\, |1\rangle$, $|0\rangle$ con una probabilidad de $|\alpha|^2$ y $|1\rangle$ con una probabilidad de $|\beta|^2$, Es decir la mitad de las ocasiones que se mida su valor será $|0\rangle$ y la otra mitad de las ocasiones será $|1\rangle$, esto se debe a que los estados están normalizados por lo tanto:

$$|\alpha|^2 + |\beta|^2 = 1$$

ecuación 71

Existe una herramienta matemática que nos ayuda a la representación de los estados del Qubit, llamada la esfera de Bloch esta es una esfera unitaria que está en el plano de los números complejos, donde el $|0\rangle$ está representado por el eje Z y el estado $|1\rangle$ está representado por el eje $-Z$



Gráfica 12 - Esfera de Bloch

La ecuación del estado de Qubit se puede escribir usando la siguiente ecuación:

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

ecuación 72

3.2 Multiples Qubit

Existen dos grandes operaciones que se pueden hacer con múltiples Qubits. La primera es la superposición y esta se representa como la suma de los estados bases con su respectiva probabilidad.

$$|S\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

ecuación 73

Para un sistema con 2 Qubits obtenemos cuatro estados bases $|00\rangle$,$|01\rangle$, $|10\rangle$ y $|11\rangle$. y α_0, α_1, α_2 y α_3 son números complejos y la suma de sus probabilidades siempre es 1. La superposición se representa así:

$$|S\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

ecuación 74

Para un sistema de N Qubits tenemos.

$$|S\rangle = \alpha_0|x_0\rangle + \alpha_1|x_1\rangle + \cdots + \alpha_{N-1}|x_{N-1}\rangle$$

ecuación 75

Matemáticamente la probabilidad para cada uno de los estados del sistema es $\left|\frac{1}{\sqrt{N}}\right|^2$, donde n es número de estado base del sistema y esto se conoce como **superposición uniforme.**

La segunda es el **entrelazamiento** se presenta en un sistema con múltiples Qubits, donde dos o más de sus Qubits poseen una alta correlación sin importar la distancia que exista entre ellos. Es decir, no se pueden medir estados individualmente, por lo que es necesario medirlo en conjunto.

Por ejemplo, teniendo los estados base para dos Qubits $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$ se pueden describir de forma individual por lo que no hay entrelazamiento. Otro ejemplo donde no hay entrelazamiento es si tenemos un sistema que está en estado $\frac{(|00\rangle + |01\rangle)}{\sqrt{2}}$ se puede describir dado que el primer Qubit siempre está en estado $|0\rangle$ y el segundo Qubit en estados $|0\rangle + |1\rangle$, por lo que no importa el estado del segundo Qubit será un estado valido del sistema.

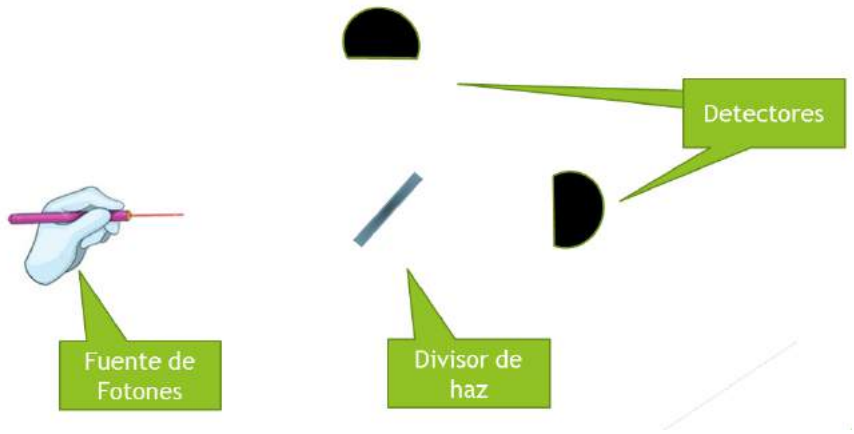
Por otro lado, si tenemos un sistema que está en estado $\frac{(|10\rangle + |01\rangle)}{\sqrt{2}}$ se dice que están entrelazados, dado que, no se puede expresar como una lista de estados individuales ya que el estado del segundo Qubit depende del estado directamente del primer Qubit y viceversa. Es decir, si el primer Qubit este estado $|1\rangle$ el estado del segundo Qubit deberá ser $|0\rangle$ para

generar un estado valido del sistema.

3.3 Implementación de un Qubit

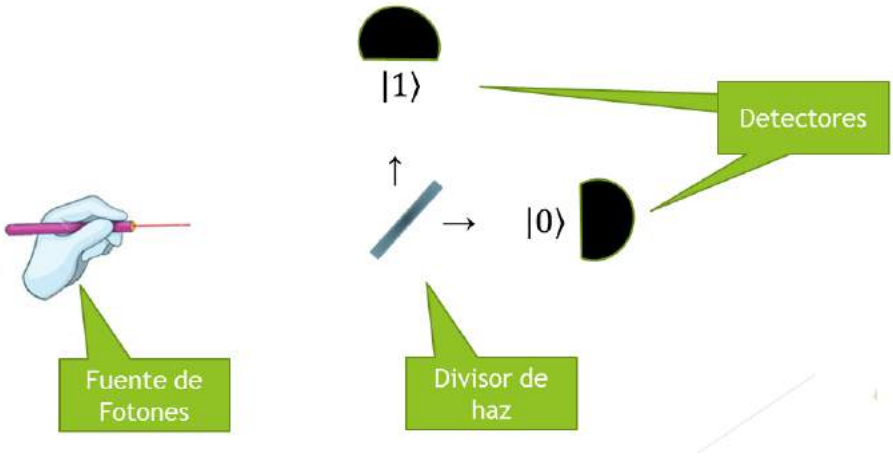
No existe una única forma de implementar un Qubit de hecho existe una implementación de Qubits que utiliza una fuente de fotones que lanza un solo fotón a la vez, divisores de haz, espejos, un panel oscuro y unos medidores de fotones.

Primero vamos a ubicar la fuente de fotones, el divisor de haz y los medidores con la siguiente configuración.



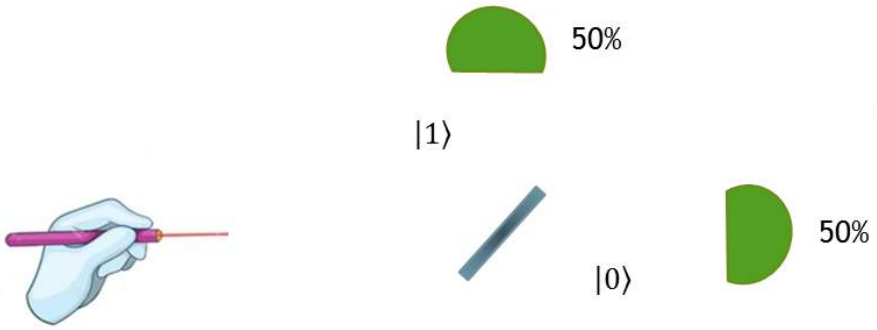
Gráfica 13

Vamos a decir que si el fotón va en dirección horizontal este tendrá un estado $|0\rangle$, si el foton va en dirección vertical este tendrá $|1\rangle$.



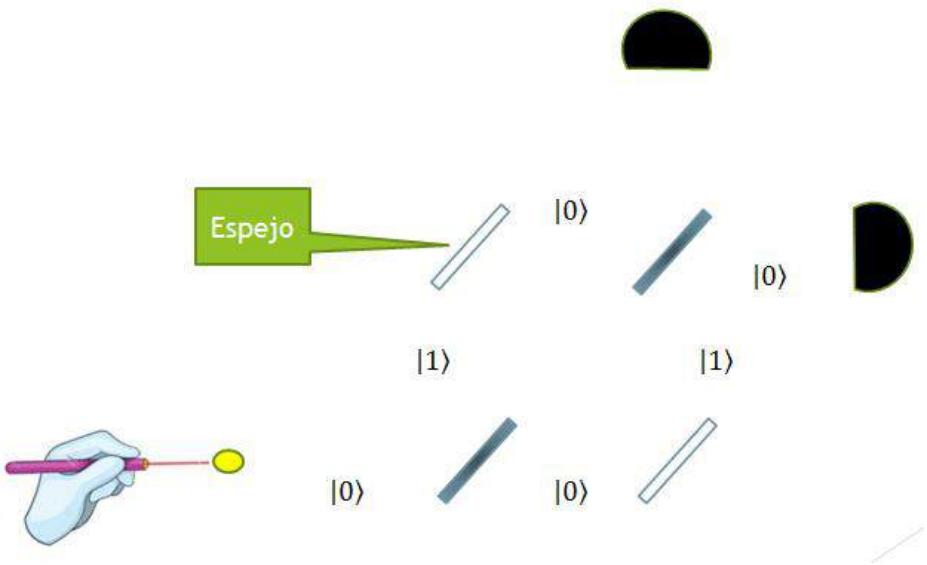
Gráfica 14

Cuando lanzamos un fotón vemos que hay un 50% de probabilidades de que el divisor de haz cambie el fotón de estado y sea detectado por uno de los dos sensores.



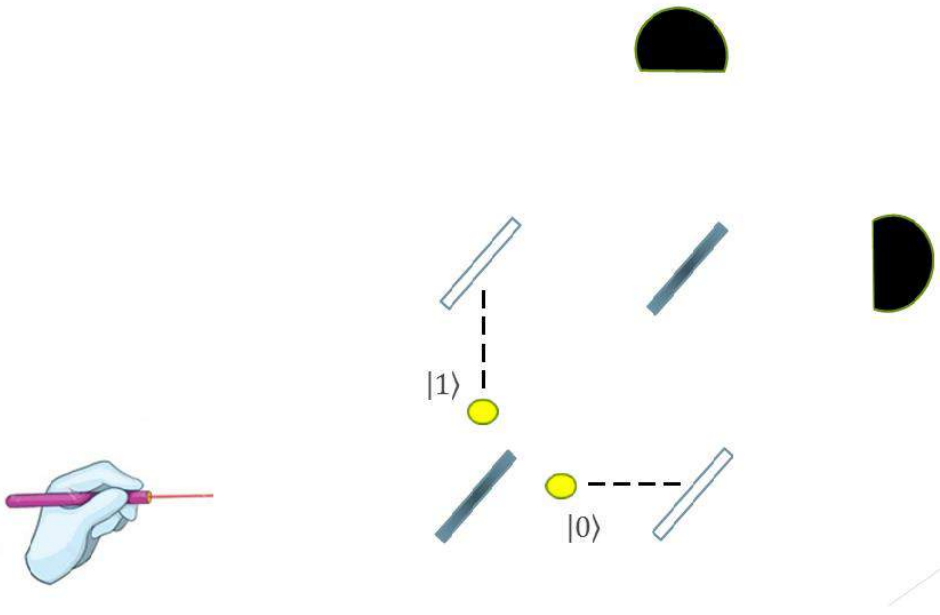
Gráfica 15

Es decir, el sistema está en superposición uniforme de sus estados base, bien ahora modificamos el experimento agregando otro haz de luz y par de espejos, iniciamos con un estado cero y luego tenemos todas las posibles combinaciones que se pueden generar.



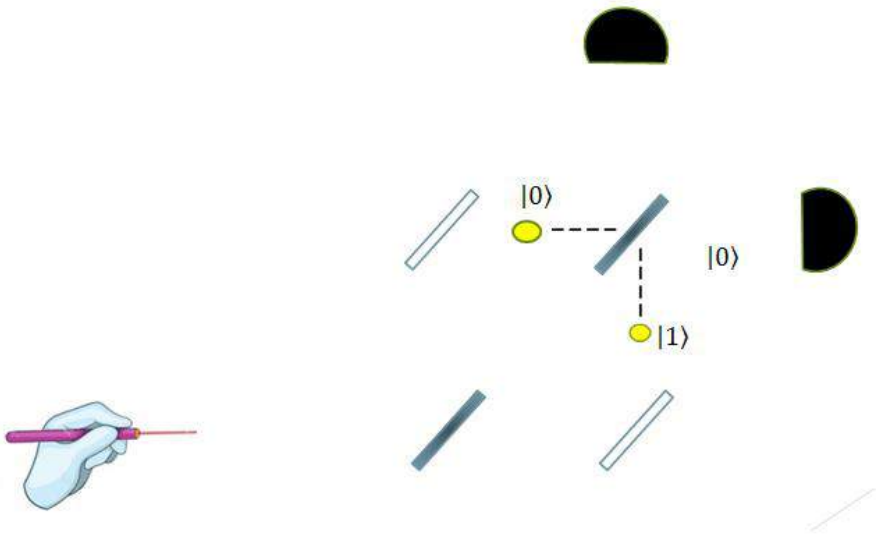
Gráfica 16

Cuando lanzamos un fotón por defecto está en estado cero, luego por la acción del divisor de haz este tiene 50% de probabilidades para el estado |0⟩ y 50% para el estado |1⟩.



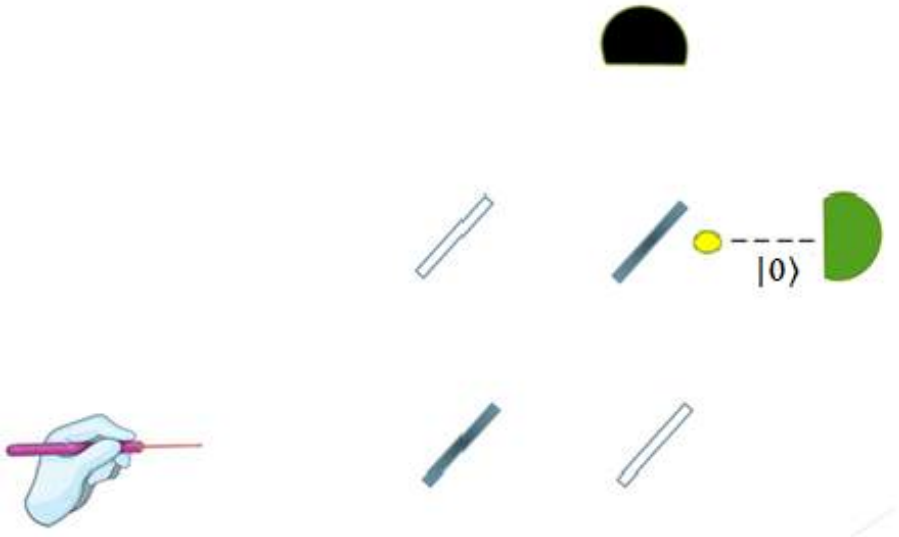
Gráfica 17

Luego el fotón rebotara en el espejo



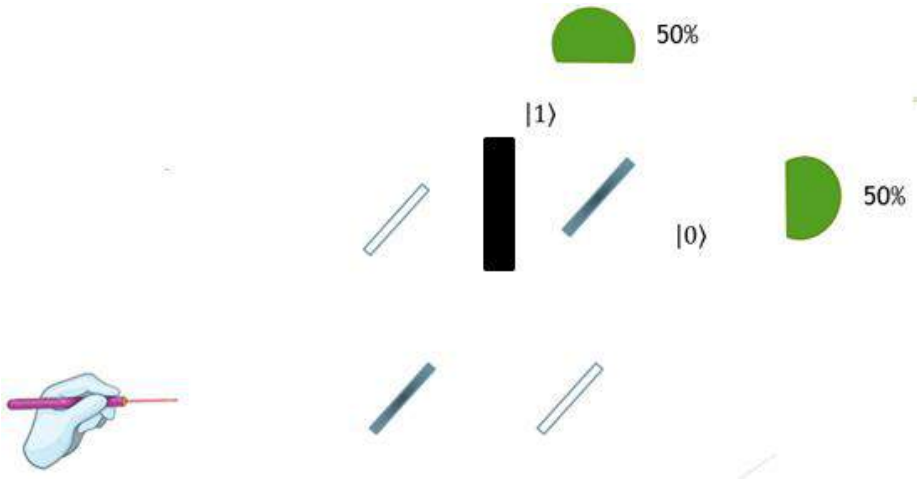
Gráfica 18

En este momento sucede un fenómeno muy extraño, sin importar el número de fotones y el lapso de tiempo es que se lance el fotón este siempre termina en estado $|0\rangle$, este fenómeno es llamado interferencia cuántica.



Gráfica 19

Ahora si modificamos de nuevo el experimento y añadimos un panel oscuro, volvemos al sistema donde existe 50% de probabilidades para el estado $|0\rangle$ y 50% para el estado $|1\rangle$.

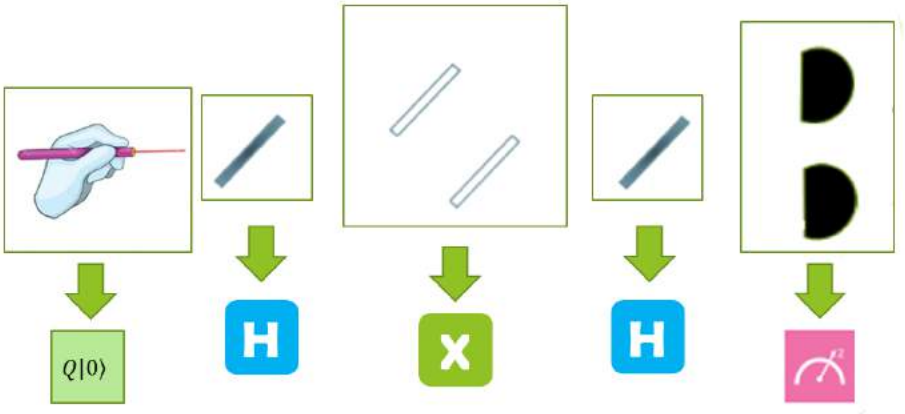


Gráfica 20

Ahora vamos a volver a la configuración sin el panel oscuro, pero por motivos de visibilidad vamos cambiar la posición de los elementos sin modificar su funcionalidad, de la siguiente manera.

Gráfica 21

De esta manera hemos construido un circuito cuántico donde $Q|0\rangle$ Es el Qubit en estado cero y es representado por la fuente de fotones, H y X son compuertas lógicas cuánticas y son representadas por los divisores de haz y los espejos respectivamente y por último los sensores son los medidores.



Gráfica 22

Otro tipo de implementación es el que tiene IBM, ellos usan fuertes campos magnéticos de un láser óptico para atrapar iones en el espacio. Estas trampas evitan que los iones interactúen con el medio ambiente, en este se eligen un par de estados de energía en el ion para que actúen como los estados bases del Qubit $|0\rangle$ y $|1\rangle$. El par de estados se seleccionan para tener una baja coherencia, es decir, una baja tasa de pasar de un estado de energía más bajo, pata las compuertas lógicas cuánticas se hacen con impulsos laser que provocan cambios en el estado de los iones, es importante mencionar que el sistema debe tener una temperatura extremadamente baja para evitar que se mezclen los Qubits.

3.4 Compuertas lógicas cuánticas

Lo más interesante que se puede hacer con un solo bit clásico es la negación de este, en computación cuántica existe un equivalente para los Qubits llamado NOT esta se puede representar por medio de una matriz que modifica los estados del Qubit,

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

$$Compuerta\ NOT = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$$

$$Compuerta\ NOT\ |0\rangle = |1\rangle$$

$$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$$

ecuación 76

$$Compuerta\ NOT\ |1\rangle = |0\rangle$$

$$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$$

ecuación 77

Cuando en NOT es aplicado a un estado que no base, se intercambian los números complejos que los acompañan, es decir se intercambian las probabilidades.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

ecuación 78

$$NOT|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$$

ecuación 79

Al poder representar modificaciones de estados por medio de matrices se pueden obtener infinidad de modificaciones a los estados cuánticos, estas matrices deben ser unitarias y cumplir la siguiente propiedad:

$$(U * U^{\dagger} = I),$$

ecuación 80

Las compuertas cuánticas logias se pueden ver o representar como movimientos en la esfera de Bloch.

Algunos ejemplos son:

Compuerta de Hadamard opera sobre un Qubit, representa una rotación sobre los ejes x y z.

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

ecuación 81

Compuerta de desplazamiento de fase opera sobre un qubit, es como trazar una circunferencia horizontal sobre la esfera de Bloch de θ radianes.

$$R(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

ecuación 82

Compuerta SWAP opera sobre dos qubits, intercambia los dos qubits.

$$\text{SWAP}=\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

ecuación 83

Compuerta NOT controlada, trabaja sobre dos qubits y realiza la operación NOT en el segundo qubit solo cuando el primer qubit es $|1\rangle$, en otro caso lo deja intacto.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

ecuación 84

U, opera en un único qubit usada en U-Controlada.

$$U = \begin{bmatrix} W & X \\ Y & Z \end{bmatrix}$$

ecuación 85

U-Controlada Opera sobre dos qubits de manera que el primer qubit actúa como controlador.

$$C(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & w & x \\ 0 & 0 & y & z \end{bmatrix}$$

ecuación 86

Las compuertas cuánticas poseen la propiedad de ser compuertas reversibles, esta es una propiedad que me permite obtener el estado antes de aplicar una compuerta, por ejemplo, el NOT es una compuerta que es reversible, mientras que en AND o el OR no lo son. Se dice que una compuerta es reversible si al hacer el mapeo de posibles antiguos estados contra los nuevos es una función uno a uno.

4 Algoritmos cuánticos

4.1 Algoritmo de Grover

4.1.1 Introducción

El algoritmo de Grover es uno de los principales algoritmos de la computación cuántica y es uno de los más básico, el cual explota al máximo el principio fundamental de superposición, mostrando la superioridad de las computadoras cuánticas sobre las clásicas. Este algoritmo se conoce por su poder de búsqueda sobre un conjunto de datos no estructurados, es decir imaginemos que tenemos un conjunto con N datos de estudiantes, pero necesitamos encontrar uno en específico el cual para este algoritmo lo llamaremos target (w), si realizamos la acción de búsqueda sobre estos N estudiantes, con un algoritmo clásico debería mínimo buscarlo en $N/2$ operaciones. En un sistema cuántico dada la superposición de estados, este problema se puede resolver examinando simultáneamente todas las posibles combinaciones. Como resultado, el número de pasos para encontrar el nombre del estudiante que deseamos se puede obtener en solo O ($\sqrt{N}$) pasos.

4.1.2 Como funciona

Una de las cosas muy importantes en un computador cuántico es saber la forma en la que se ingresan elementos de la lista, para la implementación de este algoritmo se establece una función f la cual tiene como objetivo marcar el estado como $f(x) = 0$ si el elemento que estamos buscando no es w (target) y si cambiamos por el estado marcado, entonces, $f(w) = 1$ es el marcado, al decodificar la función en una matriz unitaria esta se llamara el oráculo U_f. Una vez establecido el comportamiento de la función, si la observamos a

manera de qubits obtenemos que $f:\{0,1\}^n \rightarrow \{0,1\}$ dado que $N = 2^n$ por el número de qubit que necesitamos para la representación del numero N.

$$f(x) = \begin{cases} 1 & x = x_0 \\ 0 & x \neq x_0 \end{cases}$$ El objetivo de la función es hallar x_0

ecuación 87

Para definir la matriz U_f (oráculo) tenemos que tener en cuenta que esta debe actuar sobre todos los estados $|x\rangle$, esta matriz está definida de la siguiente manera:

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

ecuación 88

Como podemos observar en la función anterior si es un estado x el cual no es el marcado, no tendrá efecto sobre el estado $|x\rangle$, ahora bien, si $U_f|w\rangle = (-1)^{f(w)}|w\rangle$ el resultado será $U_f|w\rangle = -|w\rangle$. Geométricamente, la matriz unitaria corresponde a hacer una reflexión en su amplitud al estado marcado dentro del conjunto de N elementos.

Con la función anterior podemos marcar el estado que deseamos buscar, y este, nos modifica la amplitud del estado para que "resalte" sobre los demás estados. Como lo mencionamos anteriormente este algoritmo funciona utilizando la superposición, dado que, en sí, no conocemos donde está el articulo marcado dentro del conjunto de N elementos. Por lo tanto, utilizamos la definición matemática de la superposición uniforme aplicada a los estados cuánticos.

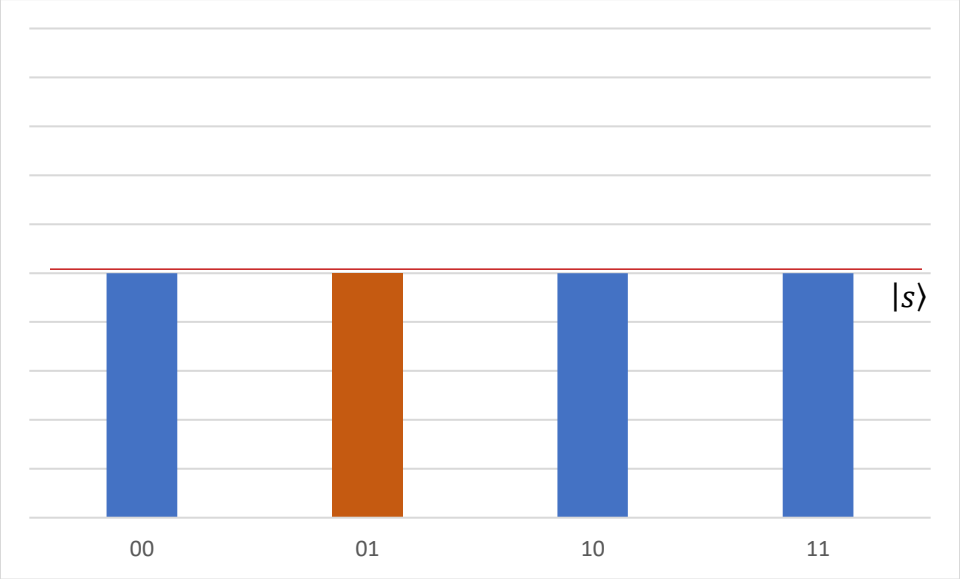
$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

ecuación 89

Esta superposición permite que, por medio del procedimiento anterior de amplificación de amplitud, que es como el computador cuántico aumento significativamente esta

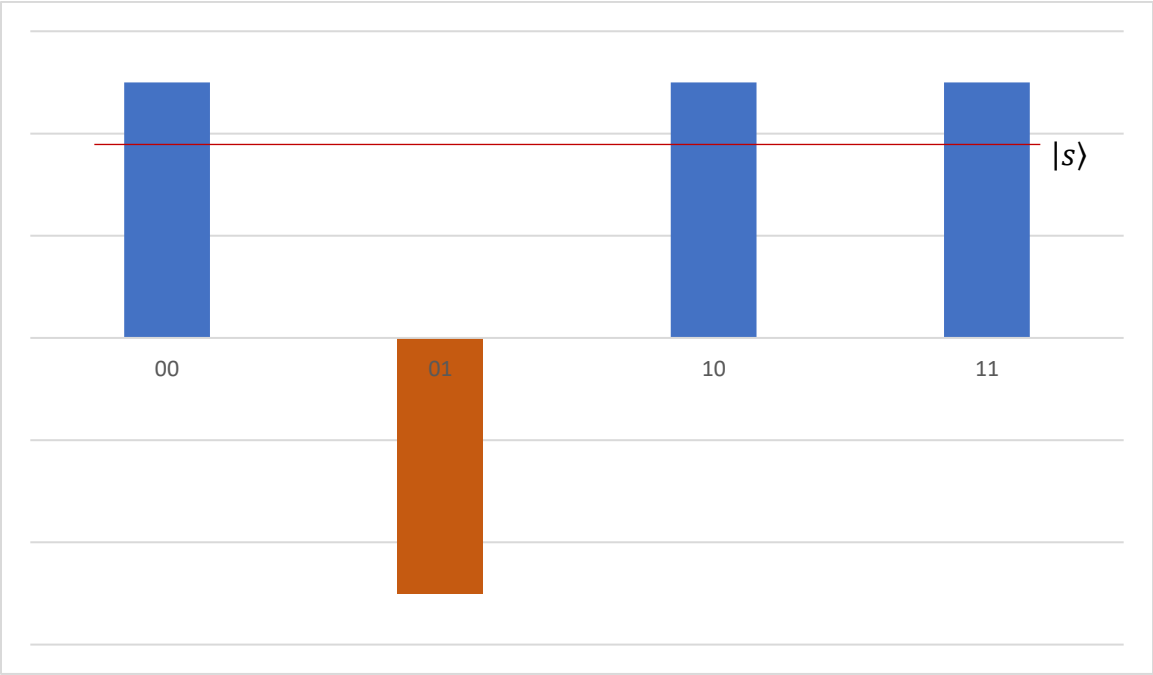
probabilidad. Este procedimiento cuando amplifica la amplitud del elemento marcado reduce la amplitud de los otros elementos, por lo que la medición en el estado final devolverá al elemento correcto casi con certeza y con una probabilidad casi de 100% del estado marcado.

Este algoritmo trabaja en 3 pasos, el primero de estos es la inicialización de las amplitudes de los estados, las cuales corresponden al hacer superposición $|s\rangle$, esta superposición se expresa por medio de compuertas cuánticas como $|s\rangle = H^{\otimes n}|0\rangle^{n}$. Por lo tanto, en el instante $t = 0$ es $|\psi_t\rangle = |s\rangle$.



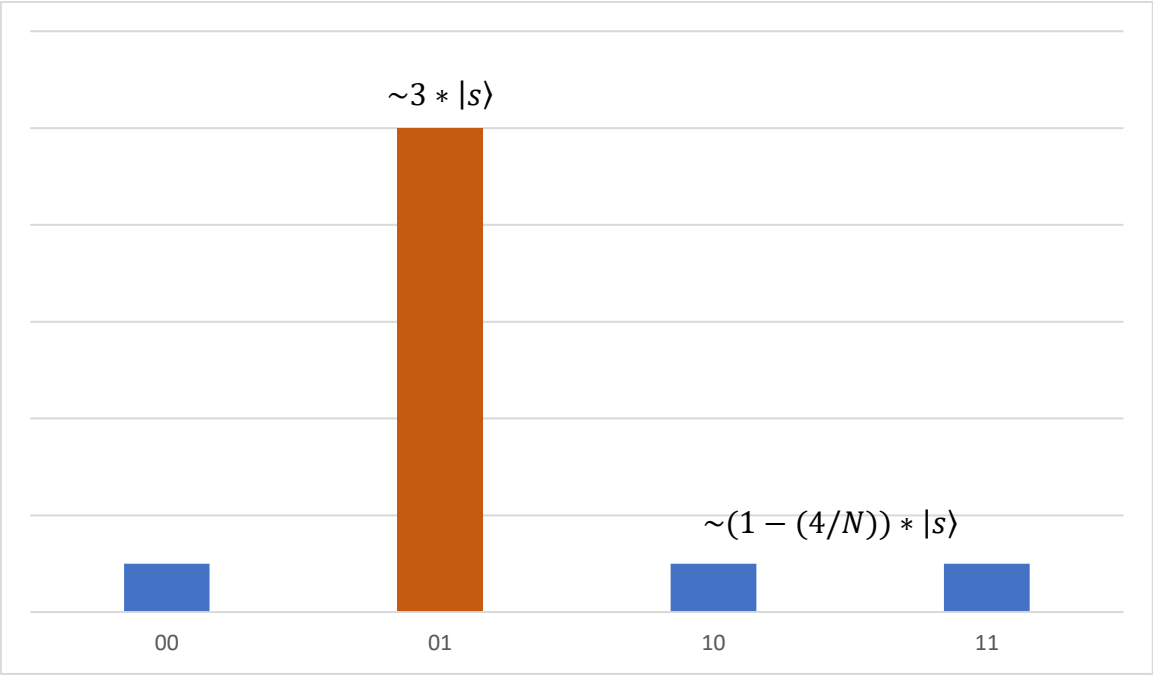
Gráfica 23 - Amplitudes iniciales paso 1 Grover

En el segundo paso, se aplica la reflexión U_f a todos los estados $U_f|\psi_t\rangle = |\psi_{t'}\rangle$, donde como vimos anteriormente si $|\psi_t\rangle$ es el estado $|w\rangle$ este, geométricamente se puede representar como la reflexión negativa $-|w\rangle$ y si son estados no marcados $|x\rangle$ la función no tiene ningún efecto.



Gráfica 24 - Amplitudes trasformación Uf paso 2

Y por último el tercer paso, aplicamos una reflexión en el estado $|s\rangle$, la cual se escribe como $U_s = 2|s\rangle\langle s| - 1$. Esta trasformación modifica todos los estados a $U_s|\psi_{t'}\rangle$ y completa la transformación $|\psi_{t+1}\rangle = U_s U_f |\psi_{t'}\rangle$.



Gráfica 25 - Amplitudes trasformación U_s paso 3

Matemáticamente U_s se puede representar como la multiplicación de las matrices:

$$U_s = 2\begin{bmatrix} 1/\sqrt{N} \\ \vdots \\ 1/\sqrt{N} \end{bmatrix}\begin{bmatrix} 1/\sqrt{N} & \cdots & 1/\sqrt{N} \end{bmatrix} - I = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{bmatrix}$$

ecuación 90

Por lo tanto, resumiendo un poco por medio de sumatorias.

$$U_s|\psi_t\rangle = (2|s\rangle\langle s| - 1)|\psi_t\rangle$$

$$U_s|\psi_t\rangle = \left(2\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\right)\left(\frac{1}{\sqrt{N}}\sum_{x'=0}^{N-1}\langle x'|\right) - 1\right)\sum_{x''=0}^{N-1}\alpha_{x''}|x''\rangle$$

$$U_s|\psi_t\rangle = \left(\frac{2}{N}\sum_{x=0,x'=0,x''=0}^{N-1}\alpha_x{}''|x\rangle\langle x'|x''\rangle - \sum_{x=0}^{N-1}\alpha_x|x\rangle\right)$$

$$U_s|\psi_t\rangle = \left(\frac{2}{N}\sum_{x''=0}^{N-1}\alpha_x{}''\sum_{x=0}^{N-1}|x\rangle - \sum_{x=0}^{N-1}\alpha_x|x\rangle\right)$$

$$U_s|\psi_t\rangle = \sum_{x=0}^{N-1}\left(2\sum_{x''=0}^{N-1}\frac{\alpha_x{}''}{N} - \alpha_x\right)|x\rangle$$

$$U_s|\psi_t\rangle = \sum_{x=0}^{N-1}(2A - \alpha_x)\,|x\rangle$$

ecuación 91

Donde A es el promedio de cada α_x, $A = \sum_{x''=0}^{N-1}\frac{\alpha_x{}''}{N}$, Después de algunas reducciones por las sumatorias y el promedio, para el estado $|\psi_{t+1}\rangle = U_s U_f|\psi_{t\prime}\rangle$.

$$|\psi_{t+1}\rangle = \left[\frac{2^{n+1}+2^n-4}{2^n\sqrt{2^n}}\right]|x\rangle \quad \text{Para } x = \omega$$

ecuación 92

$$|\psi_{t+1}\rangle = \left[\frac{2^{n+1}-2^n-4}{2^n\sqrt{2^n}}\right]|x\rangle \quad \text{Para } x \neq \omega$$

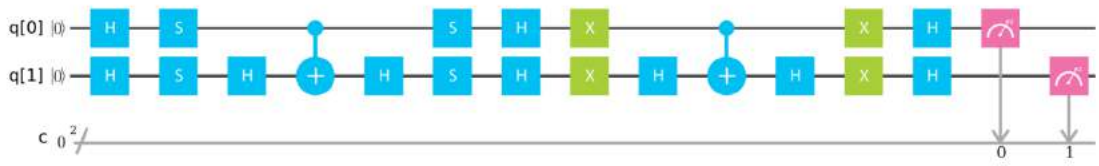
ecuación 93

Al implementar el algoritmo en un computador cuántico esté repite los 3 pasos, y se obtiene una respuesta más acertada, con estas dos reflexiones U_s, U_f obtenemos una rotación y una amplificación de la amplitud, geométricamente es una ampliación sobre el promedio de las amplitudes, como lo vemos en el paso 2 donde en la gráfica el valor de $|s\rangle$ es menor a las

amplitudes de los estados no marcados, ya que el estado marcado (Estado 2) es negativo. Y por último en el paso 3 al volver hacer una reflexión este valor negativo es convertido en positivo.

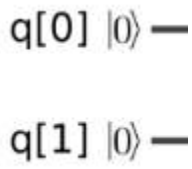
4.1.3 Implementación en la máquina de IBM

El compositor de IBM es donde se implementan los algoritmos cuánticos dadas las compuertas cuánticas, en pocas palabras es un lenguaje ensamblador cuántico.



Gráfica 26 - Búsqueda N=2 algoritmo de Grover

Para programar este algoritmo se deben tener en cuenta los 3 pasos anteriormente mencionados, para comenzar como podemos observar en el algoritmo brindado por IBM en su ejemplo todos los Qubits inicializan con un valor de 0.

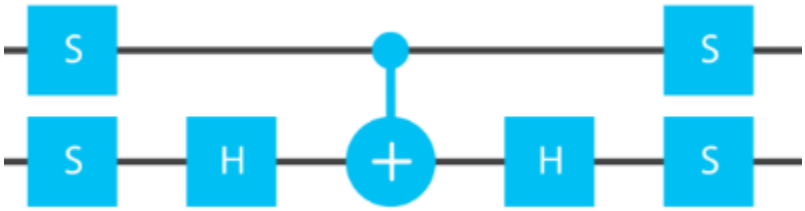


Gráfica 27 - Qubits en ceros algoritmo de Grover

Como vimos anteriormente en los pasos de implementación del algoritmo el primer paso es establecer todos los Qubits en superposición $|s\rangle = H^{\otimes n}|0\rangle^{n}$, en el compositor se representa con la compuerta H o de Hadamard.

Gráfica 28 - Establecer superposición en los Qubits algoritmo de Grover

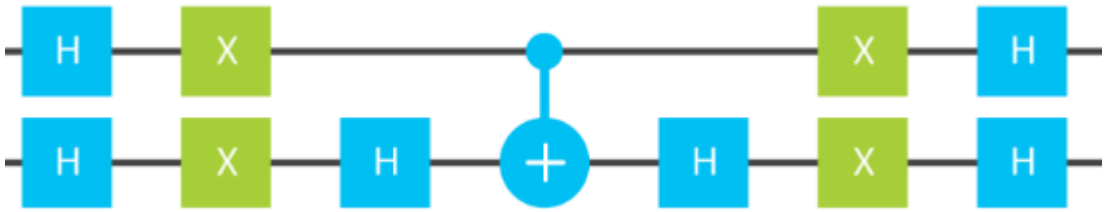
Ahora bien, para implementar la función U_f anteriormente mencionada en el paso 2 para hacer el marcado de nuestro target se implemente una compuerta CNOT, en conjunto con una compuerta S o SWAP con la cual esencialmente es con la que se marca el objetivo de busqueda dado la cantidad de Qubits.



Gráfica 29 - Marcación U_f algoritmo de Grover

Las ultimas compuertas H y S, se ultilizan para volver a su estado original el Qubit modificado con el fin de garantizar una buena medicion.

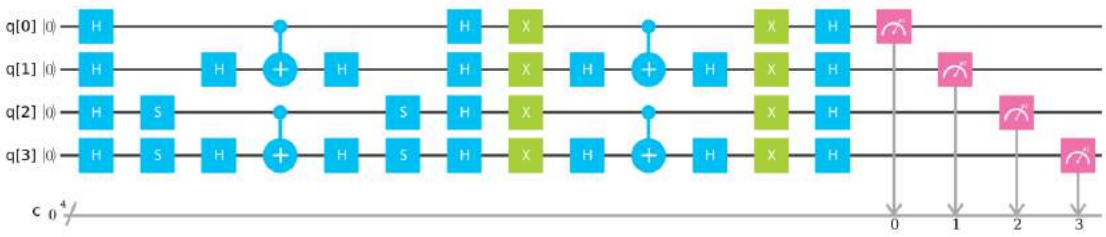
Para realizar el paso 3 se introduce la compuerta X, que si lo vemos desde la computacion clasica se puede traducion como una compuerta negadora o NOT.



Gráfica 30 - Paso 3 matriz U_s algoritmo de Grover

Como se mencionó anteriormente el paso 3 es una matriz aplicada a todos los Qubits, haciendo una negación de los estados, por lo tanto, el estado que está marcado y se traduce a una probabilidad menor, con este cambio de estado, su probabilidad será positiva, mientras que la probabilidad de los estados positivos tendrán una probabilidad negativa y por lo que sabemos en matemática no existen probabilidades negativas por lo tanto se traducen en cero.

Para la implantación de este algoritmo en 4 Qubits ampliando así la capacidad de búsqueda, se puede utilizar dos veces la implementación anterior, la cual una implementación buscara en los 2 primeros Qubits y la siguiente implementación buscara en los Qubits de mayor precedencia.

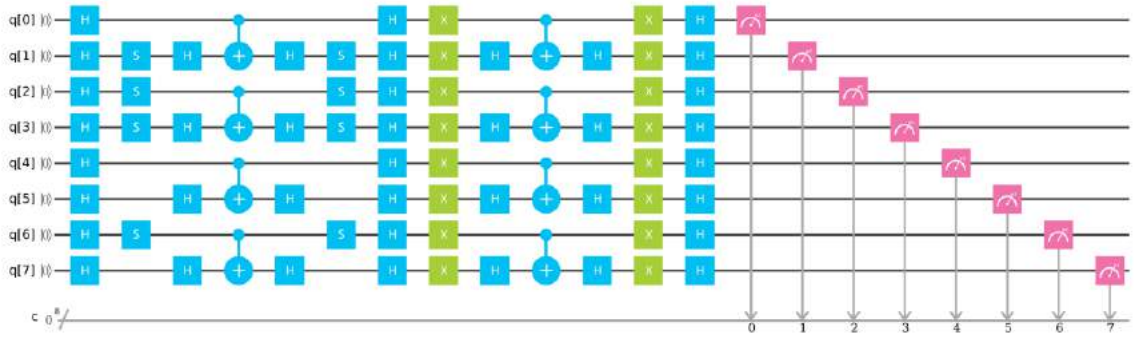


Gráfica 31 - Implementación algoritmo de Grover N=4

Como podemos ver una primera implementación buscara en los Qubits de menor precedencia (0 y 1), y la segunda implementación en los otros Qubits (3 y 4). Por lo cual si

lo vemos todo como un conjunto se pueden obtener búsquedas de 3 Qubits también donde el Qubit 3 siempre tomara un valor de 0.

En ese orden de ideas donde una implementación de búsqueda en 2 Qubits se puede implementar búsquedas en 8 Qubits, y así sucesivamente, por lo cual se pueden establecer búsquedas para N elementos implantados en la máquina de IBM.



Gráfica 32 - Implementación algoritmo de Grover N=8

4.2 Algoritmo de Shor

4.2.1 Introducción

Aunque cualquier número entero tiene una descomposición única en un producto de primos, encontrar los factores primos se cree que es un problema no tratable, en 1995 cuando Peter Shor propuso un algoritmo cuántico de tiempo polinomial para el problema de factorización.

El problema de la factorización consiste en expresar un número N en forma de producto

$$N = A * B$$

ecuación 94

Esta descomposición en factores de un número N se logra en tiempo O ((log N)3) y espacio O (log N), usando los algoritmos actuales se pueden demorar meses o incluso años en la descomposición en factores dependiendo de la cantidad de dígitos que compongan al número, mientras que el algoritmo de Shor lo resuelve en minutos o horas.

Muchas Criptografías de clave pública, tales como RSA, llegarían a ser obsoletas si el algoritmo de Shor es implementado alguna vez en una computadora cuántica práctica.

4.2.2 Como funciona

Lo que pretende este algoritmo es encontrar X, donde X es un factor propio de N, es decir

$$N\ mod\ X = 0$$

ecuación 95

En 1970 los matemáticos descubrieron que si encontraban un periodo de la función modular exponencial podrían resolver de manera más fácil el problema de la factorización, la función modular exponencial consiste en tener dos números enteros N y A, y encontrar un r, donde es el entero positivo más pequeño tal que $a^r - 1$es múltiplo de N, el numero r es llamado periodo del A modulo N:

$$(\downarrow r | 1 < r < N : (a^r - 1)\ mod\ N = 0)$$

ecuación 96

Escrito de otra manera

$$(\downarrow r | 1 < r < N : a^r mod\ N = 1)$$

ecuación 97

Recuerde que el operador mod es residuo de la división entera.

Vamos a tomar el ejemplo donde A=7, N=15

Tabla 1 – Ejemplo periodo algoritmo de Shor

A	N	r	$a^r mod\ N$
7	15	2	4
7	15	3	13
7	15	4	1

Para este caso el periodo es 4.

Ahora vamos a explicar el proceso desde la búsqueda del periodo hasta la factorización, para casos de simplicidad vamos a suponer:

Se conoce el periodo del A modulo N. N tiene solo dos factores primos y que estos son diferentes entre sí.

$$N = P_1 * P_2$$

ecuación 98

$$a^r - 1 = (\ a^{r/2} - 1)(a^{r/2} + 1)$$

ecuación 99

$$(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$$

ecuación 100

$$= \ll Multiplicación\ de\ polinomios \gg$$

$$a^r + a^{r/2} - a^{\frac{r}{2}} - 1$$

ecuación 101

$$= \ll Suma\ de\ polinomios \gg$$

$$a^r - 1$$

ecuación 102

Como primer paso vamos a calcular el valor A, este valor será un número aleatorio entre 2 y N-1, calcule el mcd (máximo común divisor) entre (N, A), si N y A comparten factores primos existe la posibilidad de que alguno de estos factores sea $P_1 \, O \, P_2$, con lo cual concluiríamos el proceso.

Ahora supongamos que N y A son coprimos (el máximo común divisor entre estos números es 1) y halle el periodo, como lo podemos ver en la tabla, Podemos observar que en su mayoría todos tiene periodo par.

Tabla 2 - Encontrando el periodo de un número

A	r
2	4
4	2
7	4
8	4
11	2
13	4
14	2

Usando la identidad $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$, podemos concluir que ni el multiplicando($a^{r/2} - 1$), ni el multiplicador ($a^{r/2} + 1$) es múltiplo de N pero el producto entre ellos sí , esto solo es posible por que P_1 es un factor primo de ($a^{r/2} - 1$) y P_2 es un

factor primo de ($a^{r/2}+1$) (o viceversa), por lo cual nosotros podemos encontrar P_1, P_2 computando el máximo común divisor de ($a^{r/2}-1$) y ($a^{r/2}+1$), como lo podemos ver a continuación.

Tabla 3 - Encontrando los números algoritmo de Shor

A	**r**	**MCD($a^{r/2}-1$)**	**MCD($a^{r/2}+1$)**
2	4	3	5
4	2	3	5
7	4	3	5
8	4	3	5
11	2	5	3
13	4	3	5
14	2	1	15

Ahora que conocemos el procedimiento general vamos a definirlo en un procedimiento.

Paso 1: Elegir un numero aleatorio entre 2 y $N-1$, al que llamaremos a

Paso 2: Si $mcd(a, N)$ es diferente de 1 es de decir no son coprimos, volver al primer paso

Paso 3: Determinar r o periodo de N donde r es el mínimo número tal que:

$$a^r mod\ N = 1$$

Paso 4: Si r es impar volver al primer paso

Paso 5: Si $mcd(a^{r}/_2 + 1,\ N)$ y $mcd(a^{r}/_2 - 1,\ N)$ es diferente de N, devolver estos valores.

Ejemplo vamos a factorizar 77

Paso 1: Elegir un numero aleatorio entre 2 y 76, para ejemplo a=3

Paso 2: $mcd(3,\ 77) = 1$, podemos seguir al paso 3

Paso 3: $3^{30} mod\ N = 1$

Paso 4: como el periodo es par podemos seguir al paso 5.

Paso 5: $mcd(3^{15} + 1,\ N) = 7$, $mcd(3^{15} - 1,\ N) = 11$

Lo más costoso en este algoritmo es el paso 3 donde se determina el periodo, Peter Shor ideo una solución basado en la utilización de un computador cuántico gracias a la superposición.

Paso 1: Elegir un numero aleatorio entre 2 y $N-1$, al que llamaremos a.

Paso 2: Si $mcd\,(a, N)$ es diferente de 1 es de decir no son coprimos, volver al primer paso

Paso 3: Comience con un par de registros Qubits de entrada y salida con $log2N$ qubits cada uno, e inicialícelos a

$$N^{-\frac{1}{2}} \sum_{0}^{N-1} |x\rangle|0\rangle$$

ecuación 103

Paso 4: Construya $f(x) = a^x mod\, N$ como función cuántica y aplíquela al estado antedicho, para obtener

$$N^{-\frac{1}{2}} \sum_{0}^{N-1} |x\rangle |f(x)\rangle$$

ecuación 104

Paso 5: Aplique la transformada cuántica de Fourier $(UQFT)$ al registro de entrada.

$$U_{QFT}|x\rangle = N^{-\frac{1}{2}} \sum_{y} e^{(2\pi i x y/N)} |y\rangle$$

ecuación 105

Esto nos deja en el estado

$$N^{-1} \sum_{x} \sum_{y} e^{(2\pi i x y/N)} |y\rangle |f(x)\rangle$$

ecuación 106

Paso 6: Realice una medición. Obtenemos un cierto resultado *y* en el registro de entrada y $f(x_0)$ en el registro de salida.

Paso 7: Convierta $\frac{y}{N}$ en una fracción irreducible (simplifique la fracción), y extraiga el denominador r', que es un candidato a r

Paso 8: Compruebe si $a^x mod\ N = a^{x+r} mod\ N$, de lo contrario devolverse al Paso 3.

Paso 9: Si r es impar volver al primer paso

Paso 10: Si $mcd(a^{r/2} + 1,\ N)$ o $mcd(a^{r/2} - 1,\ N)$ es diferente de N, devolver este valor.

Como podemos observar este algoritmo se compone de dos partes la parte clásica y la parte cuántica donde utilizamos la transformada cuántica de Fourier.

5 Conclusiones y logros

Entre los logros destacados de este proyecto se encuentran Hacer una documentación robusta y creación de artefactos pedagógicos para un curso de computación cuántica. Hacer una revisión de los alcances de la computación cuántica y compararla con la computación clásica. Y por último se seleccionaron 2 algoritmos e implementación de uno de ellos con una extensión de este.

Para concluir la implementación y desarrollo de los algoritmos propuestos en este proyecto con lleva a la preparación en múltiples disciplinas como física y matemática, lo cual permitió la ejecución de estos en el computador cuántico de IBM y entender la complejidad de la mecánica cuántica.

La computación quántica revolucionara el mundo digital dado su nivel de computo exponencialmente mayor a las supercomputadoras actuales. Es una tecnología que necesita más gente trabajando en ella y no solo las grandes compañías.

6 Bibliografía

Yanofsky, N. and Mannucci, M. (2013). Quantum computing for computer scientists. 1st ed. New York: Cambridge University Press.

Deutsch, D. (1985, July). Quantum theory, the Church-Turing principle and the universal quantum computer. In Proceedings of the Royal Society of London A: Mathematical, Physical and Engi-neering Sciences (Vol. 400, No. 1818, pp. 97-117). The Royal Society.

Research.ibm.com. (2017). IBM Q - US. [online] Available at: http://research.ibm.com/ibm-q/ [Accessed 13 Mar. 2017].

Anon, (2017). [online] Available at: http://users.df.uba.ar/paz/pag_comp_cuant/resumenes/clase10.pdf [Accessed 2 Dec. 2017].

Grover, L. (2017). *A fast quantum mechanical algorithm for database search*. [online]

Arxiv.org. Available at: https://arxiv.org/abs/quant-ph/9605043 [Accessed 2 Dec. 2017].

Research, I. (2017). *IBM Q experience*. [online] Quantumexperience.ng.bluemix.net. Available at: https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=full-user-guide&page=004-Quantum_Algorithms~2F070-Grover%27s_Algorithm [Accessed 2 Dec. 2017].

Nielsen, M. Chuang, I. (2010). Quantum Computation and Quantum Information. 10th Anniversary Edition: Cambridge University Press.