VNIVERSITAT DE VALÈNCIA Facultat de Física

Máster en Física Avanzada

Especialidad Física Teórica

Trabajo Fin de Máster

Introducción a los Algoritmos Cuánticos

Francisco Javier Gálvez Ramírez

Tutores:

Eugenio Roldan Serrano

German Jose de Valcarcel

Curso Académico 2013/2014

Introducción a los Algoritmos Cuánticos

5 de octubre de 2014

Índice

1. Introducción

Este trabajo pretende dar una visión del estado actual de los algoritmos cuánticos y en particular de una herramienta que que se considera sumamente útil para el diseño y la implantación de los mismos como es la caminata cuántica. Es pues una exposición de los algoritmos fundamentales sobre los que descansan posteriores desarrollos y de como la caminata aleatoria, que ha tenido un éxito notable en la computación clásica ha sido llevada al mundo cuántico para ser aplicada allí también al desarrollo de algoritmos.

En la sección 2 se exponen los conceptos básicos a manejar en computación cuántica, qubits, operadores y puertas lógicas, sin profundizar en el formalismo matemático pero haciendo uso de la notación de Dirac que es el estándar más aceptado en este campo en lo que a notación se refiere.

En la sección 3 se exponen los principales algorimos cuánticos y se da una breve explicación de cada uno de ellos. Aunque los 4 primeros (Deutsch, Deutsch-Josza, Berstein-Vazirani y Simon), podrian considerarse como simples ejercicios matemáticos sin aplicación ni interés alguno fuera de este campo, no ocurre lo mismo con el algoritmo de Shor y el de Grover, ya que son considerados algoritmos que podrían tener una aplicación práctica real y más aún un fuerte impacto en las tecnologías existentes [1]

La sección aborda el tema de la caminata cuántica. En primer lugar se da una descripción de la caminata aleatoria y luego muestran las dos versiones existentes de caminatas cuánticas, a saber discretas y continuas. En esta sección se trata tan solo la caminata cuántica en una dimensión, su extensión a más dimensiones es conceptualmente sencilla y existen en las referencias documentación sobre este tema [14],[7],[15]

Por último en la sección 5 se comentan algunos algoritmos cuánticos que pueden ser creados con la caminata cuántica.

En la década de los 80 Richard Feynman [13] ya sugirió que resolución de ciertos problemas físicos de naturaleza cuántica no es alcanzable con ordenadores que no sean capaces de generar comportamientos cuánticos y la creación de un computador cuántico es una tarea en la que muchos grupos de investigación públicos y privados se hayan inmersos desde entonces. Sin embargo, es lógico pensar que los algoritmos actuales serán incapaces de aprovechar de manera óptima características y funcionalidades, tales como el paralelismo, la superposición y la coherencia que deberían prestar los computadores cuánticos.

Se han creado ya algunos algoritmos cuánticos que han demostrado una

[1] De hecho, el anuncio del algoritmo de Shor y su confirmación como un algoritmo efectivo para la descomposición de grandes números en factores primos en tiempos muy cortos hizo puso en alerta roja a los responsables de seguridad de muchas entidades financieras, gubernamentales y compañías de telecomunicaciones de todo el mundo

eficiencia teóricamente superior en la resolución de los problemas para los que fueron diseñados. Durante la primera parte de este trabajo se hace una exposición de aquellos algoritmos cuánticos más relevantes creados hasta la fecha. Aun así, no todos los algoritmos clásicos tienen porqué tener su equivalente cuántico, y en aquellos que lo tienen, el algoritmo cuántico no es siempre más eficiente que su homólogo clásico.

Por otra parte, la Caminata Aleatoria ha servido como modelo para el diseño de algoritmos de computación estocásticos que se han implantado con éxito durante mucho tiempo en los computadores clásicos existentes. Es aquí donde nos preguntamos si el concepto de caminata aleatoria no tendría un equivalente cuántico, es decir una caminata cuántica y cuyas características fuesen igualmente exportables al campo de la algoritmia, con el fin de generar algoritmos cuánticos que puedan ejecutarse de forma óptima en los futuros computadores cuánticos. Hay que indicar que a la vista de los trabajos y publicaciones que han ido apareciendo en los últimos años [27], [19], la caminata cuántica, se vislumbra como una técnica con gran potencial para el desarrollo de futuros algoritmos cuánticos.

2. Conceptos básicos de computación cuántica

2.1. Qubits

La información clásica que manejamos en los computadores se construye en base binaria y para ello se utiliza el concepto de bit. En computación cuántica se construye su equivalente cuántico que se denomina qubit. Un qubit es una entidad abstracta que proporciona libertad para poder construir una teoría general de la computación cuántica y de la información cuántica que no dependa de un sistema físico específico para su implantación. Un qubit es un sistema que al igual que un bit, puede encontrarse en dos estados que denotamos por $|0\rangle$ y $|1\rangle$. La gran diferencia entre qubits y bits es que un qubit, estos estados $|0\rangle$ y $|1\rangle$, son los estados base de un espacio de estados constituido por cualquier combinación lineal de dichos estados base, y por consiguiente, el qubit puede encontrarse en alguno de los estados base o en cualquier estado que sea superposición lineal de estos. En base a esto, un qubit se representa generalmente, mediante un vector de la forma

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

Cuando se realiza un medida sobre un qubit, se puede obtener como resultado el estado $|0\rangle$ con probabilidad $|\alpha|^2$ o el estado $|1\rangle$ con probabilidad $|\beta|^2$. Los valores α y β son números complejos que cumplen la condición de normalización:

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

Por tanto, el estado de un qubit se representa por un vector $|\psi\rangle$ en un espacio vectorial complejo de dos dimensiones H. Los estados $|0\rangle$ y $|1\rangle$, se conocen como los estados de la base computacional y forman una base ortonormal para este espacio vectorial.

Un qubit puede encontrarse en un estado de superposición, por ejemplo, un qubit podría encontrarse en el estado:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Sin embargo al realizar una medida para comprobar su estado, se obtendrá un resultado de $|0\rangle$ con probabilidad $\frac{1}{|\sqrt{2}|^2}$ o un resultado $|1\rangle$ el $\frac{1}{|\sqrt{2}|^2}$ de las veces que se realice la medida.

Tal y como se ha dicho el qubit es una entidad abstracta que no depende de un sistema físico concreto. Para la implementación física de los qubits hay varios sistemas físicos que pueden utilizarse, a saber:

- Las dos polariaciones de un fotón.
- El alineamiento del spin nuclear en un campo magnético uniforme.
- Los estados de un electrón que orbita alrededor de un nucleo.

2.1.1. Transformaciones de sistemas de un qubit

Los circuitos que representan computadores clásicos estás compuestos de cables y puertas lógicas. Los cables se utilizan para transportar la información, mientras que las puertas lógicas manipulan esta información y la transforman de un estado a otro. Siguiendo este esquema, ¿Sería posible realizar un tratamiento similar de la información cuántica mediante circuitos cuánticos?

Dado que los qubits pertenecen al espacio vectorial generado por su base computacional, los estados generados entre ellos deben seguir perteneciendo al mismo espacio y por tanto las puertas lógicas cuánticas que transformen estos estados deben corresponderse con operaciones que se que preserven la norma del espacio en el que están definidos. Esta operaciones entre qubits tendrán lugar con operadores unitarios que se representan por matrices 2×2. La única restricción para la matrices que representan puertas cuánticas es que toda matriz $\mathbb{U}$ que represente una puerta cuántica debe ser unitaria, es decir, se debe cumplir que $\mathbb{U}^\dagger = \mathbb{I}$. A continuación se listan las matrices 2×2 más utilizadas en la representación de operaciones unitarias sobre un único qubit.

1. **Hadamard:** Esta puerta cuántica transforma un estado $|0\rangle$ es otro estado $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ y el estado $|1\rangle$ en $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$. Esta es la operación más utilizada en computación cuántica. Transforma un qubit en una superposición de estados.

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

   Dado que la puerta de Hadamard es una de las más útiles, es conveniente tratar de visualizar su forma de operar con la ayuda de la esfera de Bloch. La operación de Hadamard consiste en una rotación de 90º sobre la esfera alrededor de el eje $\hat{Y}$, seguida de una reflexión en el plano $\hat{X} - \hat{Y}$

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \beta|0\rangle + \alpha|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|0\rangle + \beta|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle\rangle}{\sqrt{2}}$$

2. **Fase:** Esta operación aplica una transformación de fase sobre el estado $|1\rangle$, sin embargo dado que las transformaciones de fase no tienen un significado físico, se puede decir que deja los estados computacionales $|0\rangle$ y $|1\rangle$ inalterados.

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

   Los casos más interesantes y utilizados en computación cuántica son aquellos para los que θ vale: $\dfrac{\pi}{8}, \dfrac{\pi}{4}, \dfrac{\pi}{2}$ y π. En concreto para $\theta = \frac{\pi}{4}$ tenemos

la matriz $\mathbb{T}$ que también se denomina matriz $\pi/8$, ya que admite la siguiente representación:

$$\mathbb{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \longrightarrow e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}$$

3. **Pauli-X:** Actua de forma equivalente a una puerta lógica NOT, transformando el estado $|0\rangle$ en $|1\rangle$ y el estado $|1\rangle$ en un estado $|0\rangle$. Geométricamente puede representarse sobre la esfera de Bloch como una rotación alrededor del eje X

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

Al contrario que su equivalente clásico, la puerta cuántica NOT actúa linealmente, es decir, que toma la superposición de estados:

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

y la transforma en otra superposición en la que se intercambian los estados:

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

4. **Pauli-Y:** Esta operación transforma el estado $|0\rangle$ en $i|1\rangle$ y el estado $|1\rangle$ en un estado $-i|0\rangle$. Geométricamente puede representarse sobre la esfera de Bloch como una rotación alrededor del eje Y

$$\mathbb{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

5. **Pauli-Z:** Esta operación deja inalterado el estado $|0\rangle$ y transforma el estado $|1\rangle$ en un estado $|-1\rangle$, lo cual geométricamente es equivalente a una rotación de π radianes alrededor del eje Z en la esfera de Bloch. La matriz de Pauli-Z es equivalente a un matriz de fase con ángulo de rotación $\theta = \pi$.

$$\mathbb{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Algunas relaciones interesantes que se dan entre estas matrices son:

1. Propiedad fundamental de las matrices de Pauli.

$$\mathbb{XYZ} = \mathbb{I}$$

2. La transformación de Hadamard $\mathbb{H}$ permite realizar un intercambio de $\mathbb{X}$ y $\mathbb{Z}$

$$\mathbb{HXH} = \mathbb{Z}$$

$$\mathbb{HZH} = \mathbb{X}$$

3. La transformación de Hadamard $\mathbb{H}$ permite realizar una inversión de $\mathbb{Y}$

$$\mathbb{HYH} = -\mathbb{Y}$$

4. $\mathbb{H} = \dfrac{\mathbb{X} + \mathbb{Z}}{\sqrt{2}}$

5. $\mathbb{R} = \mathbb{T}^2$

6. Dada un puerta cuántica arbitraria para un único qubit, esta puede descomponerse como un producto de rotaciones del tipo:

$$\begin{bmatrix} cos\frac{\gamma}{2} & -sen\frac{\gamma}{2} \\ sen\frac{\gamma}{2} & cos\frac{\gamma}{2} \end{bmatrix}$$

y una rotación alrededor del eje $\hat{Z}$:

$$\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}$$

Junto con un corrimiento global de fase. Una constante multiplicativa de la forma $e^{i\alpha}$.

Aunque haya varias puertas lógicas que pueden utilizarse para realizar operaciones sobre un qubit[2], hay que remarcar que cualquier operación unitaria sobre un qubit puede construirse utilizando tan solo la puerta de Hadamard $\mathbb{H}$ y la puerta de Fase $\mathbb{S}$

2.2. Sistemas de dos qubits

Dos bits clásicos pueden conformar cuatro posibles estados, a saber:

$$(0,0)\ ,\ \ (0,1)\ ,\ \ (1,0)\ ,\ \ (1,1)$$

De forma equivalente, un sistema compuesto por dos qubits tiene cuatro estados en su base computacional que se pueden representar como:

$$|00\rangle\ ,\ \ |01\rangle\ ,\ \ |10\rangle\ ,\ \ |11\rangle$$

Sin embargo, dos qubits también pueden encontrarse en un estado de superposición de estos cuatro estados base, por tanto, una forma más genérica de expresar el estado de dos qubits sería:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

El resultado de una medida x, siendo $x = \{00, 01, 10, 11\}$ tiene lugar con probabilidad $|\alpha_x|^2$ y con el estado de los qubits después de la medida siendo $|x\rangle$.

[2]Para una revisión más profunda de los conceptos básicos es muy recomendable referirse al libro de Nielsen y Chuang [23] y al árticulo de DiVicenzo [10].

La condición de normarlización es $\sum_{x\in\{0,1\}} |\alpha_x|^2 = 1$, donde la notación $\{0,1\}$ hace referencia al conjunto de estado de longitud dos con cada letra siendo cero o uno.

Ya es sabido que en general, en un estado de n qubits se pueden preparar estados que son superposición de los estados que forman la base computacional. Sin embargo, se pueden distinguir dos tipos de estados mezcla: aquellos que son separables y aquellos que no los son.

Son estados separables [11] aquellos que pueden expresarse como un producto vectorial de estados de un qubit. Por ejemplo, para un estado de dos qubits, se puede medir solo un subconjunto de qubits. Si se mide solo el primer qubit, la probabilidad que se obtiene es: $|\alpha_{00}|^2 + |\alpha_{01}|^2$ dejando el sistema, después de la medida el siguiente estado:

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Para satisfacer la condición de normalización, este estado está renormalizado por el factor

$$\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$$

Este estado puede expresarse como:

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle = |0\rangle \otimes (\alpha_{00}|0\rangle + \alpha_{01}|1\rangle) \tag{1}$$

De forma general se puede decir que:

$$\sum_{x\in\{0,1\}} \alpha_x|x\rangle = \sum_i |\psi_i\rangle \tag{2}$$

2.2.1. Los estados de Bell

Hay estados de dos qubits (en general de n-qubits), que no pueden expresarse como producto vectorial de estados de un qubit. Es decir:

$$\sum_{x\in\{0,1\}} \alpha_x|x\rangle \neq \sum_i |\psi_i\rangle \tag{3}$$

Dado por ejemplo, el estado $\alpha_{00}|00\rangle + \alpha 11|11\rangle$, se obsevar que este estado no puede escribirse como un producto tensorial de otros estados. Se dice entonces, que estos estados están entrelazados.

Un estado de dos qubits que tiene cierta importancia es el estado de Bell o par EPR, que viene dado por:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

El estado de Bell tiene la propiedad de que al medir el primer qubit se obtienen los siguientes posibles estados:

$$\mathcal{P}(0) = 1/2 \longrightarrow |\varphi'\rangle = |00\rangle$$

$$\mathcal{P}(1) = 1/2 \longrightarrow |\varphi'\rangle = |11\rangle$$

Es decir, la probabilidad de obtener 1 o 0 es 1/2 y después de la medida en Una medida, el estado en que se queda el sistema es: φ'.

Por tanto una medida del segundo qubit siempre da el mismo resultado que una medida en el primer qubit, esto quiere decir que los resultados de las medidas están correlacionados.

Las correlaciones de las medidas en el estado de Bell son mucho más fuertes que aquellas que pudieran existir entre estados clásicos.

Si se considera un sistema de n qubits, los estados sobre la base computacional de este sistema serán de la forma $|x_1, x_2, \ldots, x_n\rangle$ y por tanto, un estado cuántico de este sistema se especifica mediante un conjunto de 2^n amplitudes. Para $n = 500$, es como si la naturaleza mantuviese 2^{500} piezas de borradores ocultos sobre los cuales realiza los cálculos a medida que el sistema evoluciona.

2.2.2. Transformaciones de sistemas de dos qubits

Las transformaciones más comunes que se aplican a sistemas de dos qubits son:

1. **Walsh-Hadamard:** Esta transformación viene definida por $\mathbb{W} = \mathbb{H} \otimes \mathbb{H}$, y su matriz asociada es:

$$\mathbb{W} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{4}$$

2. **C-NOT:** La transformación NO-Controlado definida por $\mathbb{C}_{NOT}$, cambia el valor del segundo qubit segun el valore que tenga el primero, el cual actua como quubit de control. Su matriz asociada es:

$$\mathbb{C}_{NOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{5}$$

3. **Swap:** Esta transformación realiza un intercambio entre los dos qubits del sistema. Su representación matricial es la siguiente:

$$\mathbb{S} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{6}$$

Hay que hacer notar que las transformaciones $\mathbb{C}_{NOT}$ y $\mathbb{S}$ no pueden expresarse como un producto de matrices simples (de un qubit), lo cual significa que producen estados entrelazados.

Por otro lado, el conjunto de transformaciones formado por la transformación $\mathbb{C}_{NOT}$ y todas las transformaciones simple forman un sistema universal de transformaciones, lo cual significa que cualquier transformación unitaria puede expresarse como una combinación de transformaciones simples y la transformación $\mathbb{C}_{NOT}$.

En la bibliografía [8], [23], pueden encontrarse información adicional sobre los conceptos que se mencionan en este apartado.

3. Algoritmos Cuánticos

Hablando en términos computacionales, un algoritmo es la especificación del conjunto de instrucciones que sigue un computador para realizar una tarea o resolver un problema, independientemente de que el computador sea clásico o cuántico. Los algoritmos clásicos pueden ser deterministas o estocásticos. En el primer caso, se toma una información de entrada, el algoritmo la procesa y es capaz de generar un resultado que dependerá únicamente de la información de entrada, y mientras esta no cambie, el resultado sera siempre el mismo. Por otro lado los algoritmos estocásticos generan información de forma probabilística, esto es, para el mismo conjunto de datos de entrada cada ejecución del algoritmo puede generar una salida distinta.

Al igual que en un algoritmo clásico, la información de entrada para un algoritmo cuántico viene dada por un conjunto de n bits, y de igual forma la información que genera a la salida es también un conjunto de n bits. Sin embargo, lo que es radicalmente distinto entre un algoritmo clásico y un algoritmo cuántico es la forma en la que se produce el procesado de esa información.

Podriamos decir que el procesado cuántico pasa por los cuatro postulados de la mecánica cuántica

1. La información de entrada consiste en un vector de estado que define el estado del sistema.

2. El algoritmo cuántico aplica un operador o conjunto de operadores unitarios que hacen evolucionar a dicho estado.

3. Tras la aplicación del operador u operadores de evolución y las consiguientes operaciones cuánticas, el estado inicial se transforma en una superposición de estados que evolucionan acorde a las leyes de la mecánica cuántica.

4. Finalmente se realiza una medida sobre la superposición de estados que colapsa el sistema y proporciona un resultado con una probabilidad determinada.

En el tiempo de vida de la computación cuántica, no han sido muchos los algoritmos que se han generado. Hay que decir, que a pesar de las propiedades de superposición y paralelismo con que cuenta la computación cuántica, no todos los algoritmos cuánticos son más eficientes que sus correspondientes algoritmos clásicos a la hora de realizar un cálculo. Existen sin embargo un conjunto de algoritmos que si han demostrado su eficiencia frente a los algoritmos clásicos y son estos algoritmos y las técnicas que utilizan los que sientan las bases para el desarrollo de la computación cuántica.

3.1. El Algoritmo de Deutsch

El algoritmo de Deutsch es uno de los primeros algoritmos que demuestra de forma fehaciente que los algoritmos cuánticos pueden ser más eficientes que los algoritmos clásicos. El algoritmo de Deutsch se utiliza para determinar si una función binaria es constante o es balanceada. Una función binaria, siempre devolverá valores 0 o 1. Si la función es contante, entonces siempre devolverá el mismo valor o bien 0 o bien 1, independientemente del valor de entrada. Si la función es balanceada, entonces la mitad de las entradas generarán un resultado igual a 0 y la otra mitad un resultado igual a 1.

Dada la función:

$$f : \{0,1\} \longrightarrow \{0,1\} \tag{7}$$

se aprecia que solo existen cuatro casos posibles

$$\begin{aligned} f_1 &: 0 \longrightarrow 0, 1 \longrightarrow 0, \\ f_2 &: 0 \longrightarrow 1, 1 \longrightarrow 1, \\ f_3 &: 0 \longrightarrow 0, 1 \longrightarrow 1, \\ f_4 &: 0 \longrightarrow 1, 1 \longrightarrow 0. \end{aligned}$$

Para los casos f_1 y f_2, el resultado es siempre el mismo, y por lo tanto diremos que la función es constante. Para los casos f_3 y f_4 diremos que la función es variable.

En el caso clásico, si se desea averiguar con que tipo de función estamos tratando, es necesario realizar al menos dos medidas. Lo que permite el algoritmo de Deutsch es determinar si la funcion es constante o variable con una única medida.

En su forma inicial, el algoritmo de Deutsch se aploica a una función booleana entre $\{0,1\}$ y $\{0,1\}$, pero puede generalizarse y aplicarse a dominios más extensos. $f : \{0,1\}^2 \longrightarrow \{0,1\}$

- f es una función constante o Balanceada
- Hay que averiguar si f es constante o balanceada con el menor número posible de llamadas a la función.
- Clasicamente hay evaluar la función hasta un máximo de un número de veces exponencial en n. Cuánticamente, se genera un estado mezcla de los qubits de entrada que posibilita obtener el resultado con una sola medida.
- Los operadores que se utilizan son: el operador Hadamard H y el operador U_f que evalúa la función f. sobre el estado mezcla de qubits generado. Esta puerta lógica U_f, se define como:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \tag{8}$$

donde $\oplus$ es la suma $mod(2)$ bit a bit.

La transformación de Hadamard $H^{\otimes n}$, se define como:

$$H^{\otimes n}|x\rangle = \sum_{y}(-1)^{x\cdot y}|y\rangle \tag{9}$$

Siendo $x \cdot y$, el producto escalar bit a bit.

Los pasos de los que consta el algoritmo de Deutsch son:

1. Se parte de un sistema de dos qubits el mismo estado $|0\rangle$ y se aplica una operación de negación sobre el segundo qubit, esto es:

$$|00\rangle \longrightarrow |01\rangle \tag{10}$$

2. Se aplica una operación de Hadamard sobre ambos qubits. De esta forma se genera la mezcla de estados.

$$|01\rangle \longrightarrow \frac{1}{2}\left(|0\rangle + |1\rangle\right) \oplus \left(|0\rangle - |1\rangle\right) \tag{11}$$

3. Se evalúa f mediante la aplicación del operador de evaluación U_f

$$\frac{1}{2}\left(|0\rangle \oplus |\left(|f(0)\rangle - |1 - f(0)\rangle\right) + |1\rangle \oplus \left(|f(1)\rangle - |1 - f(1)\rangle\right)\right) \tag{12}$$

Simplificando: $\bar{f}(x) = 1 - f(x)$:

$$\frac{1}{2}\left(|0\rangle \oplus |\left(|f(0)\rangle - |\bar{f}(0)\rangle\right) + |1\rangle \oplus \left(|f(1)\rangle - |\bar{f}(1)\rangle\right)\right) \tag{13}$$

4. Se aplica de nuevo el operador de Hadamard, pero esta vez solo al primer qubit.

$$\frac{1}{2}\left(|0\rangle + (-1)^{\alpha}|1\rangle\right) \oplus \left(|f(0)\rangle - |\bar{f}(0)\rangle\right) \tag{14}$$

5. Se realiza una medida sobre el primer qubit. Esta medida consiste en evaluar α de tal forma que:

$$\alpha = \begin{cases} 0 & \text{si } f \text{ es constante} \\ 1 & \text{si } f \text{ No es constante} \end{cases} \tag{15}$$

3.2. El Algoritmo de Deutsch-Josza

Como hemos comentado anteriormente, el algoritmo de Deutsch puede ampliarse para considerar un espectro más amplio de funciones. Su generalizacion se conoce como el algoritmo de Deutsch-Jozsa y fue propuesto por David Deutsch y Richard Jozsa en 1992.

El problema sigue siendo el mismo, es decir, determinar si una función binaria arroja un resultado constante o variable, si embargo ahora el dominio sobre el que se aplica la función es más amplio.

Se considera un registro de entrada de N-bits, $x = (x_1, x_2, \ldots, x_N) \in \{0,1\}^2$. Se comienza con un estado $|0^n\rangle$ y le aplica la siguiente serie de transformaciones:

1. Transformación de Hadamard de forma independiente a cada qubit:

$$\frac{1}{\sqrt{2^n}} \sum |i\rangle \tag{16}$$

2. Se aplica un operación de inversión de signo

$$\frac{1}{\sqrt{2^n}} \sum (-)^{x_i} |i\rangle \tag{17}$$

3. Se aplica de nuevo una transformación de Hadamard:

$$\frac{1}{2^n} \sum (-1)^{x_i} \sum (-1)^{i \cdot j} |j\rangle \tag{18}$$

siendo: $i \cdot j = \sum_{k=1}^{n} i_k j_k$. Se puede apreciar que la amplitud del estado $|0^n\rangle$ en la superposición final es:

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} = \begin{cases} 1 & \text{si } x_i = 0 \quad \forall i, \\ -1 & \text{si } x_i = 1 \quad \forall i, \\ 0 & \text{si } x \text{ es balanceada.} \end{cases} \tag{19}$$

4. Finalmente se realiza la medida.

Si x es constantes, resultará que al realizar la medida u observación del estado se obtiene $|0^n\rangle$ y si por el contrario se obtiene cualquier otro estado.

De nuevo como en el caso anterior, cualquier algoritmo clásico determinista requeriría de al menos $N/2+1$ consultas para determinar el tipo de x, sin embargo el algoritmo de Deutsch-Josza resolvía [23] este problema con tan solo dos consultas.

3.3. El Algoritmo de Berstein-Vazirani

El algoritmo de Berstein-Vazirani es prácticamente el mismo algoritmo de Deutsch-Josza pero redefiniendo la función para poder resolver otro tipo de problema. El problema que se plantean Bernstein y Vazirani es el siguiente: Dada una función $f(x) = x \cdot a$

$$f : \{0,1\}^n \longrightarrow \{0,1\} \tag{20}$$

se desea encontrar a.

Dado que ahora $(-1)^{f(x)} = (-1)^{(i\cdot a) mod\ 2} = (-1)^{i\cdot a}$, el estado obtenido después de la consulta se puede escribir como:

$$\frac{1}{\sqrt{2^2}} \sum_{i\in\{0,1\}} (-1)^{f(x)}|i\rangle = \frac{1}{\sqrt{2^n}} \sum_{i\in\{0,1\}} (-1)^{x\cdot a}|i\rangle \tag{21}$$

Aplicando la tranformación de Hadamard a cada qubit se obtiene el estado $|a\rangle$ con tan solo una consulta y un numero de operaciones $\mathcal{O}(n)$. Sin embargo un algoritmo clásico, tanto determinista como estocástico necesitaría realizar n consultas.

El algoritmo de Bernstein-Vazirani puede utilizarse para probar cuales son las variables de entrada de las que depende una función. En cierto sentido, esta tarea es mucho más general que distinguir entre funciones booleanas lineales, que es la tarea para la que originalmente se diseñó el algoritmo.

3.4. El algoritmo de Simon

El algoritmo de Simon resuelve problema que se detalla a continuación. Disponemos de una función $f(x)$ que esta definida como:

$$f : \{0,1\}^n \longrightarrow \{0,1\}^n \tag{22}$$

La función $f(x)$ cumple con la siguiente condición: Existe una cadena $a \in \{0,1\}^n$ tal que:

$$f(x) = f(y) \iff x \oplus y \in \{0^n, a\} \tag{23}$$

se trata pues, de obtener la cadena a.

Vamos a poner un sencillo ejemplo que ilustre de forma más compresiva este problema y su resolución. Supongamos que $n = 3$, con lo que tenemos que la función $f : \{0,1\}^3 \longrightarrow \{0,1\}^3$, podría presentar los siguientes valores:

x	$f(x)$
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

Para resolver el problema clásicamente, es necesario encontrar dos inputs x e y, para los cuales se cumpla que $f(x) = f(y)$. Dado que no hya ningún restricción en la función, ni ninguna estructura que ayude a dar con esos inputs, seria necesario tantear del orden de $\mathcal{O}(\sqrt{2^n})$ inputs antes de encontrar un par

que cumpliesen la condición mencionada (para $n = 3$, serían 3 tanteos).

El algoritmo de Simon consiste en la aplicación iterativa de la secuencia de operadores $H\,B_f\,H$, donde H es el operador de Hadamard y B_f se define como:

$$B_f|x, y\rangle = |x, f(x) \oplus y\rangle \tag{24}$$

Así pues, partiendo de un estado $|0^n, 0^n\rangle$ se tiene:

$$|0^n, 0^n\rangle \xrightarrow{H} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x, 0^n\rangle \xrightarrow{B_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x, 0^n\rangle \xrightarrow{H} \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y}|y, f(x)\rangle$$

Cuando se ejecuta este proceso se pueden dar dos casos:

- **caso 1:** $s = 0^n$ con probabilidad $p_y = \frac{1}{2^n}$
- **caso 2:** $s \neq 0^n$ en cuyo caso la probabilidad de obtener cada cadena y será:

$$\begin{cases} 2^{-(n-1)} & \text{si } a \cdot y = 0 \\ 0 & \text{si } a \cdot y = 1 \end{cases}$$

En ambos casos la medida sobre una cadena y que satisfade $acy = 0$ y la distribución es uniforme sobre todas las cadenas que satisfacen esta restricción. Con esta información es suficiente para determinar a ya que el proceso se repite varias veces y se acepta una pequeña probabilidad de error. Para $n - 1$ ejecuciones del proceso se obtiene un sistema de ecuaciones lineales del tipo $y_i \cdot a = 0$ que de ser linealmente independientes solo obtiene una solución de a no igual a cero. Si existe dependencia lineal, se puede resolver igualmente.

la conclusión es que para $\epsilon > 0$, el algoritmo de Simon puede resolver este problema con una probabilidad de error máxima ϵ utilizando $\mathcal{O}(n)$ consultas.

3.5. El Algoritmo de factorización de Shor

El número de pasos que un computador clásico debe ejecutar para encontrar los factores primos de un numero N formado por d dígitos crece exponencialmente con d. El algoritmo de Shor resuelve de forma efectiva el problema de la descomposición en factores primos de un número N, y lo hace utilizando un mecanismo cuántico en un tiempo $\mathcal{O}((logN)^3)$. De llegar a ejecutarse en un computador cuántico lo suficientemente grande como para poder descomponer grandes números, dejaría inservibles los actuales sistemas de encriptación basados en descomposición en números primos. La efectividad del algoritmo de Shor se comprobó por primera vez en 2001 en el IBM Almaden Research Center para $N = 15$ utilizando un sistema de Resonancia Magnética Nuclear (NMR)de siete qubits [18][3]. Posteriormente otros grupos ha ejecutado el algoritmo de Shor utilizando sistemas basados en qubits fotónicos [20]

[3]En este experimento no se observo la propiedad de Entanglement

El algoritmo de Shor consta de dos partes. Primero transforma el problema de la descomposición en factores primos a un problema de encontrar el período de una función y esto se puede implantar clásicamente. Después haciendo uso de la transformada de Fourier cuántica, encuentra el periodo de la función. Esta última partes es la que proporciona la aceleración cuántica del algoritmo. El algoritmo de Shor implementa los siguientes pasos:

1. Se elige de forma aleatoria un número entero positivo, sea m.
2. Se determina el periodo P de la siguiente función

$$f(x) = m^x mod N \tag{25}$$

   Siendo:

   - N es el número a factorizar.
   - m es un número elegido aleatoriamente tal que $m < N$

   Hay que encontrar el periodo P de la función $f(x)$, tal que: $f(x+P) = f(x)$. Se puede dar el caso (1), en el que P divide el número de puntos $N = 2^n$ sobre el que se evalua la función $f(x)$, es decir:

$$\frac{N}{P} = m \longrightarrow \qquad m \in \mathbb{Z} \tag{26}$$

   El caso general añade más complicación pero no cambia la idea general.
3. Si se obtiene P como un número impar, entonces se vuelve al Paso 1.
4. Si se cumple que $m^{P/2} + 1 = 0 \; mod \, N$, entonces, volver al Paso 1.
5. Se calcula el factor de N : $d' = m.c.d.(m^{P/2} - 1, N)$ Como $(m^{P/2} - 1) \neq mod N$, entonces ocurre que d' es un factor no trivial de N.

3.6. El Algoritmo de búsqueda de Grover

El algoritmo de Grover resuelve la búsqueda de elementos en un espacio no estructurado, esto es un espacio donde no existe ninguna estructura, tal como índices u ordenación alguna, que facilite el establecimiento una metodología de búsqueda.

Por tanto, dado un espacio E no estructurado de tamaño N, con un modelo clásico de computación es necesario evaluar un promedio de $N/2$ elementos para encontrar el elemento buscado. En el mejor de los casos se puede dar con el elemento buscado en la primera evaluación, pero en el peor de los casos se puede tener que realizar un número de evaluaciones igual al tamaño del espacio de búsqueda. El orden de complejidad es de $O(N)$.

En 1996, Lov Grover publicó una algoritmo cuántico capaz de resolver un problema de búsqueda de un elemento único en un espacio no estructurado

con un orden de complejidad (número de evaluaciones) de $O(\sqrt{N})$.

El algoritmo de Grover está basado en una técnica denominada amplificación de amplitud, la cual partiendo de un estado cuántico y tras sucesivas transformaciones, va amplificando la amplitud de los "componentes" que verifiquen una condición de búsqueda (impuesta por un operador que denominamos Oráculo). En cada iteración se modifica la amplitud de aquellos que no cumplan la condición. Al medir se tiene pues un valor con probabilidad de acierto alta.

Se trabaja en un espacio no estructurado que contiene N elementos, de tal forma que N se pueda expresar como $N = 2^n$ para algún valor de n. Lo elementos se numeran desde $x = 0$ hasta $x = 2^n - 1$, y se pretende hallar aquel elemento tal que $f(x) = 1$.

Un computador cuántico permite evaluar la función f sobre todos los posibles inputs, sin más que construir el estado $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ la cual se obtiene a partir del estado inicial $|00\cdots0\rangle$ con la transformación de Walsh-Hadamard. El problema es que no se puede leer el resultado obtenido sin destruir el estado.

El procedimiento general es el siguiente: se parte de un estado inicial $|\psi_0\rangle$, este estado se va evolucionando con la aplicación de operador unitario U_f y se va incrementado la amplitud de los estados $|x\rangle$ en los cuales $f(x) = 1$ y al mismo tiempo se disminuye en aquellos en los que $f(x) \neq 1$. Los pasos que sigue el algoritmo de Grover son:

1. **Cambio de signo de la amplitud.** Dado un estado cuántico, representado genéricamente como $\sum_{j=0}^{N-1} a_j |x_j\rangle$, la inversión de la amplitud consiste en hace rel cambio $a_j \longrightarrow -a_j$ para todos aquellos x_j que verifiquen $f(x_j) = 1$. Esto se consigue meidante la implementación de la transformación

$$U \ : \ |x\rangle \longrightarrow (-1)^{f(x)} |x\rangle \tag{27}$$

Esta transformación no modifica los estados $|x\rangle$ en los cuales se cumple que $f(x) = 0$, sin embargo, aquellos en los cuales $f(x) = 1$ resultan modificados por un coeficiente -1.

El operador cuántico U_f realiza la siguiente evaluación de la función booleana f:

$$U_f \ : \ |x, b\rangle \longrightarrow |x, b \oplus f(x)\rangle \tag{28}$$

donde $\oplus$ es la suma de módulo 2. Nóstese que:

Si $f(x) = 0$, entonces $|b \oplus f(x)\rangle = b$

si $f(x) = 1$, entonces $|b \oplus f(x)\rangle = \frac{1}{\sqrt{2}}|1\rangle - |0\rangle)$

Por lo tanto:

$$U_f\left(|x, b\rangle\right) = (-1)^{f(x)}|x, b\rangle \tag{29}$$

La actuación de U_f sobre un estado cualquiera será:

$$U_f\,|\psi, b\rangle) = \left(\sum_{x_j \in X_0} a_j|x_j\rangle - \sum_{x_j \in X_1} a_j|x_j\rangle\right) \oplus |b\rangle \tag{30}$$

siendo $X_0 = \{x : f(x) = 0\}$ y $X_1 = \{x : f(x) = 1\}$. De esta forma el efecto que produce U_f sobre las amplitudes es el cambio de signo deseado.

2. **Inversión sobre el promedio.** Si se aplica el operador $G = 2|\psi\rangle\langle\psi| - I$ a un estado cuántico $\sum_{j=0}^{N-1} a_j|x_j\rangle$, se produce la transformación:

$$\sum_{j=0}^{N-1} a_j|x_j\rangle \longrightarrow \sum_{j=0}^{N-1}(2A - a_j)|x_j\rangle \tag{31}$$

siendo A el promedio de los coeficientes a_j. Grover propuso que esta transformación podria implementarse de forma eficiente con un sistmea de $\mathcal{O}(log(N))$ puertas elementales. Para ello, la matriz correspondiente al operador G:

$$G = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix} \tag{32}$$

debe expresarse como $G = W_n R W_n$ siendo W_n la transformación de Walsh-Hadamard, esto es: $W_n = H \otimes \overset{n}{\ldots} \otimes H$ y $R = (r_{ij})$ una matriz diagonal tal que $r_{11} = 1$ y $r_{ii} = -1$ para $i = 2 \ldots N$. Esta matriz R se puede implantar con $n = log(N)$ puertas de Toffoly.

Originalmente el algoritmo de búsqueda de Grover fue diseñado para realizar búsquedas de un elemento en una base de datos no estructurada, con solución única, es decir, que no tiene elementos repetidos. Desde su aparición este algoritmo ha sido optimizado y ampliando por varios autores [refs] para realizar búsquedas sobre bases de datos con elementos repetidos.

En 2001 Zalka [32] demuestra que para un número de iteraciones menor que $\pi\sqrt{N}/4$, el algoritmo de Grover da la máxima probabilidad de encontrar el elemento buscado.

El algoritmo de Grover es el primer algoritmo cuántico que realmente muestra la superioridad de forma significativa que pueden tener los computadores cuánticos sobre los computadores clásicos en un problema de utilidad práctica.

El algoritmo de Grover y su generalización son ejemplos de uso del método de la amplificación de amplitud. En este caso, el operador A es $H^{\otimes n}$, $|\psi\rangle$ es $|0\rangle^{\otimes n}$ y $A|0\rangle^{\otimes n}$ es $|D\rangle$.

Si se miden los qubits en el estado $|D\rangle$ en la base computacional, obtenemos un elemento marcado con probabilidad $\frac{m}{N}$. Por tanto, el número de aplicaciones de U_f para encontrar un elemento marcado es $O\left(\sqrt{\frac{m}{N}}\right)$

Mediante algunos otros ejemplo podemos entender mejor la elección de $A = H^{\otimes n}$ en el algoritmo de Grover. Notese que:

$$R_D = H^{\otimes n} R_0 H^{\otimes n} \tag{33}$$

donde $R_0 = 2|0\rangle\langle 0| - I$. (ejercicio 4.1). ¿Podriamos generalizar el algoritmo de Grover utilizando un operador genérico A en lugar de $H^{\otimes n}$?. La respuesta sería afirmativa si la nueva versión del algoritmo de Grover tiene un operador de evolución que es el producto de dos operadores de reflexión. El operador R_D es una reflexión alrededor del vector $|D\rangle$, la cual se obtiene aplicando $H^{\otimes n}$ a $|0\rangle$. Si reemplazamos $H^{\otimes n}$ por A, el nuevo operador, que llamaremos R_ψ se define como:

$$R_\psi = A R_0 A^\dagger \tag{34}$$

y el estado $|\psi\rangle$ se define como:

$$|\psi\rangle = A|0\rangle \tag{35}$$

R_ψ es un operador de reflexión alrededor del vector $|\psi\rangle$. Nótese que el operador A no es necesario que sea real como se ha considerado hasta ahora. Se preserva el análisis del algoritmo mediante el uso de reflexiones alrededor de un plano real. La elección $A = H^{\otimes n}$ es la más simple posible y significa que todas las soluciones seran consideradas por igual, es decir con la misma amplitud real. Esta elección no es la más general, y en cualquier caso es una aplicación directa del método de la amplificación de amplitud.

El análisis del algoritmo de la amplificación de amplitud es muy similar al análisis de la versión generalizada del algoritmo de Grover. Despreciemos el registro extra, el cual es necesario para implementar el operador U_f pero juega un papel muy pequeño en el análisis del algoritmo. Supongamos que:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \tag{36}$$

y definamos

$$p_0 = \sum_{f(x)=0} |\alpha_x|^2 , \tag{37}$$

$$p_1 = \sum_{f(x)=1} |\alpha_x|^2 , \tag{38}$$

Tenemos que $p_0 + p_1 = 1$. Si $p_1 = 0$, el método de amplificación de amplitud no funcionará porque no hay ningún elemento marcado. Si $p_1 = 1$ entonces no necesitamos amplificar la amplitud de los elementos marcados. Por tanto asumamos que $0 < p_1 < 1$. Definiendo los estados:

$$|\psi_0\rangle = \frac{1}{\sqrt{p_0}} \sum_{f(x)=0} \alpha_x |x\rangle, \tag{39}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{p_1}} \sum_{f(x)=1} \alpha_x |x\rangle, \tag{40}$$

Tenemos:

$$|\psi\rangle = sen\left(\frac{\theta}{2}\right)|\psi_1\rangle + cos\left(\frac{\theta}{2}\right)|\psi_0\rangle \tag{41}$$

Donde:

$$sin\left(\frac{\theta}{2}\right) = \sqrt{p_1} \tag{42}$$

y $\theta \in (0, \pi)$.

Para hacer evolucionar el estado, aplicamos el operador:

$$U = R_\psi U_f \tag{43}$$

Donde $R_f = 2|\psi\rangle\langle\psi| - I$. La condición inicial es $|\psi\rangle = A|\psi_{in}\rangle$ es el estado inicial del algoritmo original. Por ahora, lo que importa es cuantas veces tenemos que aplicar U_f para encontrar un elemento marcado con certeza cuando $n \longrightarrow \infty$. La eficiencia global del algoritmo de amplificación de amplitud depende del operador A y debe considerarse eventualmente.

La evolución del algoritmo de amplificación de amplitud tiene lugar en el plano real subtendido por los vectores $|\psi_0\rangle$ y $|\psi_1\rangle$, el estado del computador cuántico despues de t pasos viene dado por:

$$U^t|\psi\rangle = sen\left(t\theta + \frac{\theta}{2}\right)|\psi_1\rangle + cos\left(t\theta + \frac{\theta}{2}\right)|\psi_0\rangle \tag{44}$$

donde θ viene dado por la ecuación anterior: $sin\left(\frac{\theta}{2}\right) = \sqrt{p_1}$. Y como antes, tomamos t de tal forma que:

$$t\theta + \frac{\theta}{2} \approx \frac{\pi}{2} \tag{45}$$

lo cual resulta en $t \approx \pi/2\theta$ si ocurre que $\theta \ll 1$. Por tanto:

$$t = O\left(\frac{1}{\sqrt{p_1}}\right) \tag{46}$$

El número de aplicaciones de U_f es asintóticamente la raiz cuadrada del número de aplicaciones que tienen lugar en un algoritmo clásico.

El tiempo de parada del algoritmo de amplificación de amplitud depende de θ o, equivalentemente, p_1. Si $A = H^{\otimes n}$, entonces el valor de θ se obtiene del número de elementos marcados. En el caso general, esta información depende del módulo de amplitudes α_x de los elementos marcados.

4. La Caminata Cuántica

4.1. La Caminata Aleatoria Clásica

Se denomina caminata aleatoria a la trayectoria que se genera al partir de un punto y realiza una serie de pasos en distintas direcciones de forma totalmente aleatoria y donde la ejecución de un paso no depende de los pasos realizados con anterioridad.

En su forma más simple el camino aleatorio sobre una recta solo comprende dos direcciones (derecha-izquierda, o delante-atras), pero puede generalizarse a más dimensiones, no necesariamente espaciales, y muestra unas propiedades realmente interesantes.

Tan interesantes son las propiedades de la caminata aleatoria que esta ha encontrado aplicación en un amplio rango de campos tales como la física, cuyo ejemplo más significativo es el movimiento browniano, en la economía, donde explica las fluctuaciones del mercado de valores, la ecología y la biología donde puede dar cuenta del crecimiento de poblaciones o incluso la psicología para ayudar a entender el proceso de toma de decisiones.

Una caminata aleatoria es un caso específico de cadena de Markov, puesto que la posición del paso siguiente dependerá de la posición en la que se encuentre la caminata en ese preciso momento. Es decir, la posición que se ocupará en el paso $n+1$, depende de la posición ocupada en el paso n.

Matemáticamente una caminata aleatoria puede expresarse como:

$$X_n = X_0 + X_1(0) + X_2(1) + ... + X_{n-1}(n-2) \tag{47}$$

donde X_0 es la posición inicial y $X_n(n-1)$ es la posición en el paso n, proviniendo del paso $n-1$. Formalmente se establece que una caminata aleatoria está compuesta por tres partes, a saber:

- Un estado inicial X_0 que es el punto desde el que se inicia la caminata.
- Un espacio de estados o posiciones Ω sobre el que se desplaza la caminata aleatoria.
- Un proceso o mecanismo P que decida de forma aleatoria cual es el estado o posición de a caminata en cada iteración.

Para concretar en una aplicación, se podría establecer el estado inicial como el tiempo $t = 0$, un espacio de estados que comprende las posiciones X_i sobre una recta de números reales, y un proceso de Bernoulli $B(1, P)$, el cual, asigna una probabilidad p al desplazamiento en un sentido y una probabilidad $q = 1 - p$ para un desplazamiento en sentido contrario. En este caso, se puede calcular la probabilidad P de que, transcurrido un tiempo $t = n$ una partícula o caminante, se encuentre en un punto concreto de la recta X_n tras la ejecución

de n procesos de Bernouilli.

Al fijar el origen de tiempos en $t = 0$, la probabilidad P, de encontrar la particular en el origen $n = 0$, en ese instante, vendrá dada por:

$$P(t = 0, n = 0) = 1 \tag{48}$$

Un instante después, para $t = 1$, la probabilidad P de encontrar a la partícula en $n = -1$ es $1/2$ y la probabilidad de encontrar la partícula en $n = +1$ es igualmente $1/2$. Sin embargo la probabilidad de que la partícula se encuentre en $n = 0$ resulta ser ahora $P = 0$. Esto es así por definición, pero se podría considerar la opción de un movimiento nulo, es decir, que en el instante $t = 1$, se aplicase una operación de reflexión y la partícula continuase estando en $t =$, pero eso sería un caso que merecería un tratamiento aparte.

Volviendo a la caminata aleatoria, se puede decir que la probabilidad que describe la posición de la partícula en un punto n, transcurrido un tiempo t, viene dada por:

$$P(t, n) = \frac{1}{2^t} \begin{pmatrix} t \\ \frac{t+n}{2} \end{pmatrix} \tag{49}$$

siendo:

$$\begin{pmatrix} a \\ b \end{pmatrix} = \frac{a!}{(a-b)!b!} \tag{50}$$

Dado que la expresión anterior solo es válida para $n \leq t$ y cuando $t + n$ sea par, se expresaría como:

$$P(t, n) = \begin{cases} \frac{1}{2^t} \begin{pmatrix} t \\ \frac{t+n}{2} \end{pmatrix} & \text{si } (t+n) \text{ par y } n \leq t \\ 0 & \text{en otro caso} \end{cases} \tag{51}$$

El valor esperado de la posición n viene dado por:

$$\langle n \rangle = \sum_{n=-\infty}^{\infty} nP(t, n) = 0 \tag{52}$$

como es de esperar si se utiliza una distribución equiprobable como la Binomial. Sin embargo el alcance que puede llegar a tener vendrá dado por la desviación estándar de esta probabilidad de distribución, que es:

$$\sqrt{\langle n^2 \rangle - \langle n \rangle} = \sqrt{\sum_{n=-\infty}^{\infty} n^2 P(t, n)} = \sqrt{t} \tag{53}$$

Otra forma de llegar a este resultado es aplicando la aproximación de Stirling a la distribución de probabilidad y obtener una distribución normal:

$$P(t, n) \simeq \frac{2}{\sqrt{2\pi t}} \, e^{-\frac{n^2}{2t}} \tag{54}$$

Para obtener la anchura de esta distribución, se calcula el momento de segundo orden haciendo $\frac{\partial^2 p}{\partial n^2} = 0$ y se obtiene que $\sigma = \sqrt{t}$.

Dado el papel tan relevante que ha tenido la caminata aleatoria, surge la pregunta de si una versión cuántica de la misma no sería también de utilidad para explicar aquellos fenómenos cuánticos cuya descripción o simulación no pueden enmarcarse dentro de un contexto clásico.

Utilizando la versión cuántica de los argumentos empleados en la confección de la caminata aleatoria se ha construido un equivalente cuántico denominado "Caminata Cuántica". Es de notar que el término aleatorio desaparece del nombre y se sustituye por el de "Cuántica". Esto se debe a que en este nuevo enfoque, los fenómenos aleatorios ya no juegan un papel relevante durante el desarrollo de la caminata.

En este trabajo, el objetivo es la utilización de la caminata cuántica para el desarrollo de algoritmos de programación cuánticos del mismo modo que la Caminata Aleatoria sirve como base de muchos algoritmos de programación.

El concepto de caminata cuántica fue introducido originalmente por Aharonov, Davidovich y Zagury en 1993 [1], proponiendo un modelo de caminata cuántica discreta. Más tarde 1998, Fahri y Gutmann [12] presentan un versión Halmiltoniana con tiempo continuo. Aunque ambas versiones presentan muchas similitudes y pocas diferencias, desde entonces se han considerado siempre dos modelos de caminata cuántica: i) a tiempo discreto ii) a tiempo continuo. Es de notar, que al pasar del dominio clásico dominio cuántico desaparece el termino aleatorio.

4.2. La caminata cuántica en tiempo discreto

Vamos a considerar en primer lugar el modelo discreto de la caminata cuántica, en este modelo, se considera que la evolución tiene lugar en base a un proceso que se ejecuta repetidas veces con resultado aleatorio, al igual que la ejecución de un proceso de Bernouilli que se comentaba en una sección anterior.

Decíamos que la caminata aleatoria estaba compuesta por un espacio de estados o posiciones sobre el que se realizan los desplazamientos, un mecanismo aleatorio que decide en cada momento cual será la próxima posición y un estado inicial desde el que partir. Vamos a ver cuales son los equivalentes a estos componentes en la caminata cuántica.

4.2.1. Espacio de Estados

El espacio de estados sobre el que se trabaja en el dominio cuántico es un espacio de Hilbert $\mathcal{H}_p$ donde la p hace referencia a la posición en la que se encuentra la caminata en un instante dado.En este primer acercamiento vamos

a considerar que el espacio de estado es unidimensional e ilimitado como sería el caso de una línea recta. También cabe la posibilidad de considerar espacios de estados acotados por uno o ambos lados, o incluso cerrados como sería el caso de una circunferencia. Si consideramos que la distancia entre dos estados adyacentes es 1, podemos representar el espacio formado por los estados base $\{|x\rangle \ : \ x \in \mathbb{Z}\}$

Los estados que se representan en esta base son funciones de onda de la forma $|\psi_i\rangle$, esto es, donde i indica la posición actual sobre la caminata cuántica. El estado inicial en el que se inicia la caminata cuántica lo denominamos por ψ_0.

Al igual que en el caso clásico, es necesario un mecanismo para desplazar la función de onda por los distintos estados del espacio de Hilbert. Con este fin, se complementa el espacio de Hilbert $\mathcal{H}_p$ con un grado de libertad adicional que condicione el desplazamiento por el mismo. Dado que estamos considerando un espacio de Hilbert unidimensional, el nuevo grado de libertad solo pude tener dos posibles opciones, derecha o izquierda. Este nuevo grado de libertad lo denominados Quiralidad y sus dos estados los representamos por $|u\rangle$ y $|d\rangle$. En la mayoría de los textos consultados, se denomina espacio moneda haciendo referencia a que este proceso puede asimilarse al lanzamiento de una moneda cuyos rango de valores está limitado a dos (cara y cruz). Adoptamos el término "Quiralidad" porque aporta más generalidad y más similitud con sistemas físicos reales tales como el spin del electrón.

Si el sistema tiene más de una componente, entonces el espacio de Hilbert sobre el que se representa es el producto tensorial de los espacios de Hilbert sobre los que se describen los componentes y al igual que para un sistema cuántico independiente. Así pues, el espacio de Hilbert que describe el espacio completo del sistema viene dado por el producto tensorial de ambos:

$$\mathcal{H} = \mathcal{H}_q \otimes \mathcal{H}_p \tag{55}$$

- $\mathcal{H}_q = \{|u\rangle, |d\rangle\}$.
- $\mathcal{H}_p = \{|x\rangle \ : \ x \in \mathbb{Z}\}$

4.2.2. Operador de Evolución

En el marco de la mecánica cuántica, la evolución de los estados de un sistema viene gobernada por operaciones unitaria, para poder adoptar este enfoque, es necesario considerar que el sistema está totalmente aislado del exterior, con lo que no hay posibilidad de que esté sometido a efectos aleatorios ni cabe el fenómeno de la decoherencia. Habiendo definido el espacio de estados global $\langle$ y el estado inicial ψ_0, un desplazamiento en el sistema podrá expresarse de la siguiente forma:

$$|\psi_1\rangle = U|\psi_0\rangle \tag{56}$$

Después de t pasos, o lo que es lo mismo, después de transcurrir t unidades de tiempo

$$|\psi_t\rangle = U^t|\psi_0\rangle \tag{57}$$

El operador unitario U debe actuar de forma coordinada sobre los espacio de posición y de quiralidad, y por tanto estárá compuesto por una parte que actual sobre el espacio de Quiralidad y otra que actua sobre el espacio de posiciones $U(C, S)$

El operador de Quiralidad C, es el primero en actuar y realiza su acción en el espacio del mismo nombre donde solo se tienen dos posibles estados $|u\rangle$ y $|d\rangle$ y por tanto debe ser una matriz 2×2. El espacio de Hilbert $\mathcal{H}_q$, tiene como base computacional los estados $|u\rangle$ y $|d\rangle$, pero realmente, puede existir cualquier estado que sea combinación lineal de estos dos. La esfera de Bloch [23] proporciona un visión geometrica de esta situación en la cual cualquier punto de la misma puede asimilarse a un estado cuántico definido en un espacio con dos grados de libertad. Un operador unitario que actua sobre los estados componentes, puede visualizarse de forma geométrica como una rotación del un vector de la esfera de Bloch.

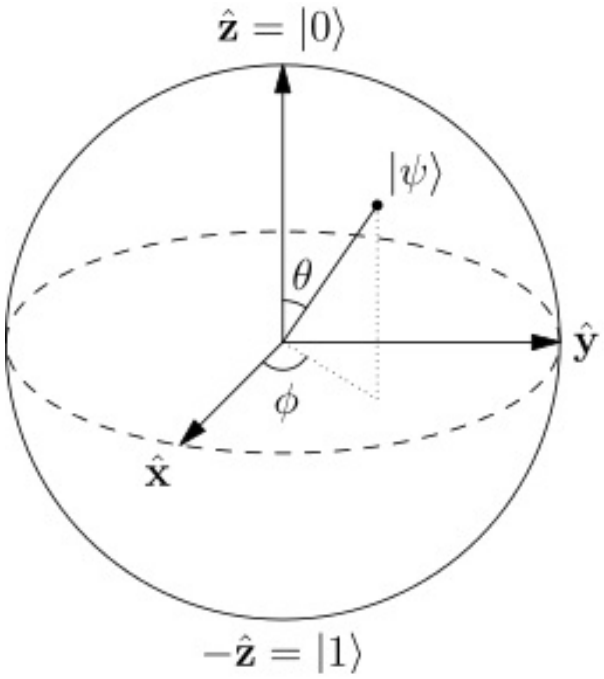

Figura 4.1 Esfera de Bloch.

La forma general de expresar una rotación de un vector cuyo origen es el centro de la esfera y cuyo extremo está en la superficie de la misma es:

$$C = \begin{pmatrix} cos\theta & e^{i\alpha} sen\theta \\ e^{i\beta} sen\theta & -e^{i(\alpha+\beta)} cos\theta \end{pmatrix} \tag{58}$$

Donde α y β son fases y θ es el ángulo de rotación. Con esto se pueden reproducir todos los posibles estados. Sin embargo aquellos que realmente son de utilidad en el caso de un sistema como el que estamos tratando son los correspondientes a $\theta = \pi/4$ con $\alpha = \beta = 0$. Esto es:

$$C(\theta = \frac{\pi}{4}, \alpha = 0, \beta = 0) = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{59}$$

El operador H solo actúa sobre los estados del espacio $\mathcal{H}_q$ por tanto para representar de forma correcta su acción sobre los estados del espacio global $|\psi_x\rangle = |q, x\rangle$ es necesario incluir una matriz unidad de la forma:

$$(H \otimes I)|\psi_x\rangle = H|q\rangle \otimes |x\rangle \tag{60}$$

De forma más específica, podemos expresarlo en con notación spinorial:

$$H \begin{pmatrix} |u,x\rangle \\ |d,x\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |u,x\rangle + |d,x\rangle \\ |u,x\rangle - |d,x\rangle \end{pmatrix} \tag{61}$$

Por otro lado, el operador S debe aplicar un desplazamiento sobre los estados base de la siguiente manera:

$$S \begin{pmatrix} |u,x\rangle \\ |d,x\rangle \end{pmatrix} = \begin{pmatrix} |u,x+1\rangle \\ |d,x-1\rangle \end{pmatrix} \tag{62}$$

La forma algebraica del operador S es:

$$S = |u\rangle\langle u| \otimes \sum_x |x+1\rangle\langle x| + |d\rangle\langle d| \otimes \sum_x |x-1\rangle\langle x| \tag{63}$$

Este operador actua sobre el espacio global $\mathcal{H}$ y proyecta el estado sobre los subespacios de quiralidad $\mathcal{H}_q$. Esta es una transformación unitaria aleatoria y al mismo tiempo balanceada, es decir existe la misma probabilidad de obtener el estado $|u\rangle$ que el estado $|d\rangle$, seguidamente desplaza el sistema en una u otra dirección según el resultado obtenido en la proyección. El operador global U vendrá dado por la siguiente expresión:

$$U = S(H \otimes I) \tag{64}$$

Supongamos que partimos de un estado localizado en $x = 0$ con la quiralidad en uno de los estados base, por ejemplo $|u, 0\rangle$. Si se elige medir el resultado de la quiralidad a lo largo del desplazamiento en la base estándar $\{|u\rangle, |d\rangle\}$ después de cada actuación de $U = S(H \otimes I)$, entonces se obtendrá la distribución de probabilidad clásica de un camino no condicionado, es decir, traslación a la derecha $|1\rangle$ con probabilidad $1/2$ o traslación a la izquierda $|-1\rangle$ en otro caso, es decir:

$$|u\rangle \otimes |0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \xrightarrow{S} \frac{1}{\sqrt{2}}(|u\rangle \otimes |1\rangle + |d\rangle \otimes |-1\rangle)$$

Al medir el estado de la quiralidad en la base estándar, se obtiene cada uno de los estados $\{|u\rangle \otimes |1\rangle, |d\rangle \otimes |-1\rangle\}$ con probabilidad $1/2$

Después de realizar esta medida no queda correlación alguna entre las posiciones. Si se continua la caminata cuántica realizando la medida a cada iteración, se obtiene la caminata aleatoria clásica sobre una línea (o sobre un círculo). La función de distribución es una gaussiana centrada en 0 y la varianza es $\sigma^2 = T$.

En la caminata cuántica, no se toma medida de la quiralidad resultante en cada una de las iteraciones intermedias de esta forma se mantienen las correlaciones entre las distintas posiciones y pueden interferir en pasos subsiguientes. Es precisamente este fenómeno de interferencia el que que genera un comportamiento totalmente distinto al de la caminata aleatoria clásica.

Una caminata cuántica que se desarrolla en t pasos se define como la transformación U^t, donde el operador U actua t veces de forma iterativa sobre el estado $|\psi_0\rangle$ definido en el espacio de Hilbert $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_P$.

Para mostrar la diferencia entre la camianta cuántica y el camino aleatorio clásico, se aplica el operador de evolución U sin realizar medidas intermedias entre las distintas iteraciones. Se comienza en un estado inicial $|\psi_0\rangle = |d\rangle \otimes |0\rangle$ y se estudia la distribución de probabilidad inducida en las posiciones.

$$U|\psi_0\rangle = |\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|u\rangle \otimes |1\rangle - |d\rangle \otimes |-1\rangle\right)$$

$$U|\psi_1\rangle = |\psi_2\rangle = \frac{1}{2}\left(|u\rangle \otimes |2\rangle - |u\rangle \otimes |0\rangle - |d\rangle \otimes |0\rangle + |d\rangle \otimes |-2\rangle\right)$$

$$\begin{aligned} U|\psi_2\rangle = |\psi_3\rangle = 2\frac{1}{\sqrt{2}}(&|u\rangle \otimes |3\rangle - |u\rangle \otimes |1\rangle - |u\rangle \otimes |1\rangle + |u\rangle \otimes |1\rangle + |d\rangle \otimes |1\rangle \\ &+|d\rangle \otimes |-1\rangle + |d\rangle \otimes |-1\rangle - |d\rangle \otimes |-3\rangle) \end{aligned}$$

Reagrupando términos:

$$|\psi_3\rangle = \frac{1}{2\sqrt{2}}\left(|u\rangle \otimes |3\rangle + |d\rangle \otimes |1\rangle - 2\left(|d\rangle \otimes |-1\rangle\right) + |u\rangle \otimes |-1\rangle - |d\rangle \otimes |-3\rangle\right) \tag{65}$$

Se puede realizar un cálculo de la distribución de probabilidad para un proceso en el que se realicen t iteraciones. El estado de la caminata cuántica se puede expresar como una combinación lineal de los componentes de su base.

$$|\psi_t\rangle = \sum a_n(t)|0\rangle + b_n(t)|1\rangle \tag{66}$$

Donde los coeficientes $a_n(t)$ y $b_n(t)$ satisfacen la condición de normalización:

$$\sum_n |a_n(t)|^2 + |b_n(t)|^2 = 1 \tag{67}$$

la distribución de probabilidad vendrá dada por la expresión:

$$P(x,t) = |a_n(t)|^2 + |b_n(t)|^2 \tag{68}$$

En concreto, se puede observar que las distribución limite de la caminata cuántica sobre una línea ya no se aproxima a una gaussiana y que la varianza σ^2 no es lineal con respecto al número de pasos t.

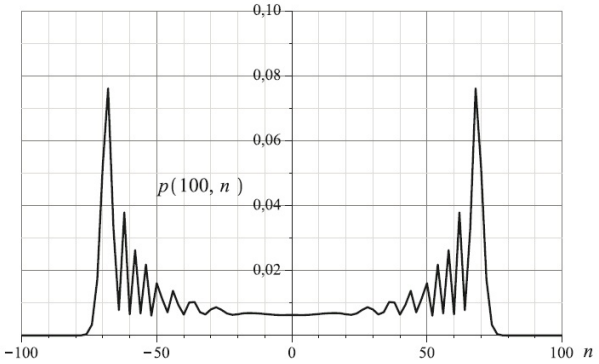

Figura 4.2 Distribución de probabilidad para 100 pasos.

Este ejemplo muestra que la distribución de probabilidad inducida por la caminata cuántica difiere de la distribución de probabilidad del camino aleatorio clásico. Al observar las gráficas generadas por uno y otro, se puede apreciar que la caminata cuántica conduce a una distribución de probabilidad asimétrica en la ocupación de posiciones. Esta asimetría tiene su origen en el hecho de que la quiralidad de Hadamard trata las direcciones $|u\rangle$ y $|d\rangle$ de forma distinta una de otra, multiplicando la fase por -1 solo en el caso $|d\rangle$.

Intuitivamente, esta diferencia en el tratamiento induce más cancelaciones para los caminos que van hacia la derecha (interferencia destructiva), mientras que las partículas que se desplazan hacia la izquierda interfieren positívamente.

Hay dos formas de reparar esta asimetría. Inspeccionando la ecuación (14) que describe el primer paso del camino de Hadamard comenzando en $|u\rangle \otimes |0\rangle$ (en lugar de $|\psi_{ini}\rangle = |d\rangle \otimes |0\rangle$) e iterando varias veces, se observa que el paso que comienza en $|u\rangle \otimes |0\rangle$ tiene un desplazamiento a la derecha exactamente opuesto al de la caminata que comienza en $|d\rangle \otimes |0\rangle$.

Para obtener una distribución simétrica, se puede comenzar el camino en una superposición de $|d\rangle$ y $|u\rangle$ y asegurarse de que ambos desplazamientos no interfieran el uno con el otro. Esto se puede conseguir, por ejemplo, comenzando con el siguiente estado simétrico:

$$|\psi_{sym}\rangle = \frac{1}{\sqrt{2}} \left(|u\rangle + i\,|d\rangle\right) \otimes |0\rangle \tag{69}$$

Como el camino de Hadamard no introduce ninguna amplitud compleja, las trayectorias desde $|u\rangle$ serán reales, y las que parten de $|d\rangle$ serán puramente imaginarias, por tanto no interferirán unas con otras permitiendo que la distribución total sea absolutamente simétrica.

Otra solución para eliminar la asimetría, consistiría en seleccionar un tipo de quiralidad distinto (también balanceada), como por ejemplo [14]:

$$Y = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \tag{70}$$

Es fácil ver que esta quiralidad trata a $|u\rangle$ y $|d\rangle$ de la misma forma, y no condiciona la caminata, independientemente de la posición inicial de la que se parta

La densidad de probabilidad límite para la caminata cuántica discreta tiene que venir dada por [30]:

$$P \approx \frac{sen\,\theta}{\pi(1-x^2\tau^{-2})\sqrt{(cos\,\theta\tau)^2-x^2}} \tag{71}$$

4.3. La caminata cuántica en tiempo continuo

A partir de las cadenas continuas de Markov es posible definir un modelo continuo de caminata aleatoria.

En el modelo de discreto, la probabilidad cambiaba con cada paso que se ejecutaba. En el modelo continuo, la probabilidad cambia en función de una variable continua. Es habitual elegir como variable continua el tiempo, así pues, en una caminata cuántica continua, la probabilidad de estar en uno u otro punto va cambiando con el paso del tiempo.

Si se supone que la probabilidad cambia de forma homogénea e isótropa en todo el espacio de estados entonces se puede decir que el ratio de transición es constante y se puede representar por γ, es decir la transición entre dos puntos adyacentes tiene lugar con una probabilidad γ por unidad de tiempo.

Si se define un intervalo de tiempo infinitesimal ϵ entonces, la probabilidad de pasar de un punto a otro tras un intervalo ϵ vendrá dada por

$$P = \gamma\epsilon \tag{72}$$

La probabilidad de permanecer en el mismo punto será por tanto:

$$Q = 1 - \gamma\epsilon \tag{73}$$

Finalmente la ecuación que marca la dinámica del movimiento es:

$$\frac{dM_{ij}}{dt} = -\sum_k H_{kj} M_{ik} t \tag{74}$$

y la solución a esta ecuación diferencial, dado un estado inicial de $M_{ij}(0) = \delta_{ij}$ es:

$$M(t) = e^{-Ht} \tag{75}$$

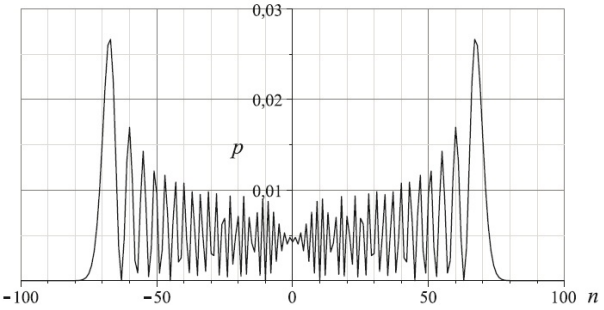

Figura 4.3 Distribución de probabilidad para 100 pasos.

Cuando se pasa a la caminata cuántica continua a partir de las cadenas de Markov continuas, se convierte la matriz de transición anterior en un operador unitario:

$$U(t) = e^{-iHt} \tag{76}$$

La evolución será: $|\psi(t)\rangle = U(t)|\psi(0)\rangle$ y la probabilidad de distribución:

$$p_k = |\langle k|\psi(t)\rangle|^2 \tag{77}$$

En una caminata cuántica continua, la evolución está dada por la ecuación de Schrödinger ($\hbar = 1$).

$$i\frac{d}{dt}\langle x|\psi(t)\rangle = \sum_y \langle|H|y\rangle\langle|\psi(t)\rangle \tag{78}$$

El Hamiltoniano se define proporcional a la matriz de transición $[M_{ij}]$, considerando que la caminata es bidireccional y el Hamiltoniano es hermítico $M_{ij} = M_{ji}$, por tanto $H = -\gamma M$, siendo γ la probabilidad por unidad de tiempo de que tenga lugar una transición entre dos puntos adyacentes.

La solución formal de la ecuación de Schrödinger viene dada por:

$$|\psi\rangle = e^{-i\gamma Mt}|\psi(0)\rangle \tag{79}$$

En el caso particular de una línea, un punto x solo conecta con los puntos adyacentes a él: $x \pm 1$, y por tanto el Hamiltoniano se reduce a:

$$H|x\rangle = -\frac{1}{2}\left(|x-1\rangle + |x+1\rangle\right) \tag{80}$$

Se fija el valor $\gamma = 1/2$ indicado la misma probabilidad de ir a derecha o a izquierda con probabilidad total 1, y con probabilidad nula de permanecer en el mismo sitio.

Dado un estado genérico representado por $|\psi(t) = \sum_x a_x(t)|x\rangle$ la solución a la ecuación de Schrödinger es inmediata, ya que los coeficientes $a_x(t)$ satisfacen:

$$i\frac{d}{dt}a_x = -\frac{1}{2}\left[a_{x+1}(t) + a_{x-1}(t)\right] \tag{81}$$

Para una condición inicial localizada en el origen $a_x(0) = \delta_{x0}$, la solución de esta ecuación es proporcional a la función de Bessel cilíndrica:

$$a_x(t) = (-i)^x J_x(t) \tag{82}$$

y por tanto la distribución de probabilidad es simplemente

$$P(x,t) = J_x^2(t) \tag{83}$$

4.3.1. Espacio de Estados

En la creación del modelo de la caminata cuántica discreta, se realiza un proceso de cuantización a partir de la caminata aleatoria clásica. Este proceso, consiste en sustituir el vector de probabilidades del caso clásico, $\vec{P}^t = \left(P_1^t, P_2^t, \ldots, P_{|V|}^t\right)$, por un vector de amplitudes de probabilidad o vector

estado $\vec{\psi^t} = \left(\psi_1^t, \psi_2^t, \ldots, \psi_{|V|}^t\right)$, y la matriz de transición M_{ij} se sustituye por un operador unitario $U(t)$.

En la creación del modelo de caminata cuántica continua, se aplica el proceso de cuantización pero esta vez partiendo de las cadenas de Markov continuas, e igualmente se sustituye el vector de probabilidades por el vector estado y la matriz de transición por el operador unitario correspondiente.

La caminata cuántica continua solo tiene lugar en el espacio de posiciones $\mathcal{H}_p$, aquí no se realiza el lanzamiento de moneda y por tanto no es necesario para nada el espacio $\mathcal{H}_c$.

Una forma sencilla de transformar la matriz de transición M en una matriz unitaria es multiplicar H por la unidad imaginaria i, por tanto el operador de evolución en la caminata cuántica continua se puede expresar como:

$$U(t) = e^{-iHt} \tag{84}$$

Condición Inicial:

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \tag{85}$$

Distribución de probabilidad:

$$p_k = |\langle k|\psi(t)\rangle|^2 \tag{86}$$

donde el índice k recorre todos los vértices de un grafo que muestra los estados de una cadena de Markov y $|k\rangle$ es el estado de la base computacional correspondiente al vértice x_k.

4.3.2. Operador de Evolución

En una linea recta los vértices son puntos enteros, si se considera el caso de la caminata cuántica continua, entonces H vendrá dado por:

$$H_{ij} = \begin{cases} 2\gamma, & \text{si } i = j; \\ -\gamma, & \text{si } i \neq j \text{ y son adyacentes;} \\ 0, & \text{si } i \neq j \text{ y no son adyacentes;} \end{cases} \tag{87}$$

Por tanto:

$$H|n\rangle = -\gamma|n-1\rangle + 2\gamma|n\rangle - \gamma|n+1\rangle \tag{88}$$

La obtención de los valores propios nos conduce al calculo de la densidad de probabilidad, (se omite este paso). Haciendo el límite densidad de probabilidad de la caminata cuántica continua [16] se llega a la expresión:

$$P(x,t) \approx \frac{1}{\pi\sqrt{(2\gamma t)^2 - x^2}} \tag{89}$$

Si se compara el gráfico con el correspondiente de la caminata cuántica discreta se observan muchos puntos en común y algunas pequeñas diferencias o detalles a considerar.

- Al igual que la caminata cuántica discreta, La distribución de probabilidad presenta dos máximos en los extremos $\pm ct$, donde $ct = 2\gamma$ para la caminata cuántica continua y $ct = 2cos\theta$ para la caminata cuántica discreta, y una zona de probabilidad muy baja en la zona del centro. En la caminata continua esto se controla mediante la elección o modificación de la quiralidad, en la caminata continua se modula mediante el parámetro γ
- En ambas caminatas, la posición del caminante presenta una Desviación Estándar que crece de forma lineal en el tiempo (o con el número de pasos en el caso discreto), aunque los experimentos realizados muestras que no son exactamente iguales, se puede decir que el comportamiento es el mismo en ambos casos y que establece una marcada diferencia con el caso de la caminata aleatoria clásica, donde la Desviación Estándar tiene un crecimiento cuadrático respecto al tiempo o al número de pasos ejecutados.

La conclusión es que el modelo continuo y el discreto son muy similares, y lo que es realmente importante es la diferencia con respecto al modelo clásico, allí es proporcional a t y aquí es proporcional a $\sqrt{t}$. Cual de los dos modelos cuánticos, continuo o discreto, es el más eficiente es algo que todavía está por determinar y es posible que varíe según el problema concreto a tratar en cada caso. De momento parecer ser que para la búsqueda de un vértice marcada en una red 2D, con condiciones de frontera periódicas, el modelo discreto resulta ser más eficiente.

4.3.3. El modelo continuo como límite del modelo discreto

La similitud entre ambos modelos invita a pensar que debe haber algún tipo de conexión entre ambos modelos. Konno [16] ha publicado algunos teoremas límite relativos a las densidades de probabilidad de la caminata cuántica discreta y continua:

$$P_{cont}(x,t) = \frac{1}{\pi\sqrt{(2\gamma t)^2 - x^2}} \tag{90}$$

$$P_{disc}(x,t) = \frac{sen\theta}{\pi(1 - x^2\tau^{-2}\sqrt{(cos\theta\tau)^2 - x^2}} \tag{91}$$

Si tomamos la expresión de la densidad de probabilidad límite obtenida por Konno [16] para la caminata cuántica discreta $P_{disc}(x,t)$ y consideramos la situación en la que $\tau \to \infty$ con $\theta \to \pi/2$ y que

$$\lim_{\substack{\theta \to \pi/2 \\ \tau \to \infty}} cos\,\theta\tau = 2\gamma t \tag{92}$$

Entonces, se obtiene la expresión de la densidad de probabilidad límite de la caminata cuántica continua $P_{cont}(x,t)$ [30]

En lo que se refiere a la relación entre amplitudes de probabilidad, tenemos que la ecuación que gobierna la evolución de la caminata aleatoria continua es la ecuación de Schrödinger en la forma:

$$i\partial_t\psi(n,t) = -\gamma[\psi(n+1,t) - 2\psi(n,t) + \psi(n-1,t)] \tag{93}$$

siendo $\psi(n,t)$ una amplitud compleja en tiempo continuo t sobre un espacio de posiciones discreto.

La caminata cuántica en tiempo discreto [Aharonov et al. Ref 4 en el articulo], tiene amplitudes de probabilidad:

$$\psi_R(n,\tau+1) = cos\theta\psi_R(n-1,\tau) - isen\theta\psi_L(n-1,\tau) \tag{94}$$

$$\psi_L(n,\tau+1) = cos\theta\psi_L(n+1,\tau) - isen\theta\psi_R(n+1,\tau) \tag{95}$$

5. Algoritmos Cuánticos Basados en La Caminata Cuántica

Como hemos visto en los puntos anteriores existen algoritmos cuánticos que pueden superar la eficiencia de los algoritmos convencionales actuales. Sin embargo la mayor obstáculo al que se enfrentan los algoritmos cuánticos es su implementación física, ya que en cualquier dispositivo o arquitectura diseñada para llevar a cabo operaciones cuánticas, el fenómeno de la decoherencia aparece inmediatamente y en cualquier punto del sistema.

La caminata cuántica es una herramienta con la que se pueden diseñar algunos de estos algoritmos cuánticos que en lo últimos años ha cobrado mucho interés. Se han hecho varias propuestas para crear un computador cuántico que implemente la caminata cuántica, esta ya se ha llevado a cabo en varios sistemas físicos. Los computadores basados en Resonancia Magnética Nuclear (NRM), han ejecutado caminatas cuánticas tanto discretas como continuas. También se han podido ejecutar caminatas cuánticas en redes formas por guías de onda , en sistemas fotónicos y en redes ópticas, sin embargo, el número de pasos que es capaz de ejecutar cada sistema antes de que aparezca el fenómeno de la decoherencia es todavía muy bajo. Los más estables han sido los sistemas de fotones en redes de guías de onda que han llegado a alcanzar apenas 100 pasos en su implementación de la caminata cuántica continua.

Existen algunos algoritmos en los que se puede basarse en la caminata cuántica, los más relevantes son:

- **Búsquedas de elementos marcados en grafos.** La búsqueda de elementos marcados en grafos es una tarea que puede acometerse mediante algoritmos basados en la caminata cuántica, tanto en su versión discreta, provista de quiralidad o en su versión continua mediante un hamiltoniano.

  Ya hemos visto en el apartado como funciona la caminata cuántica en 1-D, la única diferencia entre esta y otra que se difunde sobre un grafo de dimensión más alta es la dimensión del espacio de Hilbert utilizado para la quiralidad y la posición. En un grafo, las posiciones se corresponden con los vértices del mismo y la quiralidad es el grado del grafo [4]. Si se considera un hipercubo n-dimensional, entonces, el grado de cada uno de sus vértices será n, y el número de vértices que lo componen sera $N = 2^n$. Los espacio de Hilbert para el espacio de estados y la quiralidad será repectivamente:

  - Espacio de estados: $\mathcal{H}_v = |x\rangle : x \in \mathbb{Z}_{\mathbb{N}}$
  - Espacio de quiralidad: $\mathcal{H}_q = |q\rangle : q \in \mathbb{Z}$

[4] Aqui estamos suponiendo que todos los puntos del grafo se hallan igualmente comunicados unos con otros, es decir, todos ellos tienen el mismo número de conexiones o aristas.

Con esto se definen los operadores de desplazamiento y quiralidad como:

- Operador Desplazamiento: $S = \sum_{d=0}^{n-1} \sum_{\vec{x}} |d, \vec{x} \oplus \vec{e_d}\rangle\langle d, \vec{x}|$
- Operador Quiralidad: $C = C_0 \otimes I$

Siendo $\vec{e}_d$ los componentes de la base computacional del hipercubo de dimensión d y C_0 es un operador unitario $n \times n$ que actua sobre el espacio de quiralidad y que hay que construir en para cada grafo con el fin de que se adapte al entornos en el que estamos trabajando.

Para llevar a cabo una búsqueda cuántica es habitual utilizar un operador de quiralidad auxiliar. En el caso del algoritmo desarrollado por Shenvi, Kempe y Whaley [29] [5] se hace uso del operador:

$$C' = C_0 \otimes I + (C_1 - C_0) \otimes |\vec{0}\rangle\langle\vec{0}| \tag{96}$$

- **Distinguibilidad de elementos.** Ambainis [4] utiliza la caminata cuántica para construir un algoritmo cuántico que trate el problema de la distinguibilidad de elementos, consistente en encontrar dos elementos iguales en un conjunto de $N > 2$ elementos. Este algoritmo basado en caminatas cuánticas alcanza un nivel de complejidad $\mathcal{O}(N^{2/3})$, superando algoritmos anteriores con nivel $\mathcal{O}(N^{3/4})$. En el mismo trabajo Ambainis propone una generalización para la distiguibilidad de más elementos con un nivel de complejidad $\mathcal{O}(N^{k/3})$.

  Ambainis aplica una caminata cuántica sobre un grafo de Johnson [6] $J(n, m)$, en el que m se ha elegido acertadamente.

  La idea principal es: se tiene vertices v_s correspondientes a conjuntos $S \subseteq \{1, \ldots, N\}$, dos conjuntos v_S y v_T están conectados por una arista si los conjuntos S y T difieren en una variable. Un vértice v_S está marcado si el subconjunto S correspondiente contiene dos elementos tales que $x_i = x_y$ siendo $i \neq j$. Al lanzar ejecutar una camianta cuántica sobre los subconjuntos S, si ocurre que los elementos $x_1, \ldots, x_N$ no son todos distintos, la caminata cuántica encontrará un conjunto S que contenga $i, j : x_i = x_j$ en $\mathcal{O}(N^{2/3})$ pasos.

  En [6] Ambianis extiende el algoritmo para encontrar la distinguibilidad entre k elementos y establece que puede resolverse en $\mathcal{O}(N^{k/(k+1)})$ pasos.

- **Verificación de Productos de matrices.** La verificación del producto de matrices A, B, C de tamaño $n \times n$ consiste en decidir si se cumple que la igualdad $AB = C$. Clasicamente el mejor algoritmo conocido realiza está labor en un tiempo $\mathcal{O}(n^{2,373}$. En [5] Ambainis proponian un

[5] Consultar fuente para ver los detalles

[6] Un gráfo de Johnson es una clase especial de grafo no dirigido que se define en base a sistemas de conjuntos. Los vértices del grafo de Johnson $J(n, k)$ son los subconjuntos de k-elementos de un conjunto de n elementos.

algoritmo cuántico para este problema que empleaba un tiempo mejor $\mathcal{O}(n^{2,733}$. Posteriormente Buhrman y Spalek [9] utilizando la técnica del camino cuantico realizan un rediseño del algoritmo y obtienen un tiempo mejorado de $\mathcal{O}(n^{5/3})$.

Buhrman y Spalek utilizan un algoritmo de Szegedy [31] desarrollado como una generalización de la caminata cuántica de Ambiainis. La caminata cuántica se ejecuta sobre el producto escalar de dos grafos de Johnson. De forma muy básica (consultar las fuentes para los detalles), el algoritmo realiza los siguientes pasos:

1. Dado el producto de matrices $n \times n$": $A \times B = C$ se crea una superposición de subconjuntos $ST \subseteq [n]$ de tamaño $k = n^{2/3}$ y lee las filas de A y de B especificadas en los subconjuntos S y T.
2. Repite $\frac{n}{\sqrt{k}}$ veces el siguiente bucle:
   - *Cambio de fase*. Verifica clasicamente el producto escalar entre las matrices recortadas y multiplica la fase por -1 si encuentra algún error, es decir si: $a_S \cdot b_T \neq c_{ST}$
   - *Difusión de la caminata*. Realiza un paso en la caminata cuántica consistente en reemplaza una fila y una columna.
3. Mide S, T y las submatrices resultantes y verifica clasicamente el producto restringido de la matriz aplicando una transformación de Hadamard

6. Conclusiones y Próximos Avances

A la vista de las publicaciones existentes y las lineas de investigación abiertas en torno a la computación cuántica, es evidente que muchos investigadores y entidades han visto en este campo una vía de avance para el desarrollo de las tecnologías de la comunicación. Por todos es sabido que la ley de Moore no puede prolongarse indefinidamente y esto establece una frontera al desarrollo, ya no solo de las tecnologías de la información sino de todas aquellas ramas de la ciencia, la tecnología y el desarrollo que dependen de la computación. Se hace por tanto necesario la búsqueda de nuevas formas de manejo de la información que permitan romper la frontera de Moore y seguir avanzando en el desarrollo de nuevas tecnologías. La computación cuántica puede ser a todas luces la opción más adecuada. Es posible que no sea el próximo paso, en el camino hay otras opciones como la tecnologia fotónica, la spintrónica o la computación molecular, sin embargo las expectativas que parece prometer la computación cuántica hacen que se perfile como el modelo último a alcanzar.

Por otro lado, aún suponiendo que pudiésemos disponer de un computador cuántico, el número de algoritmos de que se dispone para hacerlo funcionar no es ni de lejos comparable con lo que existen actualmente para la computación clásica, y lo curioso del tema es que es posible que no podamos llegar tanta algoritmia como tenemos ahora ya que, en primer lugar, los algoritmos cuánticos son mucho más difíciles de codificar que los algoritmos clásicos, hay que tener en cuenta que en un marco de trabajo cuántico la intuición humana puede ser un mal aliado, ya que el comportamiento cuántico no es precisamente lógico a nuestros ojos. En segundo lugar, hay que considerar, si el tratamiento de un problema mediante computación cuántica aporta algo a su resolución, ya que no todos los problemas requieren de un "ambiente cuántico" para ser resueltos. Problemas cuya tratamiento es puramente secuencial y con resultado totalmente determinista no tienen "aparentemente" ninguna razón para necesitar un computador cuántico.

Dejando atrás los temas estas consideraciones y centrándonos en la creación de algoritmos cuánticos con la técnica de la caminata cuántica, parece evidente que al igual que la caminata aleatoria ha producido sus frutos en el campo de los algoritmos estocásticos, la caminata cuántica puede ser una herramienta muy buena para la creación de algoritmos cuánticos complejos. Esto es importante porque como hemos dichos el diseño de algoritmos cuánticos es complejo y puede ser contra-intuitivo, pero la caminata cuántica es un proceso simple y bien conocido con lo cual pasa a ser una herramienta fiel que permite trabajar con confianza.

El número de algoritmos cuánticos que hace uso de la caminata cuántica va en aumento, incluso algoritmos como el de Grover pueden implementarse con esta herramienta. Es de suponer que en los próximos años el número de algoritmos basados en caminatas cuánticas aumentará, sin embargo aun quedan algunos cabos por atar que merecen mención.

Aunque la caminata cuántica es un fácilmente comprensible su implantación no es tan sencilla. Con el tiempo distintos grupos de investigación han conseguido reproducir caminatas cuánticas en sus laboratorios, pero aparentemente, el problema de la coherencia hace que estas no vayan más alla de los 100 pasos.

El marco en el que se ha producido el desarrollo de la caminata cuántica es más bien un marco físico, es decir, tomando como modelo la caminata aleatoria, se ha realizado una "cuantización" de la misma tal y como se comenta en el trabajo. Sin embargo cuando se quiere montar el esqueleto matemático aparecen algunas dificultades. Así como la caminata aleatoria es un caso específico de cadena de Markov, la cual es a su vez una instancia concreta de un concepto más genérico como es el un proceso de Markov, seria deseable poder definir una caminata aleatoria como un caso específico de cadena de Markov cuántica, aunque asi lo hacen algunos autores, resulta que el concepto de proceso de Markov Cuántico y por ende el de Cadena de Markov cuántica no es tan intuitivo como sus contrapartidas clásicas y el establecimiento riguroso de una definición de cadena de Markov cuántica es un ejercicio matemático laborioso.

Finalmente, mencionar un área que no hemos abordado en el trabajo, es el de las simetrías, ya que actualmente no se aborda con caminatas cuánticas. Ya desde la aparición del algoritmo de Shor se vio que la búsqueda de periodicidades es una tarea que los algoritmos cuánticos pueden resolver con eficiencia, y muchos de los problemas, entre ellos la propia factorización de Shor, se reducen a la búsqueda de periodicidades en secuencias de funciones. El propio algoritmo de factorizacion de Shor, funciona convirtiendo el problema de encontrar divisores en el de encontrar periodos de una función definida sobre enteros, lo que en definitiva viene a ser un problema de encontrar las simetrías translacionales de esta función.

La idea de utilizar algoritmos cuánticos para encontrar el periodo de una función haciendo uso de la relación existente entre la mecánica cuántica y la teoría de grupos es altamente atractiva. Incluso podría tantearse si las caminatas cuánticas llevan implícito algún tipo de simetría que pueda aportar valor a la creación de este tipo de algoritmos.

Referencias

[1] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In Proceedings of the 33th ACM Symposium on The Theory of Computation (STOC-01) ACM, pp. 50-59, 2001.

[2] Y. Aharonov, L. Davidovich, and N. Zagury. "Quantum random walks". Phys. Rev. A, 48:1687-1690, 1993.

[3] L. Accardi "The noncommutative markovian property", Functional Analysis and Its Applications January-March, 1975, Volume 9, Issue 1, pp 1-7.

[4] A. Ambainis, "Quantum walks and their algorithmic applications", International Journal of Quantum Information, vol. 1, no. 4, pp. 507−518, 2003.

[5] A. Ambainis. "Quantum walk algorithm for element distinctness", SIAM Journal on Computing, 37:210-239, 2007, arXiv:quant-ph/0311001.

[6] A. Ambainis. Quantum walk algorithm for element distinctness. quant-ph/0311001.

[7] Y. Baryshnikov, W. Brady, A. Bressler, and R. Pemantle. "Two-dimensional quantum random walk". Journal of Statistical Physics, vol. 142(1), pp. 78-107, 2011.

[8] G. Benenti, G. Casati, G. Strini, "Principles of Quantum Computation and Information Vol I", "World Scientific"2003.

[9] H. Buhrman, R. Spalek. "Quantum Verification of Matrix Products", arXiv:quant-ph/0409035.

[10] D.P. DiVincenzo. "Quantum Gates and Circuits". arXiv:quant-ph/9705009v1. May 1997.

[11] A. Ekert, P. Hayden, H. Inamori. " Basic concepts in quantum comutation", arXiv:quant-ph/0011013v1, Nov 2000.

[12] E. Farhi and S. Gutmann. Quantum computation and decision trees. Phys. Rev. A, vol. 58, pp. 915-928, 1998.

[13] R. Feynman "Lectures on Computation" Westview Press, 1996.

[14] J. Kempe. Quantum random walks - an introductory overview. Contemporary Physics, vol. 44(4), pp. 307-327, 2003.

[15] V. Kendon. Quantum walks on general graphs. Int. J. Quantum Info., vol. 4(5), pp.791-805, 2006.

[16] N. Konno. "A New Type of Limit Theorems for the One-Dimensional Quantum Random Walk". quant-ph/0206103.

[17] H. Krovi, "Symmety in Quantum Walks", arxiv.org/abs/0711.1694.

[18] Lieven M. K. Vandersypen et al, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance" Nature —Vol 414 — 20/27 December 2001.

[19] K. Manouchehri, J. Wang "Physical Implementationof Quantum Walks"Springer, 2014.

[20] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X. Zhou, J.L. O'Brien (12 October 2012). "Experimental realization of Shor's quantum factoring algorithm using qubit recycling". Nature Photonics. Retrieved October 23, 2012.

[21] M. Fijisaki "Data Search Algorithms based on Quantum Walk". Proceedings of the IMECS 2012 Vol I.

[22] M. Santha, "Quantum walk based search algorithms", 5th TAMC, LNCS 4978, 31-46, 2008.

[23] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, Cambridge, UK, 2000.

[24] E. Roldán and J.C. Soriano. "Optical implementability of the two-dimensional quantum walk". Journal of Modern Optics, vol. 52, pp. 2649-2657, 2005.

[25] C.H. Papadimitriou. Computational Complexity. Addison Wesley Publishing Co., 1995.

[26] A Politi, JCF Matthews, JL O'Brien, "Shor's quantum factoring algorithm on a photonic chip" - Science, 2009.

[27] R. Portugal, "Quantum Walks and Search Algorithms" Springer, 2013.

[28] D. R. Simon, "On the power of quantum computation", Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on: 116-123.

[29] N. Shenvi, J. Kempe, K. Whaley, "Quantum random-walk search algorithm". Phys. Rev. A 67,052307.

[30] F.W. Strauch. Connecting the discrete and continuous-time quantum walks. Phys. Rev. A, 74:030301, 2006.

[31] M. Szegedy. "Quantum speed-up of Markov chain based algorithms". In Proc. of 45th IEEE FOCS, pages 32 - 41, 2004.

[32] C. Zalka "Grover's quantum searching algorithm is optimal", arxiv.org/abs/quant-ph/9711070.