Enero
2017

Computación cuántica

José Joaquin Arias Gómez-Calcerrada

Escuela Superior de Ingeniería, Universidad de Cádiz

Índice

1 Introducción

La computación cuántica es lo que se obtiene de la mezcla de la teoría cuántica y la computación. A mediados de la década de los 40 toma impulso la ciencia de la información y ahí fue cuando se cuestionó el significado del bit hasta ahora, es decir, ¿cuánto ocupa un bit?, ¿cuánta información es capaz de almacenar?, ¿qué hay del ruido?, ¿es posible enviar información a través de un canal ruidoso? Son muchas de las preguntas que surgían y a partir de las cuales se establecieron las bases de la codificación y la corrección de errores en la información, por Shannon, Golay y Hamming. Esto fue el origen de la computación.

En aquel entonces la computación se usaba para encriptar y desencriptar, y poco a poco fue haciéndose famosa en el ámbito científico. La computación no varió mucho a lo largo de los años, seguía usándose para lo mismo (matemáticas, física, etc). Sin embargo, la computación cuántica supondría un cambio significativo dado que transforma el núcleo de la computación.

En 1965, Gordon E. Moore, cofundador de Intel, postuló lo siguiente: "Cada dos años se duplica la complejidad de los componentes en los dispositivos de costo mínimo". En principio se preveía que esa tendencia se mantendría los próximos diez años, pero sin embargo es aún vigente en la actualidad. Este crecimiento exponencial predice una singularidad tecnológica, es decir, un punto en el que no se pueda crecer más debido a las limitaciones físicas o lógicas, tales como velocidades de procesamiento que no puedan exceder a la velocidad de la luz o una complejidad computacional definida de forma que sea independiente del dispositivo que lo resuelva. Para mantener la vigencia de la Ley de Moore, se han desarrollado variantes de circuitos de tipo cuántico.

2 Cómputo cuántico

A diferencia del uso del bit, que puede asumir valor 0 o valor 1, se usa el qubit como unidad básica de información para la computación cuántica. El qubit puede estar en superposición de valores 0 y 1. Al concatenarlos, al igual que con los bits se forman registros, con los qubits se forman quregistros. Su propia composición dota a los quregistros de un crecimiento exponencial que permitiría acelerar bastante los procesos. De hecho, si un computador tradicional es capaz de solucionar un problema con 2^n bits, un computador cuántico sería capaz de usar n qubits.

3 Aplicaciones de la computación cuántica

Las principales aplicaciones de la computación cuántica son las áreas de criptografía (tales como seguridad de la información, preservación de la privacidad y de la integridad de los mensajes), bases de datos (localización

de registros en información poco estructurada y recolección de información), simulación de fenómenos cuánticos (estudio de modelos de la física de partículas), cómputo masivo en ciencias como física, astronomía, química, meteorología, oceanografía y ciencias forésnicas, y simulación de procesos dinámicos (explosiones e hidrodinámica de diversos fluidos). Otra de las aplicaciones es la ingeniería a escalas atómicas y la metrología cuántica, que permitía tomar mediciones muy precisas, las cuales no podrían obtenerse de otra manera que usando mecánicas cuánticas.

Una de las áreas fuertemente beneficiadas es la medicina. Dado que los químicos deben probar muchas combinaciones moleculares para encontrar aquella que resulta máseficaz para una determinada enfermedad, un proces que puede llevar año se resolvería en pocos segundos con el uso de la computación cuántica.

Otra área es la gestión inteligente del tráfico. Los resultados de un análisis al milímetro de posibles patrones de tráfico aéreo para encontrar la ruta de vuelo más eficiente son mucho más rápidos sobre computadores cuánticos, y por lo tanto se podrán hacer cálculos más exactos en menos tiempo.

Terminamos la sección de las aplicaciones de la computación cuántica con su aplicación con el desarrollo de la inteligencia artiificial. El hecho de aprender de la experiencia con algoritmos evolutivos y variantes de este y autocorregir errores en las aplicaciones será mucho más rápido en la computación cuántica, a su vez que más eficiente.

4 Información cuántica

Como antes se ha dicho, a lo largo de décadas esta ciencia emergió para aprovechar el poder que tenía cuando se trataba de codificar, transmitir y procesar información tan solo aprovechando los efectos mecánicos cuánticos.

A la hora de desarrollar un ordenador cuántico requeriremos una maestría técnica formidable para la fabricación de dispositivos a escala del nanómetro y posiblemente a escala atómica, además de un control preciso de sus estados cuánticos.

Los requerimientos para desarrollar ese computador serían qubits físicos y escalables de dos estados cuánticos que puedan estar bien aislados del ambiente, además de inicializados, bien medidos y con capacidad de una interacción para implementar un conjunto universal de puertas lógicas cuánticas. Sin embargo, se están llevando a cabo una serie de implementaciones físicas, incluyendo resonancia magnética nuclear, ion, átomo, electrodinámica cuántica de cavidad, estado sólido y sistemas superconductores.

Durante los últimos años, los fotones fueron el enfoque líder y se intentaron relacionar de forma directa con el concepto de qubit.

4.1 Definición de Qubit

El desarrollo teórico del qubit por Benjamin Schumacher afirma que un qubit es un vector unitario en un espacio de dos dimensiones. Se puede entender como un punto en una esfera unitaria del espacio vectorial C^2 o como un sistema de dos estados tal y como un átomo de dos niveles. Cuando medimos información cuántica, realmente estamos haciendo algo bastante más abstracto que con un bit clásico. Un sistema cuántico que tenga n qubits correspondería con un espacio de Hilbert de 2^n dimensiones, es decir, tendría 2^n estados ortogonales cuánticos.

Un qubit corresponde a la ecuación $x = x_0|0\rangle + x_1|1\rangle$ con $|x_0|^2 + |x_1|^2 = 1$. Por lo tanto, los bits clásicos serían el equivalente a los qubits $|0\rangle$ y $|1\rangle$. Luego dos estados ortogonales de un qubit serían $\{|0\rangle, |1\rangle\}$.

Para visualizarlo, usaremos la esfera de Bloch (figura 1 A). Cualquier punto de la esfera de Bloch es un estado cuántico o qubit y se puede expresar como:

$-|\varphi\rangle = cos(\frac{\theta}{2})|0\rangle + e^{i\Phi}sen(\frac{\theta}{2})|1\rangle$, donde θ, Φ son números reales tales que $0 \leq \theta \leq \pi$ y $0 \leq \Phi \leq 2\pi$.

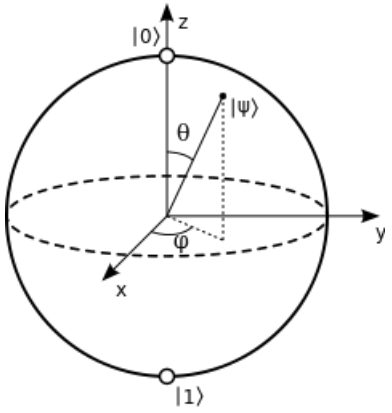

Figura 1 A: Aqui se observa la esfera de Bloch.

4.2 Fotones usados como qubits

Dado que los fotones están mayormente libres de ruido, pueden ser fácilmente manipulados para hacer puertas lógicas de un qubit. A diferencia de las puertas lógicas tradicionales, éstas permiten la codificación con varios grados de libertad. En la figura 2 A se muestra cómo un qubit puede ser codificado en la polarización de un solo fotón.

La conversión entre la polarización y la codificación puede ser fácilmente logrado mediante un divisor de haz polarizante (figura 2 B). Tras aplicar este divisor, $|0\rangle$ ó $|1\rangle$ representa un fotón en el camino superior o inferior, respectivamente.

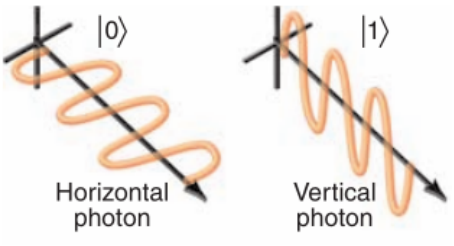

Figura 2 A: Mientras que un fotón que avanza horizontalmente se representa con el qubit $|0\rangle$, el que avanza verticalmente se representa con el qubit $|1\rangle$.

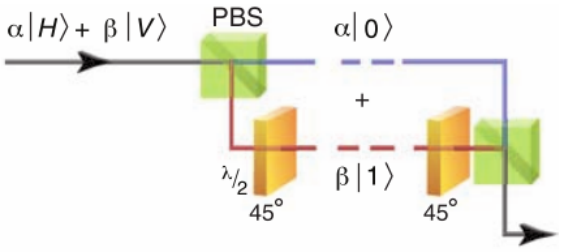

Figura 2 B: Divisor de haz polarizante.

4.3 Puertas cuánticas

Un ordenador tradicional puede ser construido por una red de puertas lógicas (figura 3 A). Las puertas cuánticas son circuitos cuánticos que operan sobre un número de qubits. Una peculiaridad que tienen estas puertas es que son reversibles. Estas puertas son representadas mediante matrices unitarias. Un ejemplo canónico es la puerta CNOT (controlled NOT gate), la cual recibe un registro de 2 qubits y se encarga de dar la vuelta al segundo qubit si y solo si el primer qubit es $|1\rangle$. En la figura 3 A se muestra una tabla con las entradas y salidas de una puerta CNOT. Por supuesto, estas puertas actúan sobre estados en superposición cuántica de dos qubits (estados $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, con $|\alpha|^2 + |\beta|^2 = 1$). Pero esta operación es más compleja de lo que parece, debido a que el primer qubit está codificado por la unión de dos fotones usando un divisor de haz con reflexión al 50%. El comportamiento sigue la base de Hadamard. A esta puerta también se le llama la puerta XOR, debido a que el efecto de una CNOT en un estado $|\alpha\rangle|\beta\rangle$ puede ser escrito como $\alpha \to \alpha$, $\beta \to \alpha \oplus \beta$, donde el símbolo $\oplus$ significa una operación XOR.

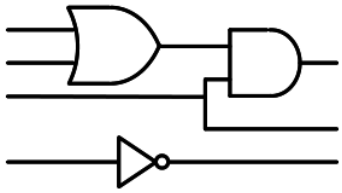

Figura 3 A: Conjunto de puertas lógicas.

Before		After	
Control	Target	Control	Target
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Figura 3 B: Entradas y salidas de la puerta CNOT.

Otras operaciones lógicas requerirán más qubits. Por ejemplo, la operación AND se consigue usando puertas lógicas de tres qubits "C-C-NOT", donde el tercer qubit sirve de NOT si y solo si los demás dos qubits están en el estado cuántico $|1\rangle$. Esta puerta obtuvo el nombre de Toffoli (1980) después de que éste mostrara al público que la versión clásica de su puerta es universal para la computación clásica reversible. El efecto de esta puerta en un estado $|\alpha\rangle|\beta\rangle|0\rangle$ se puede expresar de la forma $\alpha \to \alpha$, $\beta \to \beta$, $0 \to \alpha \cdot \beta$. Esto se resume en que si el tercer qubit tiene el estado $|0\rangle$ la puerta se comporta como una puerta clásica AND entre los dos primeros qubits.

Aquí hay otras puertas cuánticas elementales (identidad y NOT) aplicadas a un solo qubit:

- $Identidad: \ I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$
- $NOT: \ X \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$

En contradicción de la teoría clásica de la información, hay infinitas posibles puertas cuánticas, mientras que para un bit tan sólo hay 2 posibles operadores lógicos (la negación y la identidad).

4.3.1 Comportamiento de la puerta CNOT en la base Hadamard

Los problemas surgen cuando la puerta CNOT recibe más registros de entrada aparte de los qubits $|0\rangle$ y $|1\rangle$. Esto queda resuelto rápidamente con la expresión de una puerta CNOT con respecto a la base de Hadamard $\{|+\rangle, |-\rangle\}$. La base Hadamard de un registro de qubits es dada por: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$,

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Y la correspondiente base de dos registros sería: $|++\rangle = |+\rangle|+\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$.

Aplicando la puerta CNOT en esta base, el estado del segundo qubit no cambia, sin embargo sí cambia el estado del primer qubit, dándose la vuelta. Curiosamente ocurre lo mismo que con la base computacional $\{|0\rangle, |1\rangle\}$, solo que al revés. Aquí se demuestra la simetría de la puerta CNOT.

5 Teorema de la no clonación

El teorema de la no clonación dice lo siguiente: Un estado cuántico no conocido no puede ser clonado. Esto quiere decir que es imposible generar copias de un estado cuántico confiable, a menos que el estado sea conocido.

-Demostración-

Para generar una copia de un estado cuántico $|a\rangle$ debemos hacer que un par de sistemas cuánticos sufran la siguiente modificación: $U(|a\rangle|0\rangle) = |a\rangle|a\rangle$, donde U es el operador unitario de evolución. En caso de que esto funcione para cualquier estado, entonces U no depende de $|a\rangle$, y por consiguiente $U(|b\rangle|0\rangle) = |b\rangle|b\rangle$, siendo $|b\rangle$ distinto de $|a\rangle$. Sin embargo, si tenemos un estado $|c\rangle = \frac{(|a\rangle+|b\rangle)}{\sqrt{2}}$ entonces tendremos que $U(|c\rangle|0\rangle) = \frac{(|a\rangle|a\rangle+|b\rangle|b\rangle)}{\sqrt{2}}$, lo cual no es igual al esperado estado $|c\rangle|c\rangle$ luego la operación de clonación falla. Este argumento se aplica a cualquier método de clonación.

Para clonar dos estados estos deben ser ortogonales, es decir, $\langle a|b\rangle = 0$. Por lo que hemos visto hasta ahora, no podemos garantizar que un operador unitario de evolución U nos clone correctamente un estado. Podemos usar las operaciones CNOT o XOR como operaciones de copia para los estados $|0\rangle$ y $|1\rangle$, pero no para estados como $|+\rangle = \frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ ni $|-\rangle = \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$.

Para terminar esta demostración, el teorema de la no clonación está relacionado con la paradoja EPR, que juntos se ponen de acuerdo en que la mecánica cuántica no relativista es una teoría consistente. Si la clonación fuera posible, las correlaciones EPR podrían utilizarse para comunicarse más rápido que la luz, lo que conduce a una contradicción una vez que se tengan en cuenta los principios de la relatividad especial.

6 Computador cuántico universal

Una computadora cuántica es un conjunto de n qubits que cumple lo siguiente:

- Cada qubit debe ser previamente preparado en un estado conocido $|0\rangle$.
- Cada qubit puede ser medido en la base $\{|0\rangle, |1\rangle\}$.
- Una puerta cuántica universal podrá tratar a cualquier conjunto predefinido de qubits.

• Los qubits no pueden evolucionar a estados más allá de sus predeterminados estados.

Aún así esta prescripción es incompleta en cierta forma, aunque envuelve las ideas principales bastante bien. Lo que tendríamos es un modelo de conexiones de forma que las puertas lógicas son aplicadas secuencialmente a un conjunto de qubits. En un ordenador clásico que trabajará con bits y no qubits las puertas lógicas estarían colocadas a lo largo de una placa electrónica, mientras que en un computador cuántico nos imaginamos a las puertas cuánticas como interacciones que se activan y desactivan a lo largo del tiempo junto con los qubits, que se encuentran en posiciones fijas, como se puede apreciar en la figura 4 A.

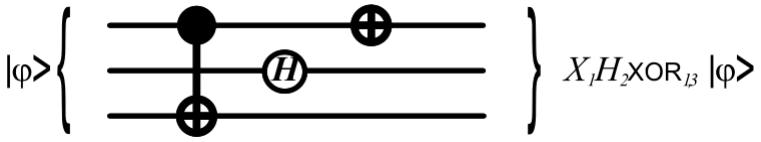

Figura 4 A: Cada línea horizontal representa la línea temporal de evolución de un qubit de izquierda a derecha. Un símbolo en una línea representa una puerta cuántica de un sólo qubit. El símbolo de la conexión de dos qubits por una línea vertical representa a una puerta cuántica que opera con ambos qubits. La red que se ve es una representación de la operación "$X_1H_2XOR_{1,3}|\phi\rangle$".

7 Ejemplos de cálculo. Algoritmos cuánticos

Tal y como conocemos a los computadores tradicionales, sabemos que son capaces de calcular el comportamiento de sistemas cuánticos. Aún así, aún no hemos demostrado que un computador cuántico sea capaz de calcular algo que no pueda un computador clásico. En efecto, mientras que nuestros algoritmos basados en su implementación con un computador clásico están relacionados directamente con ecuaciones que podemos manipular y escribir, parece ser que es improbable que problemas relacionados con la mecánica cuántica no puedan ser computados en una máquina de Turing.

Aún así, en la ciencia de la computación es bastante importante el tiempo de cómputo y el tamaño de las entradas para ciertos problemas. Ambas cosas, como hemos visto antes, se reducen bastante en el mundo de la computación cuántica debido a la diferente base que esta posee. Problemas que son computacionalmente "difíciles" pueden llegar a ser imposibles en la práctica.

Con todo esto se quiere llegar a decir que la computación cuántica introduce un nuevo campo de complejidad, es decir, las tareas para las cuales un computador clásico es muy lento pueden ser tratables en un computador cuántico.

7.1 Búsqueda del período de una función y algoritmo de Shor

Uno de los algoritmos más importantes a día de hoy es el de encontrar el período de una función. Supón una función $f(x)$ que sea periódica con período r, luego $f(x) = f(x + r)$. Supón ahora que $f(x)$ puede ser computada a partir de x y que además sabemos que $\frac{N}{2} < r < N$, para todo N. Asumiendo que a priori no se sabe el período de $f(x)$, lo que podemos hacer en un computador clásico es calcular $f(x)$ para los $\frac{N}{2}$ valores de x y darse cuenta de cuándo la función se repite.

Este método es ineficiente, dado que crece exponencialmente para el tamaño del problema. Este problema puede ser resuelto en un computador cuántico siguiendo el esquema de la figura 5 A, gracias a Shor (1994). Nuestro computador cuántico requeriría $2n$ qubits, además de $0(n)$ para el espacio de trabajo, donde $n = \lceil 2logN \rceil$. Estos están divididos en 2 registros, x e y respectivamente, en cada uno de los cuales se encontrarán n qubits. Ambos registros serán inicialmente preparados al estado $|0\rangle$.

A continuación, se aplica la operación H a cada qubit en el registro x, produciendo el estado $\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle|0\rangle$, donde $w = 2^n$. Después, se aplica un conjunto de puertas lógicas tanto a x como a y, para ejecutar la transformación $U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$.

Ahora, aplicamos U_f al estado dado y nos queda $\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle|f(x)\rangle$. Este estado se puede observar en la figura 5 B. Ahora podemos deducir que el valor de $f(x)$ ha sido calculado para $w = 2^n$ valores de x, todo en un solo paso. Aqui es donde vemos el potencial del paralelismo cuántico.

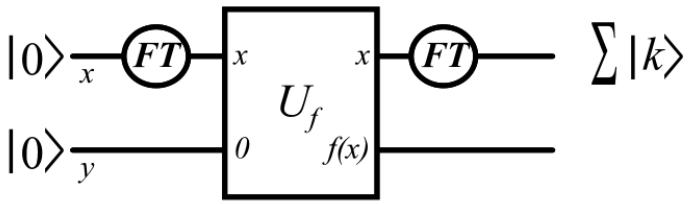

Figura 5 A: Conexiones cuánticas para el algoritmo de Shor. Aquí cada línea horizontal es un registro cuántico. Los círculos de la izquierda representan la preparación del qubit de entrada $|0\rangle$. Los círculos con el símbolo FT se refieren a la transformada de Fourier.

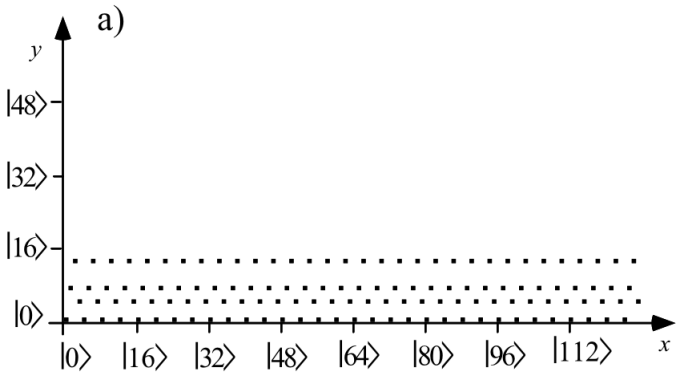

Figura 5 B: Evolución del estado cuántico en el algoritmo de Shor.

7.2 Algoritmo de búsqueda de Grover

Los algoritmos en la comunidad de la computación cuántica son bastante escasos, debido a la dificultad que suponen de encontrar. Consisten principalmente en variantes de un algoritmo llamado "algoritmo de período de búsqueda". También derivan de algoritmos de búsqueda en una lista no ordenada.

Grover (1997) presentó un algoritmo cuántico para el siguiente problema: dada una lista no ordenada de ítems $\{x_i\}$, encontrar un ítem particular $x_i = t$. Este algoritmo es un clásico en la computación tradicional y tiene un orden de búsqueda de $\mathrm{O}(N)$, siendo N el tamaño del problema. En este caso, N es el tamaño de la lista. Pero mientras que la media de pasos para encontrar el ítem en un computador tradicional es de $\frac{N}{2}$ (que pertenece, obviamente, a $\mathrm{O}(N)$), el algoritmo de Grover sería capaz de encontrar ese ítem en $\sqrt{N}$ pasos.

Este algoritmo es computacionalmente difícil. Aun así no ha sido llevado a una nueva clase de complejidad, pero difícilmente puede acelerarse más de lo que está. Según Bennet (1997), "ningún algoritmo cuántico puede hacerlo mejor que $\mathrm{O}(\sqrt{N})$".

Una descripción del algoritmo de Grover puede ser la que sigue. Cada ítem de la lista no ordenada tiene un índice i, y debemos ser capaces de probar de manera unitaria si cualquier artículo es el que estamos buscando, es decir, t. En otras palabras, debe existir un operador unitario S tal que $S|i\rangle = |i\rangle$, siempre que i sea distinto de j y $S|j\rangle = -|j\rangle$, donde j es el índice del ítem t que estamos buscando.

Este algoritmo comienza colocando un registro cuántico en superposición con todos los estados computacionales. En la figura 6 A se puede apreciar ese estado en superposición. Después de colocarse en este estado aplicamos S, que invertiría el índice del ítem que buscamos tal y como indicamos antes. Justo

después aplicamos la transformada de Fourier, cambiamos el signo de todos los componentes excepto $|0\rangle$ y aplicamos la transformada de Fourier de nuevo. De tal forma, obtendríamos la ecuación de la figura 6 B.

$$|\Psi(\theta)\rangle \equiv \sin\theta\,|j\rangle + \frac{\cos\theta}{\sqrt{N-1}} \sum_{i \neq j} |i\rangle$$

Figura 6 A: j es la etiqueta del ítem que estamos buscando. θ es un estado preparado en superposición.

$$U_G\,|\theta\rangle = |\Psi(\theta + \phi)\rangle$$

Figura 6 B: Hay que tener en cuenta que $sin\phi = 2\frac{\sqrt{(N-1)}}{N}$.

El algoritmo funciona a base de repetir U_G repetidas veces, para ser exacto alrededor de $(\frac{\pi}{4})\sqrt{N}$ veces. Después, se obtiene el valor de j que sería el índice del ítem que buscamos.

8 Relación de Computación cuántica con Máquinas de Turing: Máquina de Turing cuántica

En 1985, Deutsch introdujo la máquina de Turing cuántica como un modelo preciso de computador cuántico y, de hecho, propuso un modelo de una máquina universal de Turing cuántica, que requeriría un tiempo exponencial con respecto a una máquina de Turing cuántica.

La estructura de una máquina de Turing cuántica es muy similar a la clásica (figura 7 C). Está compuesta por los tres mismos elementos:

- Una cinta de memoria infinita, solo que cada elemento de ésta es un qubit.
- Un procesador infinito.
- Un cabezal.

Al igual que en la máquina de Turing clásica, el procesador contiene el conjunto de instrucciones a aplicar sobre el elemento de la cinta a la que apunta el cabezal. El resultado, en vez del bit, dependerá del qubit que hay dentro y del estado interno de la máquina. El procesador ejecuta una instrucción por unidad de tiempo.

Una máquina de Turing cuántica se representa con una cuádrupla $M = (Q, \Sigma, H, U)$, donde Q es un conjunto de estados internos, Σ es un conjunto de alfabetos finitos rellenos de símbolos en blanco $\#$, H es un espacio de Hilbert (Fig 7 A) y U es un operador unitario que opera sobre H definida en la figura 7 B.

$$\mathcal{H} = \left\{ \varphi \mid \varphi : \mathcal{C} \to \mathbb{C}, \sum_{C \in \mathcal{C}} \left|\varphi(C)\right|^2 < \infty \right\}.$$

Figura 7 A: Representación del espacio de Hilbert.

$$\left| \left| \langle q, T, i | U_{\delta}^{t} | c_0 \rangle \right|^2 - \left| \langle q, T, i | U_{\delta'}^{t+f(t,\frac{1}{\varepsilon})} | c_0' \rangle \right|^2 \right| < \varepsilon.$$

Figura 7 B

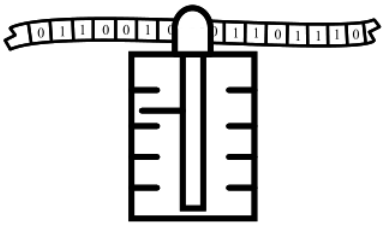

Figura 7 C: Máquina de Turing. Esto es un concepto del dispositivo mecánico que demuestra ser capaz de simular eficientemente todos los métodos clásicos de computación.

8.1 Máquina universal de Turing cuántica

Sean $M = (Q, \Sigma, \delta, U)$ y $M' = (Q', \Sigma', \delta', U')$ máquinas de Turing cuánticas y sea t un entero positivo y $\xi > 0$, decimos que la máquina de Turing cuántica M' usando como entrada c_0' simula a la máquina M junto con su entrada c_0 durante t pasos con exactitud ξ y ralentización f, donde f es una función polinómica en función de t, $\frac{1}{\xi}$. $f(t, \frac{1}{\xi})$ solo se aplica si se cumplen las siguientes condiciones:

Para todo $q \in Q$, $T \in \Sigma^*$, $i \in Z$, $||\langle q, T, i | U_{\delta}^{t} | c_0 \rangle|^2 - |\langle q, T, i | U_{\delta'}^{t+f(t,\frac{1}{\xi})} | c_0' \rangle|^2| < \xi$.

Bernstein y Vazirani probaron que existía una forma normal de una máquina de Turing cuántica M_{BV} conocida como uno de los modelos de la máquina universal de Turing cuántica. La entrada de M_{BV} es un cuádrupla $(x, \xi, t, c(M))$ donde x es el input de M, ξ es la exactitud de la simulación, t el tiempo de simulación y $c(M)$ la codificación de M. Ahora, consideremos otro modelo universal de máquina de Turing cuya entrada es $(x, \xi, c(M))$. En este modelo no necesitamos el tiempo t como input, es decir, no necesitamos saber cuándo para la máquina de Turing cuántica dada.

8.2 Definición de Q-computabilidad

Dada la existencia de máquinas de Turing cuántica en las que los elementos de la cinta de memoria infinita son qubits, se puede desarrollar un modelo de computación válido.

Una función $f : \mathbb{N}^R \to \mathbb{N}$ es computable si existe una máquina de Turing M tal que si $B\xi q_0 1^{[x_1]} 1^{[x_2]}$ ... $1^{[x_k]}$ es la configuración inicial, la configuración final es $\xi p 1^{[y]}$, siendo $y = f(x_1, x_2, \ ... \ , x_k)$.

$y = \Phi_M^{(k)}(x_1, x_2, \ ... \ , x_k)$

Luego f es parcialmente computable si:

$f(x_1, x_2, \ ... \ , x_k) = y = \Phi_M^{(k)}(x_1, x_2, \ ... \ , x_k)$

Y f es totalmente computable si:

$f(x_1, x_2, \ ... \ , x_k) = y = \Phi_M^{(k)}(x_1, x_2, \ ... \ , x_k), \ \forall (x_1, x_2, \ ... \ , x_k) \in \mathbb{N}^k$

Siendo $\Phi_M^{(k)}(x_1, x_2, \ ... \ , x_k)$ una computación resultante de aplicar la máquina de Turing M a un conjunto k de qubits, que forman la entrada del programa.

9 Bibliografía

[1] Morales-Luna, Guillermo. Revista Ingeniería Industrial, 2011, Número 2. Computabilidad y computación cuántica: revisión de modelos alternativos de computación.

[2] Jeremy L. O'Brien. Optical Quantum Computing. Science 12/2007, Volumen 318, Número 5856.

[3] Steane A. Quantum Computing Rep. Prog. Phys. 61 (1998).

[4] Adleman, Leonard M; Demarrais, Jonathan; Huang, Ming-Deh A. Quantum computability. SIAM Journal on Computing, 10/1997, Volumen 26, Número 5.

[5] Anashin, V.S. P-Adic Num Ultrametr Anal Apple (2015) 7: 169. doi: 10.1134/S2070046615030012.

[6] Note on a universal quantum Turing machine. Iriyama, Satoshi; Miyadera, Takayuki; Ohya, Masanori. Physics Letters A, 2008, Volumen 372, Número 31

[7] https://es.wikipedia.org/wiki/Esfera_de_Bloch

[8] https://en.wikipedia.org/wiki/Controlled_NOT_gate