ÍNDICE

INTRODUCCION

A mediados de los años 40 comenzaron a aparecer los primeros ordenadores. Aquellos primeros artefactos eran muy lentos y ocupaban varias habitaciones llenas de armarios. Cincuenta años después hemos llegado a construir ordenadores portátiles con el tamaño de un bloc de notas que superan con creces la potencia de aquellos gigantes. Pero aun así, la carrera por la miniaturización continua y el siguiente paso hacia el que nos movemos es la construcción de ordenadores cuyas piezas sean átomos o moléculas: los ordenadores cuánticos o moleculares.

Avances recientes en las aplicaciones físicas asociados a las tecnologías de la información basados en las propiedades de los componentes de la luz (fotones), y de la materia (electrones), así como en la aplicación de las leyes de la naturaleza a este nivel (los principios de la mecánica cuántica), nos permiten prever para las próximas décadas un avance importante en los límites de la computación y las comunicaciones. Se abrirán así grandes posibilidades para la humanidad en el siglo XXI.

La computación cuántica es un área muy reciente de investigación, con menos de dos décadas de desarrollo, pero que sin embargo ha tenido un impulso muy fuerte en los últimos años. Aunque todavía no hay ordenadores cuánticos, sólo hay pequeños prototipos, modestos procesadores de información cuántica.

Una computadora cuántica deriva su potencia de ciertas propiedades cuánticas de los átomos o núcleos que les permiten funcionar como bits cuánticos, o "qubits", y servir simultáneamente de procesador y memoria en la computadora. Dirigiendo interacciones entre qubits aisladas del entorno externo, los científicos pueden hacer que una computadora cuántica realice ciertos cálculos en forma exponencialmente más rápida que las computadoras convencionales.

HISTORIA

Cuando teóricos propusieron por primera vez el concepto de las computadoras cuánticas en las décadas de 1970 y 1980, muchos científicos dudaron que alguna vez ese tipo de computadora pudiera resultar práctica. Pero en 1994, Peter Shor, de AT&T Research, describió un algoritmo cuántico específicamente diseñado para factorizar números grandes y exponencialmente más rápido que las computadoras convencionales, lo suficientemente rápido como para birlar la seguridad de muchos criptosistemas de clave pública. El potencial del algoritmo de Shor alentó a muchos científicos a tratar de explotar las capacidades de las computadoras cuánticas. En los últimos años, varios grupos de investigación de todo el mundo han alcanzado progresos significativos en este campo.

Isaac Chiang dirigió el grupo que demostró la primera computadora cuántica de 1 qubit (en 1998 en la Universidad de California en Berkeley). En IBM Almaden, Chuang y sus colegas fueron los primeros en demostrar los importantes algoritmos cuánticos, el algoritmo de Grover concebido en 1999 para hacer búsquedas en bases de datos con ayuda de una computadora cuántica de 3 qubits, y la búsqueda de pedidos con una computadora cuántica de 5 qubits. La factorización con el algoritmo de Shor es el algoritmo más complejo que se haya demostrado hasta ahora usando una computadora cuántica.

Los científicos de IBM fueron pioneros en criptografía cuántica, en comunicaciones cuánticas (incluso el concepto de teleporte cuántico) y en metodologías eficientes para corregir errores. David DiVincenzo, miembro del cuerpo de investigadores del laboratorio Watson de IBM, ha promulgado los cinco criterios necesarios para construir una computadora cuántica práctica:

1) un sistema físico de escala flexible con qubits bien caracterizados;
2) capacidad de inicializar el estado de un qubit;
3) tiempos de descoherencia más largos que el tiempo de operación de la puerta cuántica;
4) un conjunto universal de puertas cuánticas; y
5) la capacidad de medir qubits específicos.

LIMITES FÍSICOS

La velocidad y el tamaño de los micros están íntimamente relacionadas ya que al ser los transistores más pequeños, la distancia que tiene que recorrer la señal eléctrica es menor y se pueden hacer más rápidos. Al ser los transistores cada vez más pequeños la cantidad de ellos contenidos en un microprocesador, y por consiguiente su velocidad, ha seguido la "ley de Moore", según la cual el poder de los procesadores se duplica cada 18 meses. Pero los estudios revelan que este ritmo no se puede mantener y que el límite será alcanzado tarde o temprano, ya que si se reduce más, las interferencias de un transistor provocarían fallos en los transistores adyacentes.

Con el fin de superar estos límites de tamaño y velocidad se está trabajando en la actualidad en varios centros de investigación de todo el mundo en líneas que pueden revolucionar el mundo de la informática: *Los ordenadores cuánticos.*

Fecha	Reglas de diseño
1970	20 micras
1975	10 micras
1978	4,5 micras
1980	2 a 3 micras
1996	0.35 micras
1997	0.25 micras
1999	0.18 micras

Evolución de las Reglas de diseño de los circuitos integrados.

MECANICA CUANTICA

A una escala del orden del micro- al nano-metro, la materia (los átomos y moléculas que los componen) no se comporta al modo clásico, esto es satisfaciendo las ecuaciones de movimiento que son válidas para objetos tales como manzanas, cohetes o bolas de billar, sino que su comportamiento es descrito por las leyes de la mecánica cuántica, y describiendo un comportamiento muy diferente al supuesto clásicamente, pero corroborado por los experimentos una y otra vez.

Para apreciar cómo podría actuar un ordenador cuántico, abordemos el siguiente fenómeno, descrito por la mecánica cuántica:

La dualidad onda-partícula significa que bajo ciertas condiciones, objetos (partículas) considerados normalmente como sólidos, se comportan como si fueran ondas (sonido ó luz), y a la inversa. En esencia la mecánica cuántica establece los tipos de ondas asociados a los distintos tipos de partículas, y recíprocamente.

La primera consecuencia de la dualidad onda-partícula es que los sistemas atómicos, como los átomos y sus partículas constituyentes, sólo pueden existir en estados de energía discretos. Así, cuando un átomo salta de un estado de energía a otro, absorbe o emite energía en cantidades exactas, llamadas cuántos de luz ó fotones, que podrían considerarse las partículas que componen la luz.

Una segunda consecuencia es que las ondas mecano cuánticas, como las ondas de agua, pueden superponerse; tomadas individualmente, estas ondas describen la posición de las partículas que representan, pero al combinar dos o más de tales ondas, la posición de la partícula se vuelve incierta, de forma que, por ejemplo, un electrón puede en ocasiones encontrarse en dos lugares al mismo tiempo.

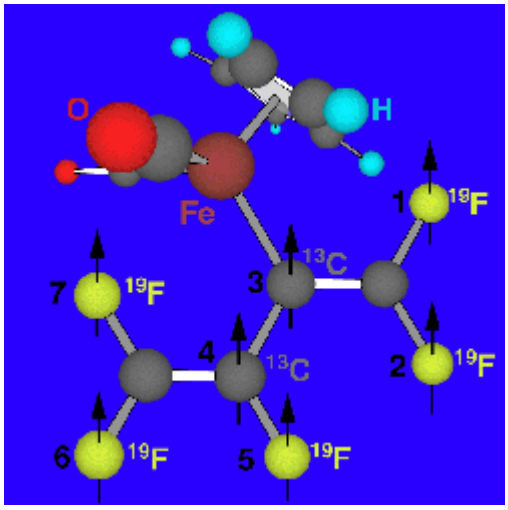
Finalmente, los conceptos de coherencia y de decoherencia, que juegan un importante papel en la descripción de sistemas cuánticos: el primero de ellos se refiere al proceso por el que dos ondas cuánticas superpuestas se comportan como una sola onda; el segundo se refiere al proceso por el cual dos ondas coherentes recuperan su respectiva identidad individual diciéndose que hay decoherencia.

QUBITS

La Mecánica cuántica afirma que el electrón esta real y simultáneamente en los dos estados hasta que alguien mide su espín, en cuyo momento el estado colapsa a uno de los valores posibles. Por tanto el espín del electrón podría contener un bit de información, pero hasta que no se realiza la medida no se decide que valor toma ese bit, que recibe el nombre de ¨qubit¨ (de ¨bit cuantico¨).

Los espines de dos electrones pueden estar en cuatro estados diferentes (almacenara dos qubits) y los de diez electrones se combinarían de 1024 formas posibles (equivalen a 10 qubits).

Sabemos que la información se representa en piezas discretas, al igual que los niveles energéticos de los átomos. La unidad básica de información es el bit. Desde un punto de vista físico, un bit es un sistema con dos estados, pudiendo ser preparado en uno de estos estados, que representan dos valores lógicos: sí ó no, 1 ó 0. Por ejemplo, en los ordenadores digitales, estaría representado por el valor del voltaje que adquieren las placas de un condensador. Así, 1 sería un valor de "a " volts, y 0 un valor de "b" volts. Pero un bit puede también ser representado por dos diferentes polarizaciones de la luz, o por dos estados electrónicos de un átomo. Ahora la mecánica cuántica nos dice que si un bit puede estar en cualesquiera dos estados distinguibles, también puede estar en cualquier superposición coherente de ellos, y claro, estos son más estados, que no tienen análogos clásicos, y en los cuales un átomo representa ambos valores 0 y 1 simultáneamente (y este comportamiento es propio de los sistemas atómicos). Es a esta representación, que puede tomar los dos valores 0 ó 1en proporciones arbitrarias, pero simultáneamente, a lo que se llama qubit ó unidad de información cuántica.



Molecula de IBM de 7 qubits. –
Computadora cuantica mas avanzada del mundo

¿Es esto un avance respecto al bit?

Veamos un ejemplo: consideremos un registro compuesto por tres bits. Un registro de tres bits clásicos podría tomar una de las 8 configuraciones posibles, 000,001,010,... , 111, representando los números del 0 al 7. Pero un registro cuántico de tres qubits podría almacenar simultáneamente hasta las 8 configuraciones en una superposición cuántica. Esto no es más sorprendente que el hecho de que los números 0 y 1 estén ambos presentes en el mismo qubit. Así, si añadimos más qubits al registro, su capacidad aumenta de forma exponencial: 4 qubits podrán almacenar 16 números diferentes a la vez, y en general X qubits podrán almacenar hasta 2*2*. x....*2 =2^X a la vez.

Ahora para estimar su potencia, se pueden hacer cálculo cuántico; de esta forma una vez que se ha preparado un registro en una superposición de varios números diferentes, se pueden realizar operaciones matemáticas de todos ellos a la vez. De hecho se ha probado que un ordenador con un tipo de registros cuánticos como los presentados anteriormente puede realizar en un mismo paso computacional la misma operación matemática que la que se realizaría con 2L inputs de números. En cambio para realizar la misma tarea, un ordenador clásico debería repetir el cálculo 2L veces, o debería utilizar 2L procesadores diferentes trabajando en paralelo. Esto representa una notable ganancia en el uso de recursos computacionales, tales como tiempo y memoria.

ORDENADORES CUANTICOS

Un computador Cuántico realiza las operaciones en bits cuánticos, llamados qubits. Un qubit al igual que un bit clásico puede estar en dos estados, cero o uno. El qubit se diferencia del bit clásico en que, debido a las propiedades de la mecánica cuántica, puede estar simultáneamente en ambos estados. Un qubit que contiene los valores cero y uno a la vez se dice que está en superposición de los estados cero y uno. Este estado de superposición es persistente hasta que el qubit es externamente medido. Al medir un qubit, su estado se ve forzado a tomar un solo valor. Porque la medición determina el valor del qubits, los posibles estados que existen deben describirse antes de realizar la medición en términos de su probabilidad de ocurrencia.

Un ordenador cuántico funcionaría asociando el conocido carácter discreto del procesamiento de información digital (esto es, los bits) con el extraño carácter de la mecánica cuántica (niveles finitos de energía, estados atómicos discretos). Así, una hilera de átomos de hidrógeno podría alojar qubits igual de bien que alojan bits una serie de condensadores. Un átomo en estado fundamental electrónico (el menor estado discreto de energía) podría ser la codificación de un 0, y en estado excitado un 1.Pero para que tal sistema cuántico pueda funcionar como un ordenador, no se debe limitar a almacenar qubits, sino que quien lo maneje ha de ser capaz de introducir información en el sistema, ha de procesar tal información mediante manipulaciones lógicas simples, y ha de poder devolver la información procesada: en conclusión han de poder leer, escribir y efectuar operaciones aritméticas.

La superposición cuántica, permite que un registro que contiene M qubits pueda representar 2^M valores simultáneos. Al realizar un cálculo usando este registro se producen todos los resultados posibles para los 2^M valores de entrada obteniendo así un paralelismo exponencial. Sin embargo para leer los resultados de un cálculo los qubits deben ser medidos. Esta medida fuerza a que el qubit tome un valor particular y se destruya el estado paralelo (descoherencia). El desafío es entonces inventar cálculos cuánticos donde una propiedad pueda derivarse del estado paralelo en un tiempo no exponencial antes de realizar una medida.

HARDWARE

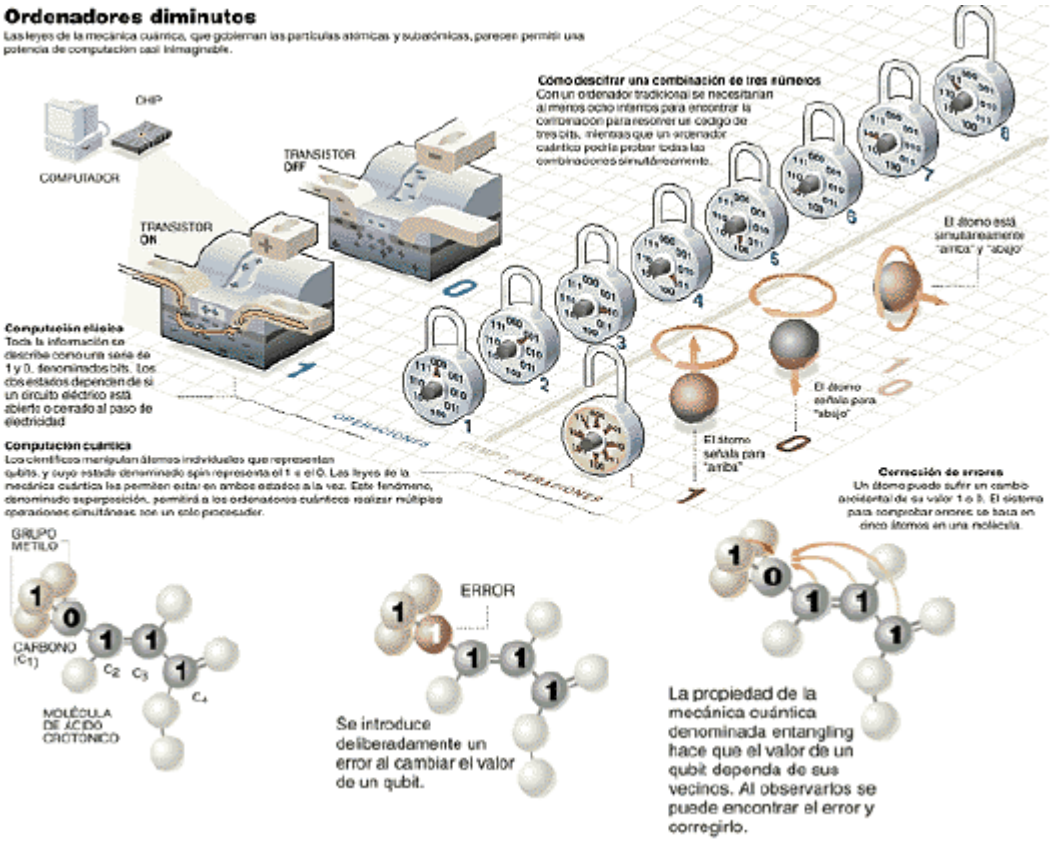
Hoy se sabe como leer y escribir información en sistemas cuánticos; veamos los procesos de lectura, escritura y un problema no resuelto.

- Escritura. Aplicado a átomos de hidrógeno, el método consiste en lo siguiente: imaginemos un átomo de hidrógeno en su estado fundamental, en el que posee una cantidad de energía E_0.Para escribir un bit 0 en este átomo no se actúa físicamente sobre él. Para registrar un 1 en él, excitamos el átomo hasta un nivel energético superior E_1.Esto se consigue bañándolo en luz láser compuesta por fotones cuya energía sea igual a la diferencia entre E_1 y E_0. Si el haz láser posee la intensidad adecuada y se aplica durante el tiempo necesario, el átomo pasa gradualmente desde el estado fundamental al excitado, al absorber el electrón del átomo un fotón. Si el átomo se encuentra ya en el estado excitado, el mismo pulso lumínico provocará que emita un fotón y regrese al estado fundamental.

Desde el punto de vista del almacenamiento de información, el pulso le dice al átomo que invierta el estado de su bit (y no qubit, porque sólo puede estar, en este caso de intensidad y frecuencias adecuadas, en uno sólo de los estados). Ahora si aplicamos el láser de la energía precisa para estos dos niveles, pero se hace en la mitad de tiempo necesario para llevar al átomo desde el estado 0 al 1, el átomo se hallará en un estado que será la superposición de la onda correspondiente al 0 y de la onda correspondiente al 1: es el qubit.

- Lectura. En un sistema cuántico sería parecida a la escritura: se empuja al átomo hasta un estado energético todavía más elevado y menos estable, E_2. Esto lo hacemos sometiendo al átomo a luz láser de energía igual a la diferencia entre E_1 y E_2; si el átomo se encuentra en E_1, se excitará hasta E_2, pero retornará rápidamente a E_1 emitiendo un fotón. Si el átomo se encuentra ya en el estado fundamental, nada ocurre. Si se halla en el estado superpuesto de 0 y 1, tiene iguales probabilidades de emitir un fotón, revelando que es un 1, como de no emitirlo, indicando que es un 0.

- Errores: Corrección de error cuántico. Los distintos sistemas que podrían utilizarse para el registro y procesamiento de información son sensibles al ruido (perturbaciones del medio) que puede invertir bits de modo aleatorio. Los métodos clásicos de corrección de errores, (dispositivo flip-flop) entrañan la medición de bits para ver si son erróneos, lo que en un ordenador cuántico provocaría decoherencia. A tenor de esto, se esta desarrollando toda una teoría sobre posibles alternativas para corregir estos defectos, la corrección de error cuántico.



Pero, ¿qué ocurre con las operaciones aritméticas que pudieran realizar los ordenadores cuánticos?.

Sabemos que si un ordenador digital(clásico) posee puertas Lógicas (esto es, circuitos que realizan operaciones elementales), como la AND, la NOT y la OR, entonces puede llevar a cabo cualquier operación lógico-aritmética. Pues bien, a un ordenador cuántico se le debería pedir lo mismo. De hecho, operaciones de lógica cuántica elemental se han demostrado posibles en experimentos, durante los últimos 50 años. Por ejemplo, la operación NOT no es más que una transición simulada entre dos niveles de energía E1 y E0; la operación XOR se puede identificar como una transición controlada en un sistema cuántico de cuatro niveles.

Sin embargo, si se quiere construir un ordenador cuántico real, es necesario encontrar un sistema que sea suficientemente controlable para permitir la implementación de puertas lógico-cuánticas (la versión cuántica de las puertas lógicas actuales), y todavía en estos días, es muy complicado el almacenar varios cubits de información en un sistema cuántico, que permitan su manipulación.

Las dificultades se presentan, puesto que es difícil el hallar estos sistemas controlables. Los candidatos iniciales (esto es, los dispositivos cuánticos)se fabricaban sobre microchips de estado sólido (siendo ésta la progresión lógica de las técnicas de microfabricación que han permitido incrementar la potencia de los actuales ordenadores). Sin embargo las operaciones cuánticas presentan complicados efectos de interferencia y de ruido. Que se sepa ningún sistema cuántico está realmente aislado del medio, y el acoplamiento a este medio produce la temida decoherencia, que destruye la superposición de los estados contruidos.

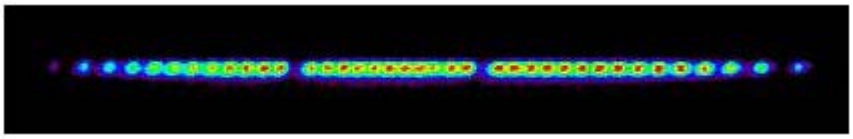
Por ejemplo en estos dispositivos de estado sólido, el medio sería el substrato sobre el que se asienta el dispositivo cuántico, y el acoplamiento a este substrato es tan fuerte que produce tiempos de decoherencia típicos del orden del picosegundo. Y claro, esto no es suficiente, pues aunque tengamos dos estados diferentes, que sean estables, precisamos también que superposiciones de estos dos estados conserven su entidad durante tiempos E_1 y E_0 comparables, y es aquí donde el tiempo de escala de decoherencia es tan corto.

LA CONSTRUCCION DEL ORDENADOR CUANTICO.

En principio se sabe como construir un ordenador cuántico: se comienza por puertas lógico-cuánticas que se va uniendo e integrando junto a la circuitería cuántica(cables cuánticos y buses apropiados). Sin embargo cuando el número de puertas cuánticas(recordar, la versión cuántica de las puertas lógicas actuales) en la red se incrementa, se manifiesta una mayor interacción entre los cubits, con el consiguiente riesgo de decoherencia en los estados construidos, y por tanto de diseminación de la información por el medio, expoliando el cálculo. La dificultad para construir el ordenador, estriba en que es preciso encontrar un sistema formado por entidades básicas (cubits) que admitan una fácil manipulación y se encuentren completamente aisladas del exterior (y de esta forma preservar el rasgo que permite realizar una misma operación sobre varias entradas (inputs) simultaneamente).

Pues bien estos sistemas no abundan; expongo a continuación los candidatos para constituir primer el ordenador cuántico(aunque humildemente se debería llamar procesador cuántico

TRAMPA DE IONES



CADENA DE IONES

Propuesto por P.Zoller y J.I.Cirac, consiste en una cadena lineal de iones(es decir, átomos ó moléculas con carga eléctrica no nula) atrapados por una configuración conveniente de campos electromagnéticos, encerrados en un recipiente aislado de campos electromagnéticos espúreos(distintos de los que permiten atrapar a los iones), y en un ambiente de alto vacío para suprimir el choque de los iones con otros átomos sueltos.

Cada uno de los iones almacena un cubit de información, correspondiéndose los valores de 0 y 1 con dos órbitas distintas de uno de los electrones del ion correspondiente.Las operaciones lógicas entre distintos cubits

se realizan enfocando luz láser sobre los iones lo que hace que cambien su órbita.Para leer el resultado se iluminan con luz de una determinada frecuencia todos los iones,y según en la órbita en la que se encuentre cada uno, emitirá luz o no,lo que permite conocer el valor del correspondiente cubit.

En los ordenadores cuánticos los cubits han de poder "comunicarse" entre ellos a la hora de crear puertas lógicas,análogas a las empleadas en los ordenadores habituales.

Por ejemplo, veamos la versión cuántica de la operación XOR en la trampa de iones. Se trata de una operación lógica entre dos cubits, en la que el 1º no cambia y el 2º pasa al estado 0, si ambos se encontraban inicialmente en el mismo estado (i.e, 00 ó 11) o al estado 1 si estaban en distinto estado(10 ó 01).

Para realizar esta operación es necesario que el primer cubit le diga al 2º en qué estado se encuentra; ha de existir, por tanto un medio de comunicación (cable cuántico) entre los cubits. En el caso de los iones la comunicación entre ellos se realiza a través del movimiento.

Imaginemos los iones dispuestos en una cadena lineal, en la que cada uno se une a los vecinos por medio de un muelle(que impide el acercamiento) y donde los átomos de los extremos permanecen unidos por sendos muelles a paredes fijas(la trampa).

Supongamos que los átomos estaban parados inicialmente; si provocamos ligeramente el movimiento de uno de ellos, éste empujará al siguiente y así hasta el último átomo, que tras rebotar en la pared empujará al anterior, etc.los átomos se pondrán a oscilar conjuntamente y cómo se muevan, dependerá de cómo se mueva el primer átomo. (Hay que indicar que este movimiento conjunto de todos los iones sólo se puede realizar en modos concretos de movimiento, y estos grados de libertad permitidos a la cadena, sirven como un único bus de cubits para transpotar la información cuántica).

Veamos cómo se comunicarían los iones: si los iones están en reposo inicialmente, iluminando uno de ellos con láser, si el ion cambia de estado los iones de la cadena empezarán a moverse(transmitiéndose la agitación del 1º al resto por medio de los "muelles"), y así dependiendo que el ion iluminado absorba o emita la luz(y por tanto su estado)se produce un tipo de movimiento o no. En resumen, según el estado en que se halle el primer ion dela cadena, el 2º se comportará de una forma u otra al enfocarle con luz láser.

Las dificultades/inconvenientes que presenta este dispositivo de cadena lineal son:

1) el enfriamiento de la cadena lineal en el estado fundamental de energía de la cadena (una temperatura sub-microKelvin!!).

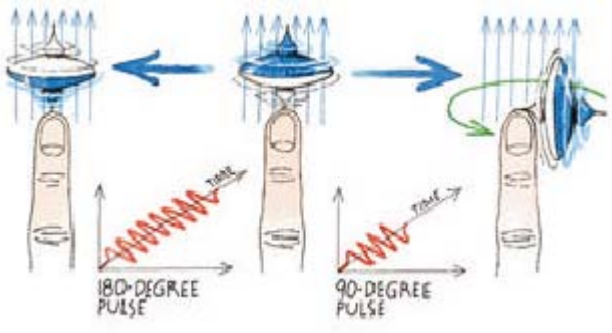
2) la velocidad a la que opera la trampa de iones,está limitada por las frecuencias de los modos vibracionales en la trampa(en recientes resultados,éstas alcanzaban los 10MHz).

RESONANCIA MAGNETICA NUCLEAR(NMR).

En este caso el procesador es una molécula, constituida por una médula de unos 10 átomos, y con otros átomos asociados a la médula por enlaces químicos (pensar en la molécula de un hidrocarburo). Ahora, es el núcleo de cada átomo de la hilera el que interesa. Cada uno de estos posee un momento magnético asociado al espín nuclear, y los estados de espín(discretos) proporcionan los cubits. Para operar sobre tal molécula, se sitúa en un campo magnético alto,que interacciona con los estados de espín del núcleo,pudiendo así ser manipulados al aplicar campos magnéticos oscilantes.

El problema que presenta esta técnica, es que el estado de espín del núcleo de una única molécula no puede ser ni preparado ni medido; para salvar este escollo, no se utiliza una única molécula, sino un recipiente con estas moléculas en estado líquido, ¡en número de 10^20!!.Es entonces cuando puede ser medido el estado de espín promedio.

En recientes experimentos, la técnica de NMR se ha utilizado para realizar cálculos con moléculas de ácido crotónico, que permitirán detectar y corregir los errores que se producen en los cálculos cuánticos.



Núcleo Magnético

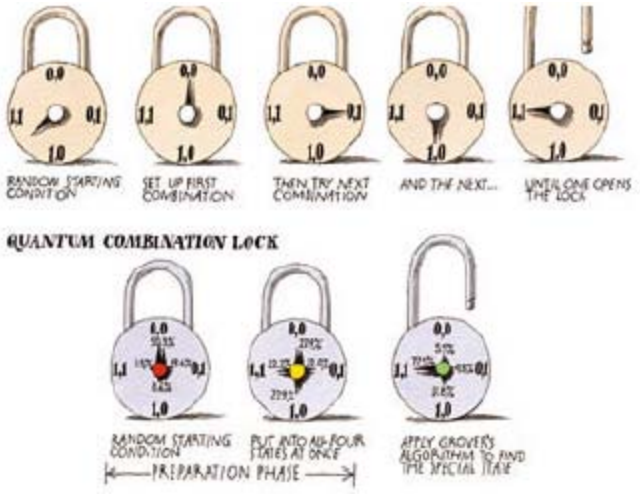
ALGORITMOS CUÁNTICOS.

Se aprecia una conexión entre mecánica cuántica y teoría de la información(la teoría subyacente a la construcción de ordenadores), que surge cuando se observa que propiedades simples de sistemas cuánticos, tales como las perturbaciones inevitables implicadas en cualquier medida del sistema cuántico, podrían tener potencial uso práctico, en la que se bautizado como la "criptografía cuántica".

Esta nueva disciplina abarca varias ideas, y entre la que está más firmemente establecida es la distribución de clave cuántica. Éste es un ingenioso método, en el cual los estados cuánticos transmitidos se usan para realizar la siguiente operación:

Establecer en dos lugares separados un par de idénticas pero aleatorias secuencias de dígitos binarios, sin permitir que una tercera parte pueda hacerse con la secuencia; Y esto es útil cuando se tiene en cuenta que una secuencia aleatoria puede ser usada como clave criptográfica para permitir comunicaciones seguras. La propiedad notable es que los principios de la mecánica cuántica garantizan un tipo de conservación de la información cuántica, de tal forma que cuando la necesaria información cuántica de la secuencia ha llegado a las partes interesadas en hacerse con una clave, pueden estar seguros que sólo ha ido a parar a ellos(y no a los espías). Ahora, de la misma forma que la potencial capacidad de estos sistemas cuánticos para garantizar la seguridad en la transmisión de información secreta, la capacidad de cálculo puede ser usada para atacar sistemas criptográficos clásicos, tales como *DES* (Data Encryption Standard) ó el *RSA* (Rivest, Shamir, Adleman).

Romper un DES requiere una búsqueda de entre 2^56 =7 x10^16 posibles claves. Si esta búsqueda puede ser comprobada a una razón de 1 millón de claves por segundo, un ordenador clásico necesitaría miles de años para hallar la clave correcta, mientras que un ordenador cuántico precisaría menos de cuatro minutos usando un algoritmo cuántico, el algoritmo de Grover.



Este algoritmo fue presentado para el problema de dado un conjunto de datos {Xi}, hallar un dato particular, X0.Esto sería similar a la búsqueda de un nº de teléfono en las entradas de un listín telefónico(recordar el algoritmo de búsqueda visto en prácticas). Pues bien, frente a los algoritmos clásicos que requieren un a media de N/2 pasos, el algoritmo de Grover requiere del orden de N^1/2.

Hay otros dos algoritmos que mejoran notablemente el tiempo de cálculo de frente a los análogos clásicos, el algoritmo de factorización de Shor y el algoritmo de búsqueda del periodo de una función.

Pero, ¿es posible realizar estos cálculos cuánticos?.

Hay que indicar que, los efectos de interferencia cuántica que permiten algoritmos como el de factorización de Shor son extremadamente frágiles: El supuesto ordenador cuántico es ultra-sensible al ruido experimental, esto es, a los efectos físicos del resto de componentes del ordenador. Así en cualquier estado altamente superpuesto de cubits, un único error que afecte sólo a uno de los cubits puede destruir la coherencia del estado completo.Por ello son precisos códigos de corrección de errores que funcionen tan efectivamente, que difícilmente un único cubit falle en el curso del cálculo.

Son la versión cuántica de los códigos de corrección de errores clásicos, tales como los de Hamming o de Huffman, pero con la particularidad de que son esenciales para un funcionamiento efectivo en la transmisión de datos.

CONCLUSION

Al rebasar cierta escala de miniaturización, el tamaño de los componentes electrónicos se convierte en un problema: los conductores atascados y los transistores apenas funcionan. Por fortuna, nuevos diseños circuitales ultra pequeños, basados en efectos de la Mecánica Cuántica, manejan los datos con mayor fiabilidad.

Por muy pequeños que sean los circuitos que se logran por las distintas técnicas de miniaturización dentro de los chips, todavía son enormes agregados de átomos. Nuevas tecnologías de Computación (Computación Cuántica) podrían operar a escalas menores, posiblemente a nivel molecular e incluso atómico.

Los computadores cuánticos utilizan, para realizar sus operaciones, las propiedades de la mecánica cuántica, que describe la naturaleza al nivel atómico y sub -atómico. En lugar de los bits 1 y 0 de las computadoras clásicas, que efectúan operaciones una a la vez sobre un conjunto de números, los computadores cuánticos están basados en bits cuánticos o qubits, que consisten en una superposición de estados 0 y 1, lo que permite resolver problemas de gran complejidad al realizar múltiples cálculos simultáneamente en cada unidad de procesamiento.

Un computador cuántico pretende explotar el hecho de que los objetos cuánticos pueden colocarse en una superposición de muchos estados a la vez. Ello permitiría a un solo procesador realizar simultáneamente una gran cantidad de cálculos en paralelo, de forma similar a un ordenador con muchos procesadores funcionando al mismo tiempo.

De esa manera se podrían atacar problemas complejos, cuya dificultad crece muy rápidamente con el tamaño de los datos de entrada. Por ejemplo, si para factorizar un número necesitamos probar todos sus posibles divisores, la tarea se hace rápidamente intratable para números grandes, sin embargo un computador cuántico seria en principio capaz de probar todos los divisores "a la vez" y determinar los correctos inmediatamente.

De hecho ya se han desarrollado buenos algoritmos para resolver en un computador cuántico problemas considerados intratables por un computador clásico. Pero en la práctica la tarea de construir un ordenador cuántico es extremadamente complicada. Primero hay que hallar el substrato físico ("hardware") adecuado para implementar los estados cuánticos representativos del computo. Por otro lado un estado de superposición cuantiíta es extremadamente frágil, a la mas mínima interacción con el ambiente experimenta un colapso que destruye todos sus estados componentes menos uno (el estado final resultante es completamente aleatorio). Además los

computadores cuánticos tienen un gran margen de error, no dan respuestas correctas todo el tiempo, lo que hacen mas bien es "adivinar" una respuesta probable que luego debe comprobarse con un ordenador clásico (la idea es que si la respuesta resulta ser incorrecta entonces el ordenador cuántico debe "proponer" otra, hasta hallar la correcta).

DESARROLLOS RECIENTES

Informática sin Límites

En enero de este año, un grupo de investigadores del Laboratorio Nacional de Sandia en Albuquerque, Nuevo México, Se puso en operación por primera vez un cristal fotónico en tres dimensiones, que es el equivalente para la luz (fotones) de lo que los semiconductores y transistores usuales son para los electrones. La luz es desviada en los diversos materiales que constituyen el cristal fotónico, que actúa como un switch de luz que servirá de base para los futuros transistores ópticos. A diferencia de los procesadores actuales que operan a velocidades en el rango de los millones de oscilaciones por segundo, los transistores ópticos tendrán capacidad de operar un millón de veces más rápido, lo que equivale ¡a un millon de millones de ciclos por segundo!

También en febrero de este año se llevó a cabo en la Universidad de Harvard un experimento nunca antes realizado, en el que la velocidad de la luz es reducida a 17 metros por segundo de su velocidad en el vacío de 300.000 kilómetros por segundo. Para lograr este efecto, se creó un medio de materia condensada llamado "transparencia inducida por electromagnetismo" utilizando un sistema de laser, que permitió reducir la velocidad de la luz por un factor de 20 millones sin ser absorbida. Se espera alcanzar próximamente velocidades tan bajas como centímetros por segundo en la propagación de la luz para aplicaciones prácticas de conversión óptico-electrónica y conversión de la luz de una frecuencia a otra, aspectos necesarios para implementar la tecnología óptica en los computadores y sistemas de comunicaciones en el futuro.

NEC de Japón avanza en el desarrollo de la Computación Cuántica

La compañía NEC Corp y un organismo de investigación pública de Japón dijeron el jueves que han logrado un importante avance tecnológico que acorta el plazo para el uso de las computadoras cuánticas ultrarrápidas. Los expertos esperan que las computadoras cuánticas, cuando sean puestas en uso práctico, sobrepasen las capacidades de las supercomputadoras más poderosas de la actualidad, especialmente en campos como la búsqueda de grandes bases de datos para piezas particulares de información.

Sin embargo, un portavoz de NEC dijo que es improbable que las computadoras cuánticas para uso comercial estén disponibles para antes del 2020. Las computadoras cuánticas usan "qubits" -formas de partículas cuánticas- como la unidad de información básica y éstas eventualmente serán más flexibles y rápidas al procesar la información que las computadoras existentes.

NEC y el grupo de investigación Riken, financiado por el gobierno japonés, dijeron que han creado con éxito un estado de "enredo cuántico" entre dos "qubits" de estado sólido por primera vez en el mundo. El enredo cuántico describe el entrelazamiento de dos o más partículas sin contacto físico. NEC desarrolló el primer "qubit" de estado sólido en 1999, usando un dispositivo superconductor. Los detalles plenos de los resultados de su investigación serán publicados en la edición del 20 de febrero de la revista científica británica Nature.

IBM logra una nueva meta histórica con su computadora cuántica

Científicos del Laboratorio de Investigación de IBM en Almaden, San José, California, llevaron a cabo el cálculo más complicado que se haya completado hasta la fecha en una computadora cuántica. En el experimento, los científicos hicieron que un trillón de moléculas diseñadas a la medida y contenidas en una probeta se transformaran en una computadora cuántica de siete qubits para resolver una versión sencilla del problema matemático que se encuentra en el corazón de muchos de los sistemas criptográficos actuales destinados a la seguridad de datos.

"Este resultado refuerza la conciencia creciente de que las computadoras cuánticas pueden resolver algún día problemas tan complejos que incluso las supercomputadoras más poderosas son incapaces de responder así trabajaran durante millones de años", manifestó Nabil Amer, gerente y estratega del grupo de física de la información del Departamento de Investigación de IBM.

En el número de hoy de la revista científica Nature, un grupo integrado por científicos de IBM y por estudiantes de segundo ciclo de la Universidad de Stanford informan la primera demostración del "Algoritmo de Shor". El ejemplo significativo más sencillo del Algoritmo de Shor es el de encontrar los factores del número 15, una operación que requiere una computadora cuántica de siete qubits. Los químicos de IBM diseñaron y elaboraron una nueva molécula que tiene siete spins nucleares -los núcleos de cinco átomos de flúor y de dos de carbono- que pueden interactuar como qubits, programarse mediante pulsos de radio frecuencias y detectarse con instrumentos de resonancia magnética nuclear (Nuclear Magnetic Resonance--NMR) similares a los actualmente utilizados en hospitales y laboratorios químicos.

En un tubo, los científicos de IBM controlaron un trillón de esas moléculas para ejecutar el algoritmo de Shor, e identificaron correctamente 3 y 5 como los factores de 15. "Aunque la respuesta puede parecer trivial, el control sin precedentes de los siete spins durante el cálculo hizo de éste el cómputo cuántico más complejo realizado a la fecha", señaló Amer.

"Ahora tenemos el desafío de convertir la computación cuántica en una realidad de la ingeniería", indicó Isaac Chuang, líder del grupo de investigación y ahora profesor adjunto en MIT. "Si podemos realizar este cálculo en escalas mucho mayores -digamos miles de qubits para factorizar números muy grandes- se necesitarían hacer cambios fundamentales en las implementaciones criptográficas".

Isaac Chaung - Tubo de prueba de computadora cuántica.

Aún cuando el potencial de la computación cuántica es enorme y los progresos alcanzados recientemente son alentadores, las computadoras cuánticas comerciales están a muchos años de distancia. Las computadoras cuánticas basadas en NMR son todavía experimentos de laboratorio y las primeras aplicaciones de la computación cuántica tomarían probablemente la forma de coprocesadores para llevar a cabo funciones específicas, por ejemplo resolver problemas matemáticos difíciles, sistemas de modelaje cuántico y búsquedas no estructuradas. Los procesadores de texto o las tareas que requieren resolver problemas sencillos se manejan más fácilmente con ayuda de las computadoras actuales.

La demostración de IBM del algoritmo de Shor muestra también el valor de los experimentos en la computación cuántica usando NMR, un enfoque introducido independientemente a mediados de la década de 1990 por Chuang y Neil Gershenfeld de MIT, y por David Cory y colegas, también de MIT. "Nuestros experimentos con NMR nos estimularon a desarrollar herramientas

fundamentales para tipos futuros de computadora cuántica", comentó Chuang. "La más importante de esas herramientas fue una manera de simular y predecir la degradación de la señal causada por la des coherencia -fluctuaciones cuánticas no deliberadas. Esta herramienta nos permitió minimizar los errores de des coherencia en nuestro experimento de 7 qubits".

Y aún cuando NMR seguirá siendo un banco de pruebas para desarrollar herramientas y técnicas de computación cuántica, será difícil desarrollar y sintetizar moléculas dotadas de más de siete qubits. En consecuencia, nuevos experimentos de IBM y de otros se proponen desarrollar nuevos sistemas de cómputo cuántico capaces de aumentar de escala más fácilmente para alcanzar el número grande de qubits requerido en las aplicaciones prácticas. Entre los candidatos principales se cuentan hoy los spins electrónicos confinados en nanoestructuras de semiconductores (llamados a menudo puntos cuánticos), spins nucleares asociados con impurezas de un solo átomo en un semiconductor, y el flujo electrónico o magnético por superconductores. Se están evaluando también implementaciones atómicas y ópticas.

IBM RESEARCH NEWS

Computadoras cuánticas: más cerca

Los circuitos lógicos tendrían una capacidad y velocidad muy superiores a los actuales.

Un equipo de científicos estadounidenses logró "entrelazar" dos partículas subatómicas situadas aproximadamente a un milímetro de distancia.

Este adelanto posibilitaría la creación de potentísimas computadoras cuánticas, con circuitos lógicos de una capacidad y velocidad muy superiores a las actuales.

Cuando dos partículas están entrelazadas, sus destinos son interdependientes, a pesar de la distancia que pueda mediar entre ambas, incluso si están en extremos opuestos del universo.

El propio Albert Einstein hallaba difícil creer que una partícula pudiera comunicarse con otra a una velocidad superior a la de la luz, el límite máximo en la naturaleza.

Einstein pensaba que tras la aparente irracionalidad de este fenómeno había algo que podía minar la credibilidad de la teoría de la mecánica cuántica, que explica cómo el universo se comporta a nivel atómico y subatómico.

Más rápido que la luz

Ya Einstein había muerto cuando, en los años 70, el físico Alan Aspect realizó un experimento que demostró que el entrelazamiento cuántico es real y que podría servir de base para la creación de supercomputadoras en un futuro no lejano.

Teóricamente, las computadoras que utilicen fotones en lugar de electrones serían más rápidas que las actuales, pues su único límite sería el de la velocidad de la luz al atravesar cristales.

Pero, según diversos científicos, la velocidad de las computadoras basadas en el entrelazamiento cuántico será superior a la de la luz, pues no dependerán de electrones o fotones.

Estas computadoras tendrían que entrelazar bits cuánticos -o qubits- situados a distancias considerables.

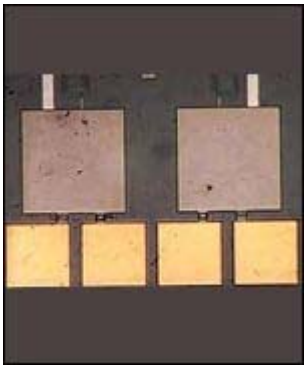
Hasta hace poco, el entrelazamiento de partícula sólo se había observado a escala micrométrica (la millonésima parte de un metro).

Cada vez más cerca

Ahora, Andrew Berkley y sus colegas de la Universidad de Maryland, Estados Unidos, han logrado reducir mil veces esa distancia, al entrelazar dos qubits dentro de un chip de silicio, a 0,7 milímetros uno del otro.

Un milímetro no representa la fabulosa distancia de un extremo al otro del universo, pero se aproxima mucho más a la escala necesaria para fabricar componentes de computadoras basadas en la mecánica cuántica.

"El entrelazamiento es esencial para la computación cuántica porque posibilita la colocación de mayor información en los bits cuánticos que lo que es posible con los bits actuales", dijo Berkley.



Entrelazamiento cuántico en un chip de silicio: un gran avance.

BCC MUNDO – mayo, 2003

Cifrado impenetrable con computadoras cuánticas

Científicos de la Universidad de Ginebra están colaborando con el Ministerio de Telecomunicaciones de Suiza en un experimento que usa computadoras cuánticas para ejecutar un algoritmo inquebrantable de encriptación.

Una de las ventajas de las computadoras cuánticas es que mientras las máquinas convencionales crean bits de información, y cada bit es un 0 ó un 1, los bits cuánticos pueden ser tanto 0 ó 1 o cualquier combinación de los dos números.

Aún mejor es que los bits cuánticos no pueden ser clonados o copiados, lo que hace virtualmente imposible que alguien rompa el código encriptado por una computadora cuántica.

DIARIO TI – Agosto, 2000

Nueva herramienta contribuye a estudiar la disipación del calor en el transporte de electrones en transistores

Los chips pueden generar suficiente calor como para, en casos extremos, incendiarse. Los ingenieros conocen bien cómo controlar las cargas eléctricas en circuitos, pero tienen problemas para librarse del calor producido por los electrones al circular. Existe ya una herramienta para estudiar a fondo el fenómeno.

Un nuevo dispositivo desarrollado por Robert Blick, de la University of Wisconsin Madison, podría resolver esta cuestión, además de proporcionarnos información sobre la aplicación del mundo cuántico en comunicaciones y computación.

Blick, junto a sus colegas Eva Hoehberger y Werner Wegscheider, ha desarrollado algo parecido a un trampolín increíblemente pequeño para que los electrones solos reboten en él. Opera como un átomo artificial, o una membrana, suspendido sobre una cavidad semiconductora.

La herramienta permitirá, por primera vez, estudiar con detalle la influencia de la disipación del calor en el transporte de electrones individuales en transistores.

El dispositivo mide sólo 100 nanómetros de ancho y actúa, de alguna forma, como lo haría una pequeñísima guitarra. La cuerda de una guitarra convencional vibra a varios miles de ciclos por segundo. Si redujéramos su tamaño hasta varios centenares de nanómetros, vibraría a una velocidad que se halla en el régimen de los gigahercios (alrededor de los mil millones de ciclos por segundo).

A esta escala, el movimiento en la cuerda (o la membrana suspendida, en el caso de este nuevo aparato) es increíblemente pequeño. Blick dice que los efectos de la disipación del calor aparecerán como vibraciones de los átomos artificiales en suspensión. El movimiento causará un cambio en el voltaje que los investigadores podrán medir.

El método permite estudiar una gran variedad de sistemas electrónicos, comenzando con el flujo bidimensional de electrones, común en muchos transistores de hoy en día. Dicho flujo será reducido en primer lugar a un canal donde los electrones fluirán en una única dirección, y finalmente, se ajustará el

dispositivo hasta alcanzar un estado de dimensión cero (transistor de un único electrón). Podremos entonces hacer rebotar estos electrones individuales, de forma muy controlada, y ver cómo envían energía sobre estas membranas tan delgadas.

Los resultados permitirán optimizar la tecnología utilizada actualmente, limitada por la disipación del calor. A más largo plazo, podría revelarnos importantes secretos que posibiliten explotar el potencial de la computación y las comunicaciones cuánticas.

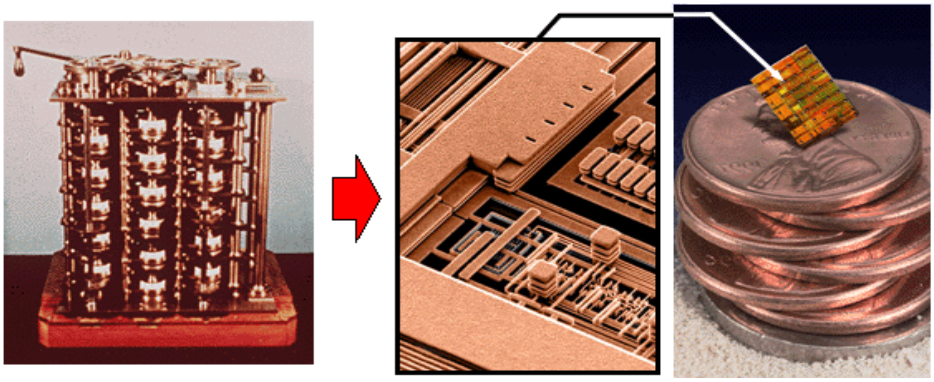
BIBLIOGRAFíA

- "A short introduction to quantum computation" A.Barenco, La Recherche, November 1996
- "Quantum Information" A.Ekert, D.Deutsch, Physic World.
- "Quantum Computation: Pro- and Con-."J.Preskill.Preprint· "Investigación y Ciencia".
- "Quantum computing with molecules". Scientific American, I.Chuang,1998
- "Suplemento FUTURO de el país digital"
- Y. Nakamura, Y. A. Paskin, J. S. Tsai, Nature 398, 786 (1999).
- A J. Legget en "Chance and Matter", ed. por Soulite et al, (Elsevier, 1987), p. 395.
- U. Weiss, "Quantum dissipative systems", World Scientific, 1999; A. O. Caldeira and A.J. Legget.

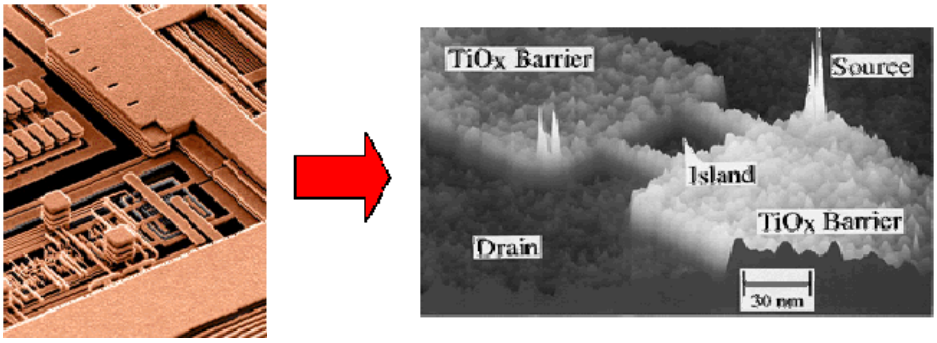
Enlaces

- http://news.bbc.co.uk/hi/spanish/science/newsid_3050000/3050497.stm
- http://www.axxon.com.ar/not/126/c-126InfoEntrelazarParticulas.htm
- http://www.diarioti.com/noticias/2000/ago2000/15193385.htm
- http://www.hipermarketing.com/nuevo%204/home_noticias/noticias.html
- http://www.fisica.edu.uy/cursos/Opcionales/2003/COMPUCUANTICA.rtf
- http://www.netmedia.info/informationweek/articulos.php?id_sec=13&id_art=3100

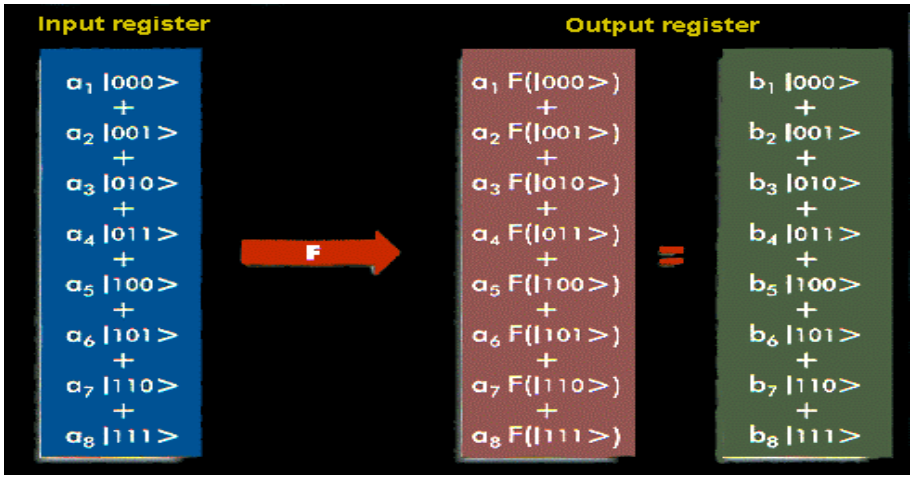
ANEXO



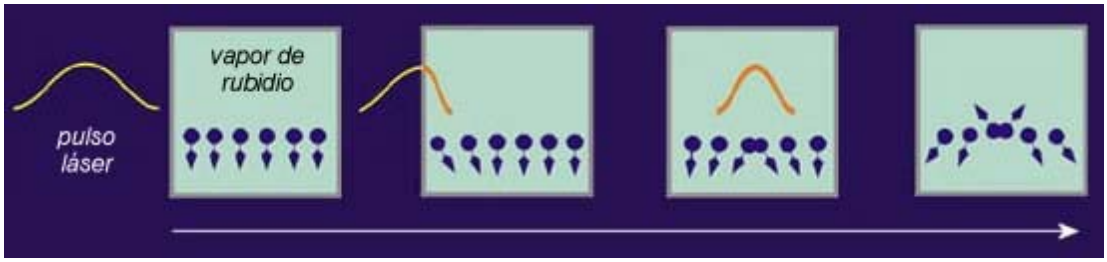
Desde el principio hasta el presente: A la izquierda una máquina de engranajes, a la derecha un chip de la IBM de 0.25 micras.



La transición de microtecnología a nanotencología.



Registro de tres qubits.



Pulso Láser