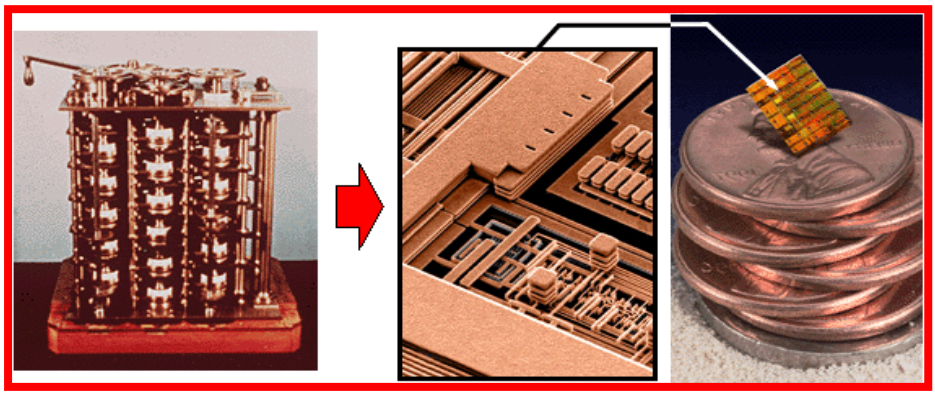
COMPUTACIÓN CUÁNTICA

Alejandro Gutiérrez Vicario
DNI: 74877186 - L
1º A de Gestión

INTRODUCCIÓN

A lo largo de la historia el ser humano ha usado diversos materiales y utilizado múltiples mecanismos en el diseño, construcción y operación de máquinas que agilicen y automaticen la realización de cálculos y el procesamiento de información, desde el ábaco hasta los ordenadores personales de hoy en día.

En los últimos años la densidad de los circuitos electrónicos ha aumentado sin cesar, gracias a la disminución en el tamaño de los componentes. Pero llegará un momento en que no sea posible reducir más los circuitos. Debido a que muy pronto la miniaturización será tal que las leyes de la física clásica ya no sean válidas, entonces se entrará en los dominios del mundo subatómico, y aquí es donde entra la mecánica cuántica.



A la izquierda una máquina de engranajes, a la derecha un chip de la IBM de 0.25 micras.

El cambio en los componentes fundamentales de las computadoras, hace necesario redefinir muchos elementos de la computación actual, la arquitectura, los algoritmos, y los componentes de hardware. Es así como nace la computación cuántica y con ella los algoritmos cuánticos.

La aplicabilidad de la computación cuántica depende de la posibilidad de desarrollar una computadora cuántica. Un ejemplo del inmenso poder de las computadoras cuánticas es el algoritmo cuántico para determinar si un número es primo. Una computadora actual tardaría miles de millones de años (dependiendo de cuan grande sea el número) en ejecutar tal algoritmo; a diferencia de una computadora cuántica a la que le tomaría tan sólo unos cuantos segundos el completar la tarea.

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 (bit cuántico), 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.

La computación cuántica está basada en las interacciones del mundo atómico, y tiene elementos como el bit cuántico, las compuertas cuánticas, los estados confusos, la teleportación cuántica, el paralelismo cuántico, y la criptografía cuántica. Una arquitectura cuántica, muy aceptada entre los investigadores y orientada a ser compatible con las actuales arquitecturas, cuenta con memoria y una unidad de procesamiento aritmético/lógico, y con elementos cuánticos como la teletransportadora de código y el planificador dinámico.

FUNDAMENTOS DE LA COMPUTACIÓN CUÁNTICA.

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.

La computación cuántica 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 rotación 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 del spin de las partículas son los que han recibido el nombre de qubits (bits cuánticos).

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 ó 1 claramente determinado. Esta es la ventaja que tiene la computación cuántica respecto a la clásica: La lógica de un bit es 0 ó 1, mientras que un qubit entraña el concepto de ambos a la vez. Si tomamos por ejemplo dos bits, sus estados posibles son cuatro: 00, 01, 10, 11. Son necesarios cuatro pares de bits para representar la misma información que un solo par de qubits con comportamiento ambiguo.

Los qubits pueden representar en este caso cuatro números a la vez, cuatro respuestas posibles a la vez, sinónimo de procesamiento paralelo real. Sus aplicaciones principales entran en el campo de la criptografía, análisis de gigantescos volúmenes de información, etc.

La computación cuántica, aprovecha la superposición cuántica, para lograr el paralelismo cuántico y el paralelismo cuántico masivo.

ELEMENTOS BASICOS DE LA COMPUTACIÓN CUÁNTICA.

El bit cuántico "qubit"

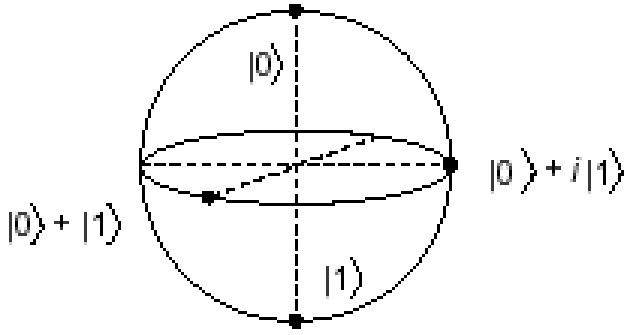
Un **qubit** (del inglés *qubit*, de *quantum bit*) es un estado cuántico en un espacio vectorial complejo bidimensional. Un qubit es la unidad mínima de información cuántica. Sus dos estados básicos se llaman, convencionalmente, |0> y |1> (se pronuncian: ket cero y ket uno). Un estado qubital puro es una superposición cuántica de esos dos estados. Esto es significativamente distinto al estado de un bit clásico, que puede asumir solamente un valor 0 ó 1.

Sin embargo, la diferencia más importante entre un qubit y un bit clásico no es la naturaleza continua de este estado (que se puede replicar con cualquier cantidad análoga), sino que múltiples qubits pueden experimentar un entrelazamiento o enredo cuántico ("Entanglement"). El enredo es una interacción no local que permite a un conjunto de qubits expresar superposiciones de diferentes cadenas binarias (01010 y 11111, por ejemplo) simultáneamente. En este "paralelismo cuántico" está la posible potencia del cómputo cuántico.

Varios qubits juntos forman un registro de qubits. Las computadoras u ordenadores cuánticos realizan cálculos manipulando qubits.

También es posible un sistema de tres estados, llamado cutrit, cuyos estados se denominan, convencionalmente, |0>, |1> y |2>.

Un qubit no puede ser clonado, no puede ser copiado, y no puede ser enviado de un lugar a otro.



Representación de cuatro estados diferentes de un qubit.

Compuertas cuánticas.

Las compuertas lógicas son operaciones unarias sobre qubits. La compuerta puede ser escrita como $P(\theta)=|0><0| + \exp(i\theta) + |1><1|$, donde $\theta = \omega t$. Aquí dos compuertas cuánticas elementales:

$I \equiv |0><0| + |1><1|$ = identidad

$X \equiv |0><1| + |1><0|$ = NOT

Donde I es la identidad, X es el análogo al clásico NOT.

Estas compuertas forman parte de uno de los más pequeños grupos de la computación cuántica. La tecnología de la física cuántica puede implementar esas compuertas eficientemente. Todos excepto el CNOT operan en un simple qubit; la compuerta CNOT opera en dos qubits.

Entrelazamiento cuántico ó "Entanglement"

La capacidad computacional de procesamiento paralelo de la computación cuántica, es enormemente incrementada por el procesamiento masivamente en paralelo, debido a una interacción que ocurre durante algunas millonésimas de segundo. Este fenómeno de la mecánica cuántica es llamado "entanglement".

Debido al "entanglement", dos partículas subatómicas, permanecen indefectiblemente relacionadas entre si, si han sido generadas en un mismo proceso. Estas partículas forman subsistemas que no pueden describirse separadamente. Cuando una de las dos partículas sufre un cambio de estado, la otra lo sufre automáticamente. Y eso ocurre de forma instantánea y con independencia de la distancia que las separe en ese momento. Esta característica se desencadena cuando se realiza una medición sobre una de las partículas.

Hoy en día se buscan aplicaciones tecnológicas para esta propiedad cuántica. Una de ellas es enviar mensajes, realmente indescifrables, uniendo entrelazamiento y el principio de indeterminación de Heisenberg (que afirma que no se puede determinar, simultáneamente y con precisión arbitraria, ciertos pares de variables físicas, como son, por ejemplo, la posición y la cantidad de movimiento de un objeto dado).

Teleportación cuántica.

La teleportación cuántica ha sido descrita como la posibilidad de *"transmitir qubits sin enviar qubits"*. En la computación tradicional para transmitir bits, estos son clonados o copiados y luego enviados a través de diferentes medios como el cobre, fibra óptica, ondas de radio y otros. En la computación cuántica no es posible clonar, copiar, o enviar qubits de un lugar a otro como se hacen con los bits.

Si enviamos un qubit $|0\rangle$ (ket cero) donde 0 es un estado desconocido, el receptor no podrá leer su estado con certidumbre, cualquier intento de medida podría modificar el estado del qubit, por lo tanto se perdería su estado, imposibilitando su recuperación. La teleportación cuántica, resuelve este problema, esta se basa en el "entanglement" para poder transmitir un qubit sin necesidad de enviarlo. El emisor y el receptor poseen un par de qubits "enredados" (entangled). Entonces el qubit es transmitido desde el emisor, desaparece del emisor y en el receptor reaparece el qubit . Este fenómeno es posible debido a un mecanismo conocido como el efecto EPR (Einstein Podolsky Rosen). En la teleportación cuántica primero dos qubits E y R son "enredados" y luego separados (entangled), el qubit R es ubicado en el receptor y el qubit E es ubicado en el emisor junto al qubit original Q a ser transmitido, al realizar la lectura del estado de los dos qubits Q y E, estos cambian su estado a uno aleatorio debido a la interacción. La información leída es enviada al receptor, donde esta información es utilizada para un tratamiento que es aplicado al qubit R, siendo ahora R una réplica exacta del qubit Q.

Paralelismo cuántico.

La superposición cuántica permite un paralelismo exponencial o paralelismo cuántico en el cálculo, mediante el uso de las compuertas lógicas de qubits.

Con una compuerta lógica de un qubit, cuando el qubit de entrada tiene en el estado una superposición igual de $|0\rangle$ y $|1\rangle$, el estado resultante es la superposición de los 2 valores de salida.

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

Esto hace que los ordenadores cuánticos sí sean eficaces en el cálculo de periodos, hasta el punto de que se reduce a un tiempo polinómico lo que requeriría un número exponencial de pasos en una máquina clásica.

Criptografía cuántica

La criptografía cuántica es una de las primeras aplicaciones de la computación cuántica cercana a una fase de producción masiva. La criptografía cuántica garantiza absoluta confidencialidad de la información transmitida por fibras ópticas, almacenando información en el elemento constituyente de la luz, el fotón.

La criptografía (del griego *kryptos*, "ocultar", y *grafos*, "escribir", literalmente "escritura oculta") es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Los diferentes métodos de criptografía actualmente utilizados necesitan que dos personas que deseen comunicar información intercambien de forma segura una o más claves; de manera que el punto donde hay menor seguridad en el intercambio de información confidencial está en el proceso de intercambio y transmisión de las claves.

La criptografía cuántica nace en los años ochenta. La transmisión se logra utilizando fotones individuales (cuantos de luz) enviados entre el emisor y el receptor mediante una fibra óptica. El *teorema de no-clonación* garantiza que es imposible reproducir (clonar) la información transmitida sin conocer de antemano el estado cuántico que describe la luz. Un interceptor que intente leer el mensaje enviado sólo podría destruir la información transmitida, sin poder reproducirla, perturbándola de tal forma que los interlocutores de la comunicación se darían cuenta de lo que se intenta hacer.

Como ejemplo está el sistema criptográfico de clave pública RSA; los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10^{100}) elegidos al azar para conformar la clave de descifrado. La seguridad de este algoritmo radica en que no hay maneras rápidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales.

El tiempo que requeriría el realizar la factorización se estima en aproximadamente $4x10^{16}$ años. Los algoritmos cuánticos de factorización, se estima que realizarían este cálculo en segundos.

COMPUTADORA CUÁNTICA

Una definición acerca de las computadoras cuánticas, ampliamente aceptada por los investigadores, la concibe como un sistema de circuitos cuánticos, actuando en un espacio de estados.
El circuito es una secuencia de transformaciones unitarias seguido por una medición. Esas transformaciones, son llamadas compuertas cuánticas, y son controladas por una computadora clásica. Así esto permite la superposición simultánea de estados básicos (correspondientes a estados clásicos "0" y "1").

Hardware cuántico

Requerimientos de implementación.

Aún no se ha resuelto el problema de qué hardware sería el ideal para la computación cuántica. Se ha definido una serie de condiciones que debe cumplir, conocida como la lista de Di Vinzenzo, y actualmente hay varios candidatos a qubits.

Requisitos a cumplir:

- El sistema ha de poder inicializarse, esto es, llevarse a un estado de partida conocido y controlado.
- Ha de ser posible hacer manipulaciones a los qubits de forma controlada, con un conjunto de operaciones que forme un conjunto universal de puertas lógicas (para poder reproducir a cualquier otra puerta lógica posible).
- El sistema ha de mantener su coherencia cuántica a lo largo del experimento.
- Ha de poder leerse el estado final del sistema, tras el cálculo.
- El sistema ha de ser escalable: tiene que haber una forma definida de aumentar el número de qubits, para tratar con problemas de mayor coste computacional.

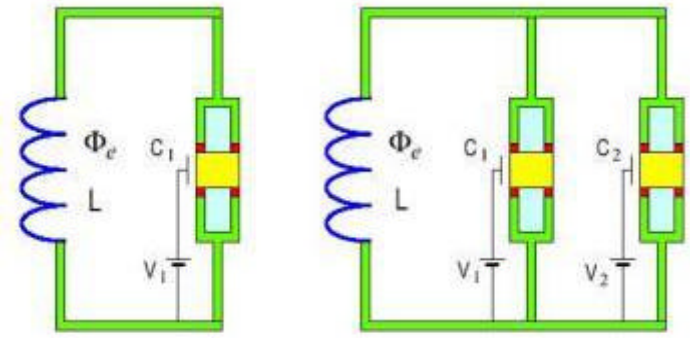
Candidatos a qubits:

- Espines nucleares de moléculas en disolución, en un aparato de RMN.
- Flujo eléctrico en SQUIDs.
- Iones suspendidos en vacío.
- Puntos cuánticos en superficies sólidas.
- Imanes moleculares en micro-SQUIDs.

Circuitos para la computación cuántica.

Los investigadores afirman que en la computación cuántica se usarán los principios de la mecánica cuántica, para realizar cálculos complejos en una fracción del tiempo necesario hoy en día en los superordenadores más veloces.

A medida que avanza la teoría al respecto, los expertos van proponiendo avances que permitirán que esta idea se haga realidad. Bajo estas líneas se propone un circuito realizable de forma experimental y una manera eficiente de implementar una computación cuántica escalable.



Es precisamente la habilidad de aumentar la escala de la tecnología, de aquella que permite realizar experimentos de 1 ó 2 qubits, habituales en el laboratorio, a la que nos proporcionará sistemas en los que participarán muchos qubits, lo que hará posible construir un ordenador cuántico.

Software cuántico

Dado que el tratamiento de la información cuántica es notablemente distinto del de la clásica, se necesitaran algunas herramientas para construir los programas cuánticos.

Existen tres cosas básicas en el software cuántico: Un conjunto apropiado de puertas, algoritmos que aprovechen el comportamiento cuántico y disponer de métodos apropiados para controlar los posibles errores.

1- Una forma de obtener puertas cuánticas es la cuantización de las puertas clásicas, que pasa por reinterpretar los bits como qubits.
Se puede demostrar que el conjunto de puertas cuánticas que afectan a un sólo qubit, conjuntamente con las puertas llamadas control-not (que afectan a dos qubits), forman un conjunto universal con las que se puede construir cualquier programa cuántico.

2- A pesar del esfuerzo que se ha dedicado a la obtención de algoritmos que aprovechen el comportamiento cuántico, en la actualidad, su número es reducido.
Ya se ha mencionado que aunque mediante superposiciones apropiadas, es posible manejar un número exponencial de estados, eso no supone que esta información esté disponible. Para acceder a esa información debemos medir sobre el estado colapsándolo, y la información se pierde casi en su totalidad. Para aprovechar los aspectos cuánticos, debemos combinar la posibilidad del paralelismo cuántico con la interferencia.

3- Quizás es éste uno de los mayores problemas a la hora de construir un ordenador. Estos errores provienen de la inexorable interacción del ordenador con su entorno, proceso denominado decoherencia.
Se pensó que no podían existir métodos para el control de errores cuánticos, pero se ha mostrado cómo es posible contener los errores mediante códigos cuánticos correctores de errores. Estos códigos, detectan y corrigen estos errores, usando sofisticadas técnicas cuánticas.

En resumen, la ventaja en la potencia de estas máquinas proviene del paralelismo masivo (exponencial) debido a la superposición de estados en los qubit. Si estos ordenadores fueran factibles en la práctica, permitirían atacar problemas que en los ordenadores clásicos implicarían tiempos astronómicos.

Aparte de las aplicaciones encaminadas a la ciencia básica, estos ordenadores podrían usarse en la criptografía, criptoanálisis, búsquedas en inmensas bases de datos, simulaciones meteorológicas, etc.

Queda por saber si el aislamiento de los sistemas permitirá escapar al límite impuesto por el decaimiento y la decoherencia que destruyen la mezcla cuántica de estados.

Otro de los problemas principales es la escalabilidad, especialmente teniendo en cuenta el considerable incremento en qubits necesarios para cualquier cálculo que implica la corrección de errores. Para ninguno de los sistemas actualmente propuestos es trivial un diseño capaz de manejar un número lo bastante alto de qubits para resolver problemas computacionalmente interesantes hoy en día.

Conclusiones.

Los ordenadores cuánticos se basan en el uso de los qubits (bits cuánticos) en lugar de bits, y da lugar a nuevas puertas lógicas que hacen posibles nuevos algoritmos.

Poseen una capacidad de cálculo muy superior a los computadores actuales gracias al paralelismo masivo (exponencial) debido a la superposición de estados en los qubit.

En el campo de la criptografía proponen un nuevo enfoque: control absoluto de seguridad a nivel de comunicación y su capacidad para realizar operaciones de factorización (descomposición en números primos), que representa una amenaza para las comunicaciones encriptadas que emplean muchas instituciones en sus sistemas de seguridad, y que se basan a su vez en la dificultad de hacer códigos.

Y decir que la computación cuántica es un campo en el que aún queda mucho por descubrir.

Bibliografía

http://es.wikipedia.org/wiki/Portada

http://www.babab.com/no12/ordenadores.htm

http://www.el-mundo.es/navegante/2000/08/16/ibm.html

http://www.monografias.com/trabajos14/computadoras-cuanticas/computadoras-cuanticas.shtml

http://www.webzinemaker.com/admi/m6/page.php3?num_web=1604&rubr=4&id=10460

http://www.tendencias21.net