# LA REVOLUCIÓN DE LA NANOTECNOLOGÍA: LA COMPUTACIÓN CUÁNTICA

Juan José Mamani Condori
Universidad Mayor De San Andrés
Carrera De Informática
linkfor04@hotmail.com

## RESUMEN

Las computadoras cuánticas hacen uso de la física cuántica y da lugar a fenómenos que contradicen nuestra intuición, se podrán hacer cálculos que tardarían millones de años en una computadora clásica, esto gracias a la superposición y enmarañamiento, en un computador cuántico la unidad básica de información es el qubit que se almacena en un átomo de hidrogeno.

## Palabras clave

Computación cuántica, física cuántica, qubit, superposición, entrelazamiento, algoritmos cuánticos.

## 1. INTRODUCCIÓN

Con el transcurrir del tiempo el ser humano fue buscando diversos materiales y utilizado múltiples mecanismos en el diseño, construcción y operación de maquinas que agilicen y automaticen la relación de cálculos y procesamiento de información, desde el ábaco hasta los ordenadores personales de hoy en día. [2]

Una de las áreas más punteras en la investigación y que probablemente revolucione más nuestra vida actual tal y como la conocemos hoy por hoy dentro del área de la nanotecnología es la Computación Cuántica[5]

Se puede crear millones de transistores en un solo chip. Algun dia los transistores podran llegar a un extremo logico(el nivel molecular), en el que la presencia o ausencia de un unico electron indique un estado de conexión o desconexion [white, 1996]. Aspectos que son estudiados por la “Nanotecnologia”.[4]

Actualmente las empresas desarrolladoras de chips miniaturas han llegado a su limite de tamaño obligándoles a buscar soluciones que permitan la creación de computadoras mas eficaces, por ello la ingeniería esta experimentando con la física cuántica para las computadoras del futuro. Esta tecnología se basa en el empleo de átomos, electrones y protones los cuales tendrán capacidad de procesamiento mayor a las actuales.

## 2. COMPUTACIÓN CUÁNTICA

En la computación cuántica, a diferencia de la computación actual donde cada bit puede estar en un estado discreto y alternativo a la vez, la unidad fundamental de almacenamiento es el qubit donde cada qubit puede tener múltiples estados simultáneamente en un instante determinado, reduciendo así el tiempo de ejecución de algunos algoritmos de miles de años a segundos. [2]

### 2.1 De bit a qubit

#### 2.1.1 Los bits

En la computación tradicional, un bit es la mínima unidad de información. Para representarlo se utiliza la ausencia o la presencia de miles de millones de electrones en un diminuto transistor de silicio. [2]

Hoy en día utilizamos el código binario en la computación, todos los datos de video, texto e imágenes son básicamente una cadena de 0’s o 1’s, un bit solo puede existir en uno de los dos estados, un 0 o un 1.

El transistor ha podido representar de manera sencilla y eficiente los valores del bit, a partir del cual se construyen todos los microchips, remplazando totalmente los tubos de vacio empleados en las primeras computadoras [White, 1996]. Sin embargo, el nivel de miniaturización de este componente esta llegando al limite donde el umbral cuántico se esta haciendo presente [Simon y Ekert, 2002]. Es aquí donde se habla del bit cuántico. [4]

#### 2.1.2 El qubit

En la computación cuántica el qubit es la unidad mínima de información y pretende utilizar un principio básico de la mecánica cuántica por el cual todas las partículas subatómicas (protones, neutrones, electrones, etc.) tienen una propiedad asociada llamada spin. El spin se asocia con el movimiento de la partícula alrededor de un eje. Esta rotación puede ser realizada en un sentido, o el opuesto. Si por ejemplo tomamos como bit al spin de un protón, podemos usar una dirección como 1 y otra como 0. Estos bits, tomados a partir de spin de las partículas son los que han recibido el nombre de qubits (bits cuánticos). [2]

Sin embargo, en mecánica cuántica el estado de una partícula se determina a través de la asignación de una probabilidad, no podemos hablar de un estado 0 o 1 claramente determinado. Esta es la ventaja que tiene la computación cuántica respecto a la clásica. [2]

Los qubits también tienen estados |0> y |1> son los dos estados posibles y cualquier combinación lineal (superposición). [3] Desde un punto de vista físico, un qubit es un vector unitario bidimensional en un espacio vectorial complejo, el cual tiene una base particular denotado por { |0> , |1> } [rieffel y polak] [4]

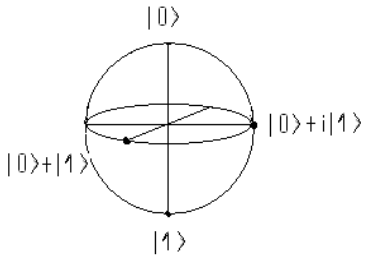


**Figura 1. Representación de cuatro estados diferentes de un qubit**

## 2.2 Superposición cuántica

Piense en un qubit como un electrón en un campo magnético. El spin del electrón puede estar en la alineación con el campo, que se conoce como un spin-up del estado, o lo opuesto al campo, lo que se conoce como un spin-down del estado. El cambio de giro del estado de un electrón a otro se consigue mediante el uso de un pulso de energía, como la de un laser, aislando completamente la partícula de todas las influencias externas: De acuerdo a la ley cuántica, la partícula entra en una superposición de estados, en los que se comporta como si estuviese en ambos estados simultáneamente. [1]

Con una computadora lógica de un qubit, cuando el qubit de entrada tiene en el estado una superposición igual a |0> y |1>, el estado resultante es la superposición de los 2 valores de salida.[2]

Esto quiere decir que para una computadora lógica de 2 qubits, que tienen dos qubits de entrada en superposición de |0> y |1>, tendríamos una superposición de 4 estados y para una compuerta lógica de 3 qubits, que tiene 3 qubits de entrada en superposición de |0> y |1>, juntos hacen una superposición de 8 estados, que son evaluados en paralelo. Por cada qubits adicional la cantidad de estados se duplica. [2]

Cada qubits utilizados podría tener una superposición de 0 y 1. Así el numero de cálculos que un ordenador cuántico podría realizar es de 2^n, donde n es el numero de qubits utilizados. Un ordenador cuántico compuesto de 500 qubits tendría un potencial para hacer 2^500 cálculos en un solo paso. Este es un numero impresionante, es infinitamente mas que los átomos que hay en el universo conocido (esto es verdadero procesamiento paralelo), ¿Cómo están partículas interactúan unos con otros? Lo harían a través de entrelazamiento cuántico. [1]

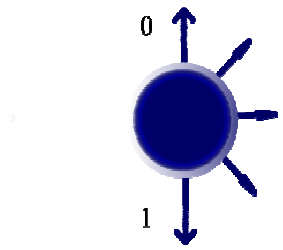


**Figura 2. El qubits puede tomar el valor de 0, 1 e intermedios a la vez**

## 2.3 Entrelazamiento cuántico

El entrelazamiento de partículas (como los fotones, electrones, o qubits) que han interactuado en algún momento, mantienen un tipo de conexión y pueden estar enredados unos con otros en parejas, en un proceso conocido como correlación. Conocer el estado de spin de una partícula, enredados, arriba o hacia abajo, permite saber que la vuelta de su compañero esta en la dirección opuesta. Aun mas asombroso es el conocimiento de que, debido al fenómeno de la superposición, la partícula medida no tiene sentido de giro único, antes de ser medido, pero es al mismo tiempo tanto en un spin-up y spin por el estado. El estado de spin de la partícula que se esta midiendo se decide en el momento de la medición y se comunica a la partícula correlacionada, que a la vez asume la dirección de giro contrario al de la partícula medida. Se trata de un fenómeno real (Einstein llamo “acción fantasmal a distancia”), cuyo mecanismo no se puede hasta ahora, se explica por una teoría, que simplemente debe ser tomado como datos. El entrelazamiento cuántico permite qubits que están separados por distancias increíbles para interactuar entre si de forma instantánea (no limitada a la velocidad de la luz). No importa cuan grande sea la distancia entre las partículas correlacionadas, que seguirá siendo enredado, siempre y cuando se encuentran aisladas. [1]

En conjunto, la superposición cuántica y entrelazamiento pueden crear una potencia de cálculo enormemente mejorada. Cuando un registro de 2 bits en una computadora normal solo puede almacenar una de las cuatro configuraciones binario (00, 01,10 o 11) en un momento dado, un registro de 2 qubits en un ordenador cuántico puede almacenar los cuatro números al mismo tiempo, porque cada qubit representa dos valores. Si se añaden mas qubits, el aumento de la capacidad se amplia exponencialmente. [1]

# 3. PUERTAS CUÁNTICAS BÁSICAS

Las operaciones unitarias simples sobre qubits se llaman puertas cuánticas, de manera análoga a las puertas lógicas de un sistema clásico. Toda puerta cuántica ha de ser reversible, lo que implica que toda operación que queramos llevar a cabo sobre un ordenador cuántico ha de ser reversible. Esto puede parecer, en un primer momento, un problema grave, porque la mayoría de puertas lógicas clásicas no son reversibles; si hacemos la operación AND sobre dos bits, obtenemos un bit del que no podemos volver a los bits originales sin alguna información extra. [6]

La solución pasa por usar unas puertas modificadas, que trabajen con más bits, de forma que vayamos guardando siempre información suficiente para volver atrás. [6]

Las leyes de la mecánica cuántica solo permiten operadores para trasformar los estados vectoriales. Dichas transformaciones son representadas por matrices. [4]. La transformación de un registro de qubits solo se la puede realizar mediante transformaciones unitarias, las cuales son utilizadas como puertas cuánticas [Rieffei y Polak, 2000]. La definición de circuito cuántico solo permite trasformaciones unitarias locales, que son trasformaciones unitarias en un numero fijo de qubits [Shor, 1996]. [4]

| Descripción | Puerta cuántica | Matriz unitaria |
|---|---|---|
| Trasformación identidad | \|0> → \|0><br>I:<br>\|1> → \|1> | $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ |
| Negación | \|0> → \|1><br>X:<br>\|1> → \|0> | $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$ |
| Y=ZX, combinación de ambas | \|0> →-\|1><br>Y:<br>\|1> → \|0> | $\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}$ |
| Z es una operación de cambio de fase | \|0> → \|0><br>I:<br>\|1> → -\|1> | $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ |

**Figura 3. Puertas cuánticas elementales aplicadas a un solo qubit [Rieffel y Polak, 200] [4]**

# 4. PROGRAMACIÓN CUÁNTICA

Tal vez aun más intrigante que el puro poder de la computación cuántica es la capacidad que ofrece para escribir programas de una manera completamente nueva. Por ejemplo, un ordenador cuántico podría incorporar una secuencia de programación que seria en el sentido de "adoptar todas las superposiciones de todos los cálculos de la técnica", algo que no tiene sentido con un ordenador clásico, que permita formas extremadamente rápida de resolver ciertos problemas matemáticos, tales como la factorización de números grandes, la criptografía, etc. [1]

Entre los ejemplos más notables se encuentra el Algoritmo de Grover, por el que se pueden localizar valores concretos en bases de datos no ordenados. Con la mayoría de manejadores de bases de datos actuales, la solución pasaría por construir un índice sobre el campo de búsqueda y luego utilizar ese índice para localizar más fácilmente el valor deseado. Este podría ser el caso, por ejemplo, si se intenta buscar el nombre de una persona dado su número de teléfono en una guía telefónica que esta ordenada alfabéticamente. Se construiría un índice sobre los numero de teléfono y con el se buscaría el nombre de la persona. [7]

### a. El algoritmo de Shor

Este es un algoritmo inventado por Peter Shor en 1995 que puede ser usado para factorizar grandes números rápidamente. Si alguna vez se implementa tendrá un efecto profundo en la criptografía, ya que pondría en peligro la seguridad. [8]

La encriptación es el método mas utilizado para el envió de datos cifrados. Con una computadora clásica no se podría descifrar el código o se tardaría mucho (tomaría mas tiempo que la edad del universo), sin embargo utilizando la computación cuántica, aplicado el algoritmo de Shor lo haría en cuestión de segundos.[8]

# 5. BORDENADORES CUÁNTICOS EXPERIMENTALES

Hasta ahora hemos hablado de puertas cuánticas y qubits de una forma ideal. En los inicios de esta disciplina se pensaba que, o bien se tardaría mucho en encontrar un sistema para crear un computador cuántico, o incluso se pensaba que nunca podría construirse uno. Pero, como pasa a menudo en la ciencia, los científicos experimentales sorprenden con su ingenio, y ahora existen diferentes ordenadores cuánticos experimentales funcionando, todavía de una manera muy rudimentaria y con pocos qubits. [6]

Para la implementación de una computadora cuántica por lo menos se necesita cumplir cinco requerimientos: [Steffen, 2001][4]

## 5.1 Requerimientos

*Primero:* Se necesita un sistema de qubits, es decir sistemas físicos con dos niveles cuánticos (átomos, fotones).

*Segundo:* Los qubits deben ser individualmente direccionales y deben interactuar recíprocamente para mantener un conjunto de puertas lógicas universales entre si. (Mantener superposiciones coherentes, borrado de registros, etc.)

*Tercer:* Debe ser posible inicializar las compuertas a un estado conocido, porque el resultado del cómputo generalmente depende de sus entradas.

*Cuarto:* Debe ser posible extractar el cálculo resultante de los qubits por alguna medida.

*Quinto:* Se necesita un tiempo de coherencia grande comparado con el promedio de duración de las puertas lógicas.

## 5.2 Métodos de implementación

Actualmente hay dos candidatos que deberían permitir la implementación de la computación cuántica, con entre 10 y 40 qubits. [6]

La primera propuesta es de Cirac y Zoller (1995), usando una línea de átomos confinados en una trampa iónica. Esta propuesta esta ampliamente superada por la mas reciente, de Gershenfeld y Chuang (1997), y simultáneamente Cory (1996), utilizando resonancia magnética nuclear. [6]

### 5.2.1 Trampa iónica

Una hila de iones se confina mediante una combinación de campos eléctricos oscilantes y estáticos en un estado de alto vacio ($10^{-8}$ Pa). Un único haz laser se divide en varios pares de haces, cada uno iluminando un ion. Cada ion tiene dos posibles estados estables (con un promedio de estabilidad de miles de años), que son ortogonales entre ellos y forman, por tanto, un qubit. [6]
Mediante los haces laser de cada ion se pueden aplicar puertas cuánticas de un solo qubit. Para aplicar puertas de dos qubits, imprescindibles para llevar a cabo cualquier computación, se recurre a la repulsión de Coulomb entre los iones, más concretamente, a la vibración conjunta de la hilera de iones. [6]

La luz no solo transporta energía, también transporta momento, y es este momento el que provoca la vibración del ion que

aprovechamos para hacer interaccionar los diferentes iones. El movimiento de los iones está cuantificado porque se encuentran atrapados en la trampa (llamada trampa de Paul). Para obtener un autentico computador cuántico todavía nos faltan dos cosas según la lista dada al comienzo. [6]

Hemos de poder ser capaces de preparar cualquier qubit (ion) en el estado |0> y de poder "leer" cualquier qubit. Lo primero es posible mediante el método de bombeo óptico y enfriamiento por laser, y el segundo mediante técnicas desarrolladas por los físicos nucleares en los últimos años. [6]

En la práctica, un computador cuántico de estas características solo se ha hecho funcionar con un solo ion, dadas las dificultades implicadas en el tratamiento tan directo de los mismos. [6]

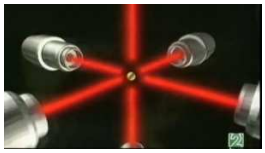

**Figura 4. Mantener al qubits en haces de rayos laser**

### 5.2.2 Resonancia magnética nuclear

El procesador cuántico es, en este caso, una molécula formada por un backbone de unos diez átomos, con otros átomos como hidrogeno conectados para completar todos los enlaces químicos. Los átomos interesantes son los del núcleo. Cada uno de ellos tiene un momento magnético asociado con el spin nuclear, incluso los estados de spin que nos da los qubits. La molécula se sitúa dentro de un campo magnético intenso y se controla mediante campos magnéticos oscilantes en impulsos de duración controlada. [6]

Hasta aquí todo bien, pero como antes, nos hace falta completar los procesos de preparación del estado inicial y de lectura del estado final. El problema es que el spin del núcleo de una molécula no se puede medir ni preparar. Para resolver este problema no se usa una sola molécula, sino una agrupación de 1020 moléculas. Así, la conjunción de todos los momentos magnéticos de los núcleos es suficientemente fuerte para ser detectable como un sutil campo magnético. Los experimentos con RMN (Resonancia Magnética Nuclear) han dado resultados positivos en estos últimos años en la manipulación y medida de estados equivalentes en complejidad a la requerida por un ordenador cuántico de unos cuantos qubits. Parece, por tanto, que los primeros ordenadores cuánticos funcionales serán sistemas RMN. Sin embargo, esta técnica no escala demasiado bien, y con más qubits la detección del estado se limita.[6]

### 5.2.3 Rydberg Sculpting

Esta es una nueva técnica que permite poner un átomo que se encuentra muy excitado (átomo de Rydberg) en muchos estados energéticos diferentes simultáneamente. Las aplicaciones de esta nueva técnica permitirán perfeccionar los actuales diseños de computadores cuánticos, que hoy día trabajan en base a qubits de dos estado. Con este nuevo método, presentado el 27 de mayo de 1999 en la Conferencia de laser y Electro-óptica de Baltimore, un pulso laser constituido por una superposición de diferentes longitudes de onda (diferentes energías) impacta el átomo que obliga a los electrones del átomo a moverse en un complejo patrón dado por el haz laser. La importancia de la técnica es que permite controlar este movimiento de electrones. [6]

## 6. CONCLUSIONES

La computación cuántica maneja los qubits, estos qubits gracias a los principios de la física cuántica, abre puertas que con la computación clásica se veía imposible, se podría hacer cálculos que llevarían miles de millones de años a las computadoras clásicas, gracias a la superposición y paralelismo con una computadora cuántica se haría en unos segundos.

Las computadoras cuánticas tienen como principal problema el aislamiento del qubits, ya que el qubit es muy sensible al manejo y las radiaciones, es necesaria mantener al qubit completamente aislado, para solucionar este problema los científicos proponen los siguientes métodos la trampa iónica, resonancia magnética molecular y Rydberg Sculpting, esto hace muy difícil imaginar que aspecto tendrá el futuro computador cuántico.

## 7. REFERENCIAS

[1] Computing fundamentals " Quantum computing"

[2] http://whatis.techtarget.com/definition/0,,sid9_gci332254,00.html

[3] Alejandro Gutiérrez Vicario "Computación cuántica" www.lcc.uma.es/~pastrana/EP/trabajos/50.pdf

[4] Stanford encyclopedia of philosophy "Quantum Computing" http://plato.stanford.edu/entries/qt-quantcomp

[5] Claudia Lizet Mayda tesis "Efectos de la computación cuántica en la tecnología ", disponible en la biblioteca de la carrera de informática, código T.1020

[6] Alejandro Oliva "La revolución de la nanotecnología: Computación Cuántica" http://blogs.creamoselfuturo.com/nano-tecnologia/2007/05/16/la-revolucion-de-la-nanotecnologia-la-computacion-cuantica/

[7] Sergi Baila Martínez "Computación cuántica" http://www.sargue.net/fitxers/quantum-es.pdf

[8] Leonel Morales Díaz "Computación cuántica www.tec.url.edu.gt/boletin/URL_12_SIS01.pdf