EL ORDENADOR CUÁNTICO.



1.RESUMEN.

En los últimos años, ha despegado y se ha constituido toda una nueva disciplina, la computación cuántica, que en último término pretende desencadenar una nueva concepción en la arquitectura de los ordenadores, para dar lugar al ordenador cuántico. A continuación, veremos tanto las motivaciones para este cambio tecnológico, como los nuevos conceptos implicados y los primeros ordenadores cuánticos.

2. INTRODUCCION.

Las grandes revoluciones en la historia de la tecnología han implicado nuevas formas de utilizar la naturaleza, explotando distintos recursos tales como materiales, fuerzas y fuentes de energía. Estas revoluciones han estado impulsadas habitualmente por progresos conceptuales, como por ejemplo, cuando Newton unificó el movimiento de todos los cuerpos(a escala de la percepción humana y por encima), notando que cualquier móvil satisfacía unas mismas ecuaciones, fuera una manzana, un péndulo o un planeta; o cuando definimos el concepto de energía, subyacente tanto en un electrón acelerado en el anillo del CERN, como en una hoja de lechuga.

Otro hito en la evolución conceptual fue el reconocimiento de que, algo que ahora llamamos información, era un concepto compartido por objetos, y que era susceptible de ser manipulado, de la misma forma en que son manipulados el momento y la energía en las ecuaciones de movimiento de un cuerpo; por ejemplo, consideremos como objetos los enunciados siguientes:

"Es un ordenador", "c'est une ordinateur", "it's a computer".

Podemos notar que tienen algo en común(su contenido de información), aunque no comparten las mismas palabras, las mismas combinaciones de letras. Para poder manipular ese "algo, asignamos por ejemplo los siguientes números a las letras :a->34,b->35,c->36,, de esta forma la expresión en español quedaría como: 38 52 54 47......

Pues bien, a lo largo del último siglo la " tecnología de la información ", ha ido implicando una secuencia de avances en los componentes de los ordenadores, de forma que éstos han ido duplicando su velocidad cada dos años, al tiempo que reducían el tamaño de sus componentes a la mitad. (Los circuitos actuales contienen transistores y líneas de conducción cuya anchura es menor que un micrómetro).

Pues bien, las técnicas de integración de microcircuitos están llegando a sus límites, puesto que los procedimientos litográficos más avanzados, por medio de los cuales los elementos podrían reducirse cien veces menos, hacen que los circuitos integrados apenas consigan funcionar, al presentarse la materia que componen los dispositivos como una muchedumbre de átomos, donde ya se percibe el carácter individual de los mismos. A esta escala, los dispositivos de los circuitos del ordenador son descritos por la teoría cuántica de la materia.

No es sólo esta barrera tecnológica la única motivación para el surgimiento de la computación cuántica; nuevos problemas de cálculo, como la simulación de la interacción de moléculas ácidas con proteínas, la descomposición prima de enteros de orden mayor que 120, la predicción meteorológica,... etc., descubren las limitaciones de la computación binaria y secuencial, invocando ya a una nueva concepción de la arquitectura y el cálculo informáticos, estando sustentada su base teórica en la mecánica cuántica.

3.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. (Ver: figura 1).

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(pensemos en el gas de las farolas cuando comienzan a encenderse o bien en los átomos de un objeto incandescente), 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 mecanocuánticas, 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 introduzco 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 sóla onda; el segundo se refiere al proceso por el cual dos ondas coherentes recuperan su respectiva identidad individual diciéndose que hay decoherencia.

4.DE LOS BITS A LOS CUBITS.

4.1.CUBITS.

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 cualquiera dos estados distinguibles, también puede estar en cualquier superposición coherente de ellos, y claro, estos son más estados, que no tienen anólogos clásicos, y en los cuales un átomo representa ambos valores 0 y 1 simultaneamente(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 simultaneamente, a lo que se llama cubit ó unidad de información cuántica.

¿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 cubits podría almacenar simultaneamente 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 cubit. Así, si añadimos más cubits al registro, su capacidad aumenta de forma exponencial: 4 cubits podrán almacenar 16 números diferentes a la vez, y en general X cubits 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 dásico 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.

4.2.ORDENADORES CUÁNTICOS.

Ahora, ¿en qué consistiría la diferencia entre un ordenador cuántico y otro clásico?. Pues bien, 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 cubits 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 cubits, 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. ¿Es esto posible actualmente?

5. HARDWARE.

Hoy se sabe como leer y escribir información en sistemas cuánticos; veamos los procesos 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 Eo. Para escribir un bit 0 en este átomo no se actua físicamente sobre él. Para registrar un 1 en él, excitamos el átomo hasta un nivel energético superior E1. Esto se consigue bañandolo en luz láser compuesta por fotones cuya energía sea igual a la diferencia entre E1 y E0. 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 cubit, 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 cubit
- Lectura. En un sistema cuántico sería parecida a la escritura: se empuja al átomo hasta un estado energético todavía más elevado y menos estable, E2. Esto lo hacemos sometiendo al átomo a luz láser de energía igual a la diferencia entre E1 y E2; si el átomo se encuentra en E1 , se excitará hasta E2, pero retornará rápidamente a E1 emitiendo un fotón. Si el átomo sencuentra ya 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. (Ver: Figura 3)

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 El 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(2000/2001), 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 E₁ y E₀ comparables, y es aquí donde el tiempo de escala de decoherencia es tan corto.

6. LA CONSTRUCCION DEL ORDENADOR CUANTICO.

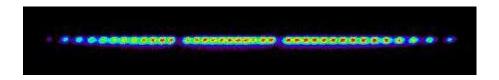
En principio se sabe como construir un ordenador cuántico: se comienza por puertas lógico-cuánticas que se va uniendo e integrando junto a la circuitería cuántica(cables cuánticos y buses apropiados). Sin embargo cuando el número de puertas cuánticas(recordar, la versión cuántica de las puertas lógicas 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):

6.1.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.

Ahora, 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).

6.2. 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, jen número de 10^20!!. Es entonces cuando puede ser medido el estado de espín promedio. En recientes experimentos(ver Suplemento FUTURO de el país digital-25 de abril-2001), 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.(ver figura 2)



7.CONCLUSIONES.

La vertiginosa evolución que ha experimentado el campo de la computación cuántica en el último decenio, permite vislumbrar posibles ordenadores cuánticos, sus potencialidades en la resolución de tareas clásicas(como la factorización de números) y nuevas aplicaciones antes apenas sospechadas, como la simulación de la evolución de sistemas cuánticos, y nuevos algoritmos que realicen más efectivamente tareas que sus análogos clásicos. El hardware en la actualidad se encuentra en su infancia, pues no se puede decir que las trampas de iones o las técnicas de NMR puedan constituir un ordenador cuántico práctico para los usuarios, pero es el inicio de una nueva tecnología, que va implicar cambios sustanciales en la forma de concebir la arquitectura de los ordenadores y de las operaciones a realizar, y todo ello sustentado en el dominio de la materia a escala microscópica, y el entendimiento más profundo de la teoría de la información y de la teoría de números.

Hoy por hoy, construir un ordenador cuántico es una tarea que excede las capacidades técnicas disponibles; sin embargo, las ventajas de un ordenador cuántico operativo y las continuas adhesiones a este empeño, hacen que el reto de hacerlo realidad esté cada vez más próximo.

APÉNDICE:

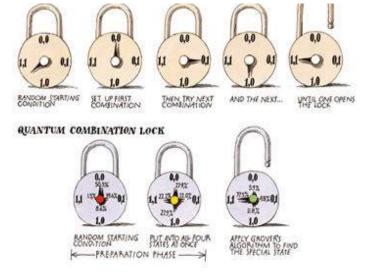
1. ALGORITMOS CUÁNTICOS.

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.

BIBLIOGRAFIA:

- "A short introduction to quantum computation" A.Barenco, La Recherche, November 1996
- "Quantum Computing" A.Steane, Reports on Progress in Physics 1998. Preprint: quant-ph/9708022
- "Quantum Information" A. Ekert, D. Deutsch, Physic World.
- "Quantum Computation: Pro- and Con-."J.Preskill.Preprint: quant-ph/9705032
- "Investigación y ciencia". Febrero 1996
- "Quantum computing with molecules". Scientific American, I. Chuang, 1998
- "Suplemento FUTURO de el país digital-25 de abril-2001"
- Course for Physics/Quantum Computation

Enlaces sobre Computación Cuántica

Figuras:

figura 1::vision de una molécula de agua.

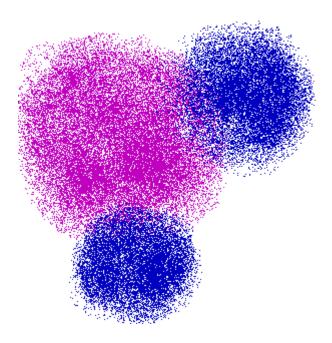


Figura 2 : Nucleo Magnético

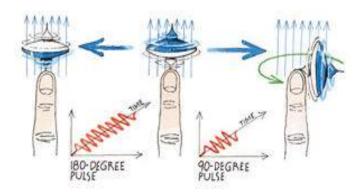
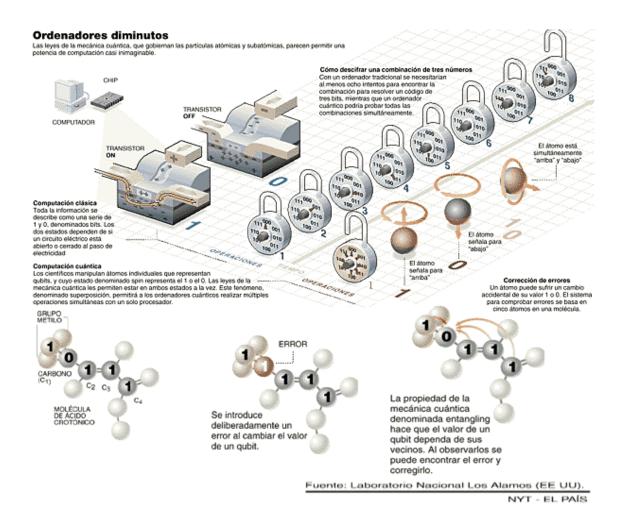
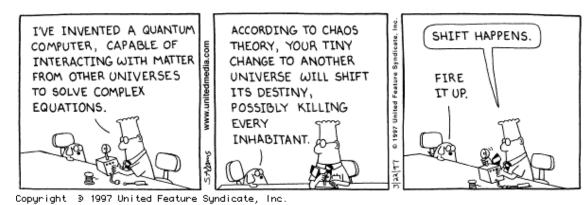


Figura 3: Ordenador cuántico y criptografía



Humor:



Redistribution in whole or in part prohibited

Realizado por: Miguel Angel Alejo Plana, 1º de Matemáticas.