

computación cuántica

Sergi Baila Martínez (www.sargue.net)
Traducción: Lupus (unodehuesca.blogspot.com)

Ésta obra está bajo una Licencia de Reconocimiento-Compartición de Creative Commons. Para ver una copia, visite <http://creativecommons.org/licenses/by-sa/2.0/> o envíe una carta a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Contenidos

CONTENIDOS	2
1.INTRODUCCIÓN	3
1.1. ¿El siglo de la incertidumbre?.....	3
1.2. Ordenadores lineales.....	3
2.INFORMACIÓN CUÁNTICA	4
2.1. Qubit.....	4
2.2. Puertas cuánticas.....	4
2.3. No duplicación.....	4
2.4. Codificación densa.....	4
2.5. Teleportación cuántica.....	5
3.EL ORDENADOR CUÁNTICO UNIVERSAL	5
3.1. La puerta cuántica universal.....	5
4.ALGORITMOS CUÁNTICOS	6
4.1. Computación cuántica.....	6
4.2. Ejemplo: buscar el período de una función.....	6
5.ORDENADORES CUÁNTICOS EXPERIMENTALES	8
5.1. Trampa iónica.....	9
5.2. Resonancia magnética nuclear.....	9
5.2. Rydberg Sculpting.....	9
6.CORRECCIÓN DE ERRORES CUÁNTICOS	10
7.CRIPTOGRAFÍA CUÁNTICA	11
8.PERSPECTIVAS DE FUTURO	11
9.BIBLIOGRAFÍA	12

1. Introducción

La humanidad ha progresado a medida que los científicos descubrían nuevos métodos de explorar los recursos físicos que nos rodean. Si preguntásemos cuáles son estos recursos a un científico anterior al siglo XX, lo más probable es que obtuviésemos una respuesta triple: materiales, fuerzas y energías. Ahora bien, resulta que en el siglo XX hemos añadido un nuevo recurso que podemos manipular, y por el cual tenemos unas leyes físicas probadas: la información. Además, la invención del ordenador ha permitido, por vez primera, llevar a cabo un tratamiento de información compleja de manera rápida fuera del cerebro humano.

El tema de la computación cuántica es un tema basto y emergente, que abarca desde la teoría de la información clásica hasta la física de partículas, pasando por la informática y la teoría matemática del tratamiento de la información. Quizá se puede englobar todo en un superconjunto que incluya la computación cuántica junto con otras disciplinas de una importancia cada vez mayor para conseguir llegar a comprender los fundamentos de la mecánica cuántica y el mundo natural. Este superconjunto es a lo que se llama teoría de la información cuántica.

1.1. *¿El siglo de la incertidumbre?*

El siglo pasado comenzó con teorías que hicieron estremecer los cimientos de lo que la mayoría entendía como física, e indirectamente, la comprensión del mundo en que vivimos. Los físicos, con el principio de Heisenberg en las manos, tiraron por tierra el determinismo, que unido al reduccionismo habían dominado el pensamiento científico-filosófico de los últimos siglos.

Análogamente, aunque al principio sin ningún tipo de conexión, Gödel hacía el papel de Heisenberg, pero en su caso en el mundo matemático. Gödel contestó unas preguntas que ya se hacía David Hilbert un poco antes.

Hilbert, un verdadero pensador matemático, propuso una serie de cuestiones en un congreso celebrado en el año 1900. Según él mismo, estas cuestiones estaban dirigidas a las generaciones futuras con el objeto de resolver una serie de problemas básicos de las matemáticas. Estas cuestiones versaban directamente sobre la propia naturaleza de las matemáticas. Resumidamente, Gödel demostró la existencia de proposiciones matemáticas que eran indecidibles, no podía demostrarse que fuesen ciertas o falsas. Antes, se pensaba que las matemáticas eran completas: toda proposición tenía una respuesta clara, cierta o falsa. Ahora primero hace falta preguntarse si la proposición es decidible.

1.2. *Ordenadores lineales*

Alan Turing, matemático, fue uno de los que buscaba un proceso automático para responder a la pregunta sobre la decidibilidad de una cuestión matemática. Ideó un dispositivo mecánico ideal, suficientemente potente para responder preguntas bastante complicadas y al mismo tiempo lo bastante sencillo como para ser analizado a fondo.

La Máquina de Turing se convirtió en una herramienta básica de los matemáticos, incluso que después sería adaptada por los informáticos para poder hablar con propiedad de la complejidad computacional de la resolución determinada de un problema (un algoritmo).

Los ordenadores de hoy en día son altamente sofisticados tecnológicamente y nos pueden parecer muy rápidos. Sin embargo, tienen una potencia computacional equivalente a las máquinas de Turing, en un sentido técnico estricto. Estamos de acuerdo que los ordenadores de hoy día (capaces de procesar miles de millones de cálculos por segundo) están muchos órdenes de magnitud por encima de los primeros ordenadores a válvulas. Pero tanto unos como otros son lineales.

La mecánica cuántica surge aquí con una posibilidad de cambio.

2. Información cuántica

Como ya se ha dicho antes, la información cuántica es una rama de la ciencia bastante nueva, pero es no quiere decir que nos podamos escapar de unas cuantas definiciones.

Antes de entrar en las definiciones, hace falta aclarar que en algunas aparecen dos personajes ficticios: Alice y Bob. Estos dos personajes ya son famosos entre los investigadores, ya que se usan en multitud de ejemplos. Nosotros haremos lo mismo.

2.2. Qubit

Es la unidad mínima de información cuántica. Puede verse como un sistema de dos estados, como un spin o un átomo de dos niveles, pero cuando lo usamos para medir información en qubits, estamos realmente haciendo algo más abstracto: un sistema cuántico se dice que tiene n qubits si tiene un espacio de Hilbert de 2^n dimensiones y dispone por tanto de 2^n estados cuánticos mutuamente ortogonales. Ésta definición se desarrollará con más claridad un poco más adelante.

La notación para escribir qubits es una lista de estados ortogonales con un número binario para cada estado. Por ejemplo, dos estados ortogonales con un número binario para cada estado. Por ejemplo, dos estados ortogonales de un solo qubit se pueden escribir como $\{|0\rangle, |1\rangle\}$. Para tres qubits tenemos: $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$.

2.2. Puertas cuánticas

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

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

2.3. No duplicación

Teorema de la no duplicación: Un estado cuántico desconocido no puede ser duplicado.

Este teorema impide generar copias de un estado cuántico dado, a no ser que el estado ya sea conocido (que exista información clásica que lo describa). El hecho de duplicarlo permitiría hacer diversas copias y posteriormente, medir en cada copia una propiedad diferente, lo que violaría el principio de incertidumbre de Heisenberg.

2.4. Codificación densa

El embrollamiento cuántico es un recurso informativo.

Los qubits se pueden usar para almacenar y transmitir información clásica. Alice puede transmitir, por ejemplo, la secuencia $|01001\rangle$ con 5 qubits con los estados correspondientes. Bob, posteriormente, puede medir cada qubit y extraer la secuencia sin ningún tipo de ambigüedad.

Se puede demostrar que si Alice y Bob disponen de un par de qubits embrollados, Alice puede transmitir a Bob dos bits clásicos por cada qubit transmitidos.

La codificación densa es complicada de implementar y no tiene mucha más utilidad que servir de método de comunicación estándar. Sin embargo, permite una transmisión totalmente segura: el qubit enviado por Alice sólo podrá dar los dos bits clásicos que le corresponden al poseedor del otro qubit embrollado (la pareja del de Alice).

2.5. Teleportación cuántica

¡Es posible transmitir qubits sin enviar qubits!

Supongamos que Alice quiere comunicar a Bob un solo qubit. Si Alice ya conoce cuál es el estado, se lo puede comunicar mediante algún sistema convencional.

Sin embargo, el problema es si Alice no conoce el estado. No puede medirlo sin modificarlo (y sólo podría enviar a Bob el estado resultante, que no es toda la información que hay dentro de un qubit), y tampoco puede hacer una copia para modificar ésta copia (recordemos el teorema de la no duplicación). Así, parece que la única manera es enviar físicamente el qubit: enviar el átomo o electrón (o lo que sea) que contiene el estado cuántico. Pero enviar un estado cuántico no es fácil; no podemos ponerlo en un sobre y enviarlo por correo. ¿Hay alguna forma de enviar el estado cuántico (desconocido) sin modificarlo mediante información clásica?

La teleportación cuántica permite resolver esta situación, o por lo menos, hallar un camino alternativo. Como en la codificación densa, se usa el embrollamiento cuántico como un recurso informativo. La idea es que Alice y Bob dispongan de un par de qubits embrollados, mediante los cuales se puede demostrar que Alice puede obtener dos bits clásicos a través de unas operaciones sobre el qubit que quiere transmitir (que queda destruido -modificado-) y el qubit pareja de los dos embrollados que tienen en común. Bob, posteriormente, puede reproducir el qubit original mediante operaciones análogas con su pareja embrollada y los dos bits clásicos.

3. El ordenador cuántico universal

La teoría de la información cuántica necesita una herramienta equivalente a la Máquina de Turing de la teoría clásica de la información. Esta máquina universal es lo que llamaríamos el computador cuántico universal. La primera definición sería de una máquina así se le atribuye a Deutsch.

Un computador cuántico es un conjunto de n qubits sobre los que las siguientes operaciones son experimentalmente factibles:

1. Cada qubit puede ser preparado en un estado conocido $|0\rangle$
2. Cada qubit puede medirse en la forma $\{|0\rangle, |1\rangle\}$.
3. Una puerta cuántica universal (o conjunto de puertas) pueden ser aplicadas a voluntad sobre cualquier subconjunto de medida fija de sus qubits.
4. Los qubits no evolucionan de ninguna otra manera que no sea mediante alguna de las transformaciones anteriores.

Esta definición no es totalmente completa en un sentido técnico estricto, pero comporta las principales ideas.

3.1. La puerta cuántica universal.

La puerta cuántica universal es el equivalente cuántico de la puerta universal clásica, una puerta mediante la que es posible generar la acción de cualquier otra puerta mediante repetidas operaciones y combinaciones.

Se han encontrado puertas de sólo dos qubits que son universales, lo cual es muy interesante. La puerta más extensa está formada por operaciones XOR y de rotación de qubits individuales.

4. Algoritmos cuánticos

Hasta ahora hemos visto cómo sería un computador cuántico y cómo haría sus cálculos. Pero de momento no hemos demostrado que haya nada que pueda hacer un computado cuántico que no sea capaz uno clásico.

La respuesta es clara: no. Ahora, si hablamos de eficiencia de un computador cuántico frente a

otro clásico la cosa cambia. Problemas que son computacionalmente 'difíciles' pueden ser, en la práctica, imposibles de resolver mediante computadores clásicos por razones de tiempo. Ejemplos de esto son factorización de grandes números o acotar el período de una función.

La factorización de un número entero se piensa que tiene una complejidad que crece más rápidamente que cualquier potencia de N (superpolinómica), aunque todavía no se haya demostrado. El algoritmo cuántico mostrado por Shor trabaja con una complejidad de N^3 .

Además de este gran resultado, otro también muy espectacular es el conocido como algoritmo de acotación de Grover. Ése algoritmo de acotación consigue hallar un elemento en una colección desordenada en un tiempo del orden de la raíz de N , mientras que en un computador clásico está demostrado que como máximo se puede hacer en un tiempo del orden de N .

4.1. Computación cuántica

Una computación cuántica cualquiera está formada por tres pasos. Primero preparamos N qubits en un estado inicial determinado. Después, aplicamos una transformación unitaria U a los N qubits (una transformación unitaria U no es más que el producto de puertas cuánticas convencionales). Finalmente, medimos el valor de los qubits colapsándolos en los estados $\{|0\rangle, |1\rangle\}$.

Una de las diferencias fundamentales a tener en cuenta es que una computación cuántica es siempre un algoritmo probabilístico, cada vez que lo ejecutamos podemos obtener diferentes resultados. De hecho, el resultado de una computación cuántica es una distribución de probabilidades de los diferentes resultados. Lo que hacemos en el último paso, la lectura -colapso- del resultado, no es más que escoger uno de los resultados posibles.

4.2. Ejemplo: buscar el período de una función.

Éste es actualmente uno de los dos algoritmos cuánticos -junto con el de factorización- más importantes que hay desarrollados. Suponemos una función $f(x)$ que es periódica con un periodo r . Entonces, $f(x)=f(x+r)$. Suponemos además que $f(x)$ puede ser eficientemente calculada dado un x (o sea, f no es una función computacionalmente difícil). Todo lo que sabemos de r originalmente es que $N/2 < r < N$ para algún N . Asumiendo que no hay ninguna técnica analítica para deducir el periodo de $f(x)$, lo mejor que podemos hacer con un computador clásico es calcular $f(x)$ para un orden de $N/2$ valores de x , y encontrar cuándo se repite la función. Eso es ineficiente dado que el número de operaciones necesarias para el cálculo es de orden exponencial sobre la entrada N .

Éste cálculo se puede resolver de una manera elegante y rápida mediante un computador cuántico. Necesitamos uno de $2n$ qubits, donde $n=2 \cdot \log N$ con tal de almacenar los operandos. Hay que notar que cada registro es el doble de grande del máximo valor para un periodo, con tal de disponer, en el peor de los casos, de dos períodos completos. Dividimos los qubits disponibles en dos registros de n qubits cada uno, llamados x e y . Antes de comenzar, preparamos los dos registros en el estado $|0\rangle$ (ponemos todos los qubits constituyentes de los registros en este estado).

A continuación, apliquemos al registro x una de las operaciones básicas que se pueden hacer sobre qubits, la operación H . Ésto sería el equivalente de una puerta lógica convencional aplicando alguna de las operaciones básicas sobre bits (como una AND o una XOR). El resultado de ésta operación es una superposición de 2^n estados, correspondientes a todos los posibles estados en los que se puede hallar el registro x . Dicho de otra forma, el registro x , que tenía longitud n , contiene en su interior todos los números posibles que puede contener con n bits. Eso se expresa matemáticamente -de manera aproximada- con la siguiente expresión:

$$\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle |0\rangle \quad \text{donde } w = 2^n$$

Posteriormente, aplicamos una red de puertas a ambos registros x e y , para llevar a cabo la transformación $U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$. Ésta transformación puede ser unitaria, ya que el estado de entrada $|x\rangle |0\rangle$ está en correspondencia biyectiva con el estado de salida $|x\rangle |f(x)\rangle$, así que el proceso es reversible, es decir, la biyección me proporciona un vínculo entre cada pareja de qubits respectiva dentro de los dos registros. Por tanto, me garantiza la decodificación. Ahora, aplicando U_f a el estado anterior obtenemos:

$$\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle |f(x)\rangle$$

Fijémonos con más detenimiento en éste estado. ¡El valor de $f(x)$ ha sido calculado por 2^n valores de una sola vez! Eso es lo que llamamos paralelismo cuántico, y representa un paralelismo real impresionante, ya que hemos de darnos cuenta de que el cálculo de todos los valores dependen **exponencialmente** de n .

Aunque presentes en el estado cuántico del computador, los 2^n valores de $f(x)$ no son directamente accesibles, ya que una medida provocaría que el valor colapsase a un solo estado. Curiosamente, éste es precisamente el siguiente paso del algoritmo. Recordemos (fijándonos en el estado que tenemos ahora mismo) que en el registro tenemos todo los valores de $f(x)$. Ahora, medimos el valor de éste registro. Ésto provoca que colapse hacia un valor concreto (aleatorio), supongamos que éste valor es $f(x)=u$. El registro colapsa a $|u\rangle$ y el estado total deriva en:

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |d_u + jr\rangle |u\rangle$$

donde $d_u + jr$, para $j = 0, 1, 2 \dots M-1$, son los valores de x para los que $f(x) = u$. En otras palabras, la periodicidad de $f(x)$ significa que el registro x se mantiene en una superposición de $M \approx w / r$ estados, donde r era, recordemos, el período de la función f que estábamos calculando. Lo que tenemos ahora, resumiendo, es una valor concreto u de $f(x)$ en el registro y todas las x que satisfacen $f(x) = u$ en superposición al estado x . El valor d_u no es más que un offset derivado del valor y que se ha obtenido al colapsar y .

El estado que ha quedado almacenado dentro del registro x parece como un truco de magia. El “secreto” está en que cada valor de $f(x)$ mantiene un vínculo con el valor de x que se ha producido, mediante el embrollamiento de los qubits de los dos registros, que se consiguieron al calcular los valores de $f(x)$.

El problema ahora se ha reducido a extraer el periodo r de el estado del registro x . Para eso se usa una transformada de Fourier discreta aplicada al registro x . La transformada que se usa es el siguiente proceso unitario:

$$U_{FT} |x\rangle = \frac{1}{\sqrt{w}} \sum_{k=0}^{w-1} e^{i2\pi kx/w} |k\rangle$$

Ésta operación ya la hemos utilizado, de hecho. Aplicada al estado $|0\rangle$ nos da la primera transformación que hemos hecho en el algoritmo (dar todos los valores posibles al registro x). Se puede demostrar que éste proceso es unitario, se puede idear una red de puertas que implementen una versión de una FFT. Para continuar trabajando y simplificar los cálculos, dado que ésto no es más que un ejemplo, asumiremos que r es divisor de w , así que $M = w/r$. Las ideas esenciales no quedan afectadas, y el cálculo completo trae algunas complicaciones que pueden ser solventadas.

El registro y ya no nos interesa, nos fijaremos sólo en el registro x , sobre el que aplicaremos la ya mostrada transformación:

$$U_{FT} \frac{1}{\sqrt{w/r}} \sum_{j=0}^{w/r-1} |d_u + jr\rangle = \frac{1}{\sqrt{r}} \sum_k \tilde{f}(k) |k\rangle$$

on

$$|\tilde{f}(k)\rangle = \begin{cases} 1 & \text{si } k \text{ es múltiple de } w/r \\ 0 & \text{altrament} \end{cases}$$

Finalmente, mediremos el estado del registro x , provocando su colapso. El valor obtenido ha de ser, forzosamente, múltiplo de w/r . Ahora sólo hace falta sacar r del valor obtenido. Tenemos que $x = k w/r$ donde k es desconocido. Si k y r no tienen factores comunes, entonces podemos reucir $x7w$ hasta una fracción irreducible, obteniendo así k y r . En el caso de que k y r tengan algún factor común, algo improbable para valores grandes de r , el algoritmo falla.

Hace falta que en este punto hagamos una pequeña pausa para reflexionar sobre éste resultado. Estamos acostumbrados a trabajar con algoritmos deterministas... y, de hecho, son los únicos algoritmos con los que podemos trabajar sobre un ordenador clásico. Dada una entrada, siempre obtendremos la misma salida. Ahora bien, en el caso de un computador cuántico, hay pasos de los algoritmos que no son deterministas. En el caso de éste ejemplo el paso indeterminista es cuando colapsamos, ya que no podemos controlar cuál será el valor que obtendremos. Eso mismo, que nos da potencia, parece que nos la quita, pues habremos de repetir del cálculo hasta obtener una solución correcta.

Afortunadamente, se puede demostrar que el número de repeticiones es muy pequeño, y de hecho, la probabilidad de éxitos se aproxima arbitrariamente a 1 con un número de repeticiones que es, en este caso, del orden del logaritmo de r . Por tanto, el coste total del algoritmo continúa siendo polinómico.

El algoritmo que hemos descrito es eficiente siempre y cuando el cálculo de $f(x)$ sea eficiente. El número total de puertas lógicas requeridas para todos los cálculos es de orden polinómico frente el valor de n .

El problema de la factorización de grandes números se puede reducir matemáticamente a encontrar el período de una función. Todo esto, incluido el algoritmo descrito, fue publicado por Peter Shor, ingeniero informático de AT&T, en Abril de 1994, demostrando finalmente la viabilidad y utilidad de un computador cuántico ideal.

5. Ordenadores cuánticos experimentales

Hasta ahora hemos hablado de puertas cuánticas y qubits de una forma ideal. En los inicios de ésta disciplina se pensaba que, o bien se tardaría mucho en encontrar un sistema para crear un computador cuántico, o incluso se pensaba que nunca podría construirse uno.

Pero, como pasa a menudo en ciencia,, los científicos experimentales sorprenden con su ingenio, y ahora existen diferentes ordenadores cuánticos experimentales funcionando, todavía de una manera muy rudimentaria y con muy pocos qubits.

Actualmente hay dos candidatos que deberían permitir computación cuántica con entre 10 y 40 qubits. La primera propuesta es de Cirac y Zoller (1995), usando una línea de átomos confinados en una trampa iónica. Ésta propuesta está ampliamente superada por la más reciente, de Gershenfeld y Chuang (1997), y simultáneamente Cory (1996), utilizando resonancia magnética nuclear.

5.1. Trampa iónica

Una hila de iones se confinan mediante una combinación de campos eléctricos oscilantes y estáticos en un estado de alto vacío (10^{-8} Pa). Un único haz láser se divide en varios pares de haces, cada uno iluminando un ion. Cada ion tienen dos posibles estados estables (con un promedio de estabilidad de miles de años), que son ortogonales entre ellos y forman, por tanto, un qubit.

Mediante los haces láser de cada ion se pueden aplicar puertas cuánticas de un solo qubit. Para aplicar puertas de dos qubits, imprescindibles para llevar a cabo cualquier computación, se recurre a la repulsión de Coulomb entre los iones, más concretamente, a la vibración conjunta de la hilera de iones. La luz no sólo transporta energía, también transporta momento, y es éste momento el que provoca la vibración del ion que aprovechamos para hacer interaccionar los diferentes iones. El movimiento de los iones está cuantificado porque se encuentran atrapados en la trampa (llamada trampa de Paul).

Para obtener un auténtico computador cuántico todavía nos faltan dos cosas según la lista dada al comienzo del punto 3. Hemos de poder ser capaces de preparar cualquier qubit (ion) en el estado $|0\rangle$ y de poder “leer” cualquier qubit. Lo primero es posible mediante el método de bombeo óptico y enfriamiento por láser, y el segundo mediante técnicas desarrolladas por los físicos nucleares en los últimos años.

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

5.2. Resonancia magnética nuclear

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

Hasta aquí todo bien, pero como antes, nos hace falta completar los procesos de preparación del estado inicial y de lectura del estado final. El problema es que el spin del núcleo de una molécula no se puede medir ni preparar. Para resolver éste problema no se usa una sola molécula, sino una agrupación de 10^{20} moléculas. Así, la conjunción de todos los momentos magnéticos de los núcleos es suficientemente fuerte para ser detectable como un sutil campo magnético.

Los experimentos con RMN (Resonancia Magnética Nuclear) han dado resultados positivos en éstos últimos años en la manipulación y medida de estados equivalentes en complejidad a la requerida por un ordenador cuántico de unos cuantos qubits. Parece, por tanto, que los primeros ordenadores cuánticos funcionales serán sistemas RMN. Sin embargo, ésta técnica no escala demasiado bien, y con más qubits la detección del estado se limita.

5.2. Rydberg Sculpting

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

6. Corrección de errores cuánticos

Anteriormente hemos visto algunos ejemplos de algoritmos cuánticos, pero éstos solo nos dan una ventaja real sobre máquinas clásicas con problemas que necesitan un número de qubits del orden de miles. Ahora hemos visto que hay sistemas experimentales que sólo nos acercan a “ordenadores” cuánticos de unos cuantos qubits. Éstos sistemas no se pueden llamar con propiedad ordenadores cuánticos dado que no son suficientemente versátiles. Son más bien, procesadores de

información cuántica.

¿Llegaremos a disponer algún día de verdaderos ordenadores cuánticos de miles o millones de qubits?. El problema radica en la descripción del computador cuántico universal que hemos dado anteriormente. El cuarto punto es físicamente imposible. No hay nada que sea una puerta cuántica perfecta, ni hay ninguna manera de disponer de un sistema totalmente aislado. El problema es que por lo mismo que una puerta cuántica aprovecha la correlación entre diferentes qubits para llevar a cabo el cálculo, éstos qubits también estarán correlacionados con otros qubits del entorno que no pertenezcan al sistema, interfiriendo así los cálculos. Esto se conoce como decoherencia. Es muy complicado encontrar un sistema con un factor de decoherencia menor que una parte por millón cada vez que actúa una puerta. Ésto significa que la decoherencia al factorizar, por ejemplo, un número de 130 dígitos es 10^7 veces superior al máximo tolerable para llevar a cabo el cálculo.

Los ordenadores clásicos son fiables no porque sean perfectos, sino porque son inmunes al ruido. La estabilidad de un dispositivo clásico se basa en una combinación de amplificación y disipación. Usan una amplificación para pasar de un estado a otro, y después, para estabilizarse en otra posición disipan la energía en forma, normalmente, de calor. Dos ejemplos: un interruptor mecánico y un biestable (circuito lógico básico que almacena un bit). En el interruptor la amplificación la da, normalmente, un muelle o similar, de tal forma que hasta que no le den una cierta energía, el interruptor no varía, pero si lo llega a hacer, dispone de más energía que la que le hace falta para cambiar de estado. Al biestable, los transistores hacen éste trabajo. En cuanto a la disipación, en el caso del interruptor, una vez ha cambiado de estado hay un shock muy inelástico que disipa la energía en forma de calor y sonido. Si no, el interruptor iría saltando de un estado a otro. Para el biestable, hay unas resistencias que disipan la energía sobrante en forma de calor.

Sin embargo, éstos métodos no nos sirven para los computadores cuánticos. El teorema de no duplicación implica que la amplificación de estados cuánticos desconocidos es imposible, y la disipación es incompatible con la evolución unitaria.

Estas consideraciones han llevado a la aceptación general de que las reglas de la mecánica cuántica juegan contra la estabilidad de un computador cuántico y que éste no podrá funcionar nunca eficientemente. Sin embargo, podemos usar los mismos principios de corrección de errores que ya se usan en la teoría de la información clásica. Así nace la corrección de errores cuánticos (QEC).

La QEC usa unos circuitos especiales, que durante los primeros estados de la investigación no se sabía si habían de ser necesariamente perfectos. Posteriormente, se encontraron redes correctoras de errores que eran tolerantes a los errores... o sea, circuitos que corregían más errores de los que introducían con su presencia. Éstos circuitos tienen la ventaja de que permiten computadores cuánticos de tamaño arbitrariamente grande, siempre y cuando se esté dispuesto a perder una parte del espacio disponible para los circuitos correctores, evidentemente. Recientemente se han estimado los requerimientos para una computación cuántica fiable mediante QEC tolerantes a errores. Son muy altos, pero viables. Por ejemplo, un computador cuántico útil (que pueda efectuar cálculos por encima de cualquier ordenador clásico) requeriría de un orden de 1000 qubits y 10^{10} puertas. Sin QEC, ésto requeriría un nivel de ruido de 10^{-13} para cada qubit y puerta, que es totalmente imposible. Aplicando QEC sólo necesitaríamos 10^{-5} para cada qubit y puerta, es difícil pero no imposible. El efecto lateral sería que necesitaríamos un computador de 10 a 100 veces más grande.

7. Criptografía cuántica

El propósito de la criptografía es crear una comunicación segura de información. Actualmente, los algoritmos criptográficos más extendidos son los llamados de clave pública, pero su funcionamiento asimétrico: hay una clave pública para encriptar la información, y una clave privada para desencriptarla. De ésta manera se eliminó el gran problema que suponía intercambiar la clave (antes única) de encriptación y desencriptación. El problema, sin embargo, es que estos sistemas se basan en algunas operaciones matemáticas que son muy fáciles de llevar a cabo en un sentido, pero al contrario es difícil y requiera montones de cálculos... hasta ahora.

Los ordenadores cuánticos han demostrado, teóricamente aún, que son capaces de hacer los cálculos necesarios para descifrar un mensaje codificado mediante estas técnicas en un tiempo razonable. De momento, todavía no disponemos de computadores cuánticos útiles para estas tareas, pero en el momento que esto sea posible, todos los sistemas de comunicación segura que hay hoy día serán completamente inútiles.

Afortunadamente, la propia teoría que puede destruir estos sistemas nos ofrece una alternativa todavía mejor: la criptografía cuántica. Basada en el principio de incertidumbre de Heisenberg, y en el embrollamiento cuántico, la criptografía cuántica proporciona un método para que dos partes intercambien una clave de encriptación con una seguridad absoluta, garantizada por las propias leyes de la física.

Actualmente hay tres métodos de sistemas criptográficos cuánticos. Por ejemplo, hay uno basado en el embrollamiento cuántico y el teorema de Bell, propuesto por A. K. Ekert en 1990.

La idea básica es transmitir una secuencia de parejas de partículas correlacionadas, con un miembro de cada pareja conocido por cada parte. Un espía en esta comunicación tendría que leer alguna de las partículas, y retransmitirla para que su presencia siguiera desconocida. Sin embargo, el acto de la detección de una partícula de un par destruiría su correlación, y las dos partes lo podrían verificar sin ninguna dificultad usando cualquier medio de comunicación abierto, sin necesidad de mostrar los resultados de sus descubrimientos.

En la práctica, estos sistemas ya funcionan en los laboratorios, y de hecho, con la tecnología actual es posible implementar sistemas de distribución de claves sobre grandes redes de área local (algunos kilómetros) transmitiendo a 20K por segundo.

8. Perspectivas de futuro

Las palabras “computación” y “cuántica” juntas suenan muy espectaculares y han generado, y generan a veces, artículos en prensa no especializada (en física) que nos ponen en un par de décadas un computador cuántico en la mesa. Nada más lejos de la realidad. Los computadores cuánticos nunca sustituirán los computadores clásicos de la misma forma que para calcular la trayectoria de un misil no se usa la teoría de la relatividad general simplemente porque no hace falta complicarse la vida: la teoría de gravitación de Newton, más simple, es más que suficiente.

De la misma manera, la mayoría de los problemas computacionales pueden ser resueltos con la misma eficiencia por un sistema cuántico y por uno clásico. ¿Por qué complicarnos con un sistema mucho más complejo (y caro) si lo podemos hacer con un simple PC? Los ordenadores cuánticos serán máquinas muy útiles para problemas que son inabordables mediante ordenadores clásicos, pero difícilmente los llegaran a sustituir nunca.

9. Bibliografía

- Barenco A, Ekert A et al 1996 Un saut d'échelle pour les calculateurs
(La Recherche Nov 1996)
- Bucksbaum P 1999 Rydberg Sculpting
(paper QTHA1, May 97, Conference of Lasers and Electro-Optics meeting in Baltimore)
- Deutsch D, Ekert A 1993 Quantum communication moves into the unknown
(Physics World, June 1993)
- Ekert A 1995 What is Quantum Cryptography
(Center for Quantum Computation - Introductions : www.qubit.org)
- Gershenfeld N A, Chuang I L 1997 Bulk Spin-Resonance Quantum Computation
(Science vol. 275 p 350-355 17 Jan 1997)
- Preskill J 1997 Quantum Computing: Pro and Con

(pre-print quant-ph/97050032)

Preskill J 1998 Quantum Information and Computation

(Lecture Notes : <http://www.theory.caltech.edu/~preskill/ph229>)

Steane A 1997 Quantum Computing

(pre-print quant-ph/9708022)

Steane A 1997 The ion trap quantum information processor

(pre-print quant-ph/9608011)