COMPUTACIÓN CUÁNTICA

Espectroscòpia, Fotoquímica i Làsers

Curso 2008/2009

Sergi Vela Llausí

INTRODUCCIÓN

La computación cuántica es lo que se obtiene de la convergencia de dos teorías tan fascinantes como la cuántica y la computación. Los mismos conceptos que hacen que la primera haya sido tan discutida en sus inicios parece que abren un nuevo horizonte a la segunda. Seguidamente, voy a ofrecer una visión lo más simple y concisa posible y a la vez completa, a nivel de licenciado, sobre este campo.

A mediados de la década de los 40 toma impulso la ciencia de la información, pronto parece claro que el concepto propio de información contiene un significado mucho más profundo. De repente, se hace importante conocer cómo la naturaleza previene o permite que la información se exprese o sea manipulada. ¿Cuánto ocupa un bit? ¿Cuántos recursos (energía, masa,...) son necesarios para transmitir un cierto tamaño de información dado? Y qué hay del 'ruido', ¿es posible enviar satisfactoriamente información a través de un canal 'ruidoso' (entiéndase ruido como interferencia)?

En esos años, Shannon, Golay y Hamming presentan las bases de la codificación y la corrección de errores en la información. Simultáneamente, y no por casualidad, nace la computación. A mediados de los años 30 Alan Turing presenta la 'maquina universal de Turing'[(1)], basada en el trabajo de Charles Babbage en el siglo XIX.

Más allá de los usos iniciales en decriptación-encriptación y otros usos militares, la computación se hizo cada vez importante en el ámbito científico. Al principio se centró en la resolución de algunas proposiciones matemáticas, como por ejemplo la conjetura 'fuerte' de Goldbach (cualquier número entero par mayor que 2 puede descomponer como suma de 2 números primos) pero pronto se extendió y hoy en día es un recurso valoradísimo en todos los aspectos cotidianos. Los avances posteriores representaron un avance enorme en cuanto a tamaño y velocidad, pero no variaron sustancialmente el concepto esencial de lo que era una computadora. La computación cuántica, en cambio, sí que transforma el 'núcleo' conceptual de la computación.

En los años siguientes, se pone de manifiesto las importantes correlaciones entre sistemas cuánticos separados que han interaccionado en (y sólo en) el pasado. El grado de correlación en estos sistemas es mayor que el que podría ser previsto en base a cualquier ley física que describa interacciones locales.

El desarrollo de todas estas teorías llevó primeramente a la criptografía cuántica, justo cuando la computación cuántica aun se encontraba en estado 'fetal'.

El desarrollo teórico del 'qubit' por Benjamin Schumacher [(5)], y el trabajo de Deutsch en 1985 [(6)] (presentando las 'puertas cuánticas', los análogos a las puertas lógicas de la computación clásica) junto con el desarrollo de los primeros algoritmos para la computación cuántica y el desarrollo de un sistema para corregir errores en la transmisión de información de forma cuántica (mediados de los 90) decidieron a la comunidad científica a apostar por esta disciplina.

Más allá de la teoría, los esfuerzos actuales también incluyen el diseño de dispositivos físicos capaces de llevar a cabo la llamada computación cuántica. En los siguientes capítulos voy a adentrarme en los principales aspectos apuntados en esta breve introducción.

TEORÍA CLÁSICA DE LA INFORMACIÓN (TCI)

De la misma forma que en determinadas circunstancias, aproximamos algunas leyes cuánticas a sus hermanas clásicas, es necesario conocer las bases de la computación clásica y la teoría clásica de la información, antes de definir sus análogos cuánticos.

Existen tres ideas centrales en la teoría clásica de la información que deben ser transportadas al contexto cuántico:

-El problema más básico en esta teoría es obtener una medida elemental de información:

La máxima cantidad de información que puede ser almacenada por una variable que puede tomar N valores diferentes es $\log_2(N)$. De esta forma, una variable doble-evaluada contiene una unidad de información. Una unidad de información se llama *bit*. Los dos valores que puede tomar un *bit* son 0 y 1.

-Por otro lado, debemos poder codificar secuencias enteras de información mediante fuentes idénticas e independientes, en este caso bits, de forma que cualquier secuencia de bits va a transportar un cierto tamaño de información (coherente o no, dependiendo del mensaje).

-No es necesario que el codificado sea totalmente exento de error, es suficiente que la fidelidad del mensaje sea cercana a 1:

Se define fidelidad (F) como la probabilidad de que el mensaje decodificado sea idéntico al mensaje anterior a la codificación. De esta forma, la probabilidad de error será: 1-F

Si podemos enviar a través del canal más bits de los estrictamente necesarios, la fidelidad se podrá hacer arbitrariamente cercana a 1. Si no podemos usar suficientes bits de información, la fidelidad será cercana a 0. Este hecho es muy común en lo cotidiano, si alguien no es capaz de escuchar lo que digo, se lo voy a repetir tantas veces sea necesario para que el mensaje sea correctamente transmitido y por lo tanto, tenga fidelidad 1. Este teorema es particularmente interesante ya que a priori podemos compensar cualquier 'ruido' en el canal mediante una secuencia suficientemente larga de *bits*.

TEORÍA CLÁSICA DE LA COMPUTACIÓN (TCC)

En este momento, nos conciernen cuestiones como: ¿qué es computable? ¿Cuántos recursos son necesarios? La segunda pregunta la puede resolver cualquier usuario de ordenador: memoria y procesador. De forma general, la computación será difícil e inefectiva si los recursos necesarios crecen exponencialmente con el tamaño del input (cantidad de información necesaria para especificar el problema), partiendo de esta máxima, se diseñan los ordenadores

a partir del uso del sistema binario, descartando el sistema unitario (1 variable) o el decimal (10 variables). Esta elección simplifica mucho el diseño de un ordenador y su sistema de análisis. Para manipular los bits, se definen las puertas lógicas de forma que:

-Cualquier transformación de n *bits* puede ser llevada a cabo mediante sucesivas transformaciones de 1 o 2 *bits*.

-Se definen un total de 16 puertas lógicas capaces de hacer dichas transformaciones. En realidad, la acción cualquiera de estas 16 puertas lógicas puede ser reproducida mediante la combinación de 2 o más puertas lógicas idénticas o diferentes, de esta forma se puede concluir que sólo una puerta lógica es necesaria para cualquier transformación: la puerta NAND (NOT AND).

Esta visión básica de la computación nos presenta los dos componentes esenciales para que ésta tenga lugar: muchos *bits* y varias puertas lógicas (y los cables para conectarlas).

Respecto a la primera pregunta (¿qué es computable?), se define la complejidad computacional como la cantidad de pasos que una 'máquina de Turing' debe realizar para completar cualquier algoritmo y resolver el problema. En general, la complejidad computacional va a depender del tamaño del Input, si la dependencia es polinomial (clase P) el problema será en general tratable. Si la complejidad crece exponencialmente (clase NP) el problema se considerará difícil y a menudo será más eficiente testear posibles soluciones en lugar de encontrar una.

Un problema de clase NP es el de la factorización. El método actualmente más eficiente (Menezes et al 1997), necesita 10^{18} pasos para factorizar un número de 130 dígitos, que equivale a 42 días a 10^{12} operaciones por segundo. Si aumentamos el número de dígitos llegamos rápidamente a tiempos de cálculo de un millón de años con la tecnología actual. La lección a aprender en este caso es que un problema computacionalmente difícil es uno que en práctica no es imposible pero necesita demasiados recursos para su resolución.

El problema de la factorización ha adquirido mucha importancia debido a su uso en sistemas de encriptación/decriptación: Un sujeto 'A' llamado por convención Alice, emite una clave codificada que consiste en un número 'c' que puede ser descompuesto en dos números primos 'p' y 'q' que sólo conoce Alice. Un espía que no conozca 'p' y 'q' deberá factorizar 'c' para encontrarlos, si 'c' es suficientemente largo, el espía necesitaría un millón de años en decodificar las claves 'p' y 'q'. Sin embargo para un receptor autorizado llamado (también por convención) Bob, sería suficiente con conocer 'p' o 'q' para obtener a partir de 'c' la otra clave del mensaje.

TEORÍA CUÁNTICA

Antes de adentrarnos en la computación cuántica, es necesario presentar algunos conceptos inherentes a la mecánica cuántica que han sido de gran importancia en su desarrollo.

En 1935, Albert Einstein, Boris Podolsky y Nathan Rosen publican un artículo [7] en el que ponen en duda la completitud de la mecánica cuántica. En su planteamiento, y sin saberlo, explican el fenómeno del entrelazamiento cuántico. Con la colaboración de John Bell en 1964 [2], y en contra de lo que pretendían, dieron un nuevo impulso a esta disciplina, al demostrarse en los años posteriores que la mecánica cuántica es completa y la existencia de correlaciones no explicadas por fenómenos locales. Algunos experimentos que se llevaron a cabo durante las décadas posteriores para confirmar el resultado de Bell (véase [3], [4]), y por lo tanto, para demostrar la completitud de la mecánica cuántica, concluyeron que cualquier interacción local presente debería viajar a velocidades mayores a las de la luz o poseer cualidades igualmente implausibles.

Las correlaciones de EPR-Bell nos muestran que la mecánica cuántica permite realizar tareas que se encuentran más allá de las capacidades de la computación clásica. Se hace necesario construir una teoría cuántica de la información.

TEORÍA CUÁNTICA DE LA INFORMACIÓN (TQI)

A partir del planteamiento clásico se define una unidad elemental de información cuántica: el qubit. Un qubit se puede ver como un sistema con dos estados posibles tal cómo el spin de un electrón, que puede ser 'α' o 'β' o como un fotón polarizado 'horizontal' o 'verticalmente'. De esta forma, un sistema de n qubits tendrá disponibles 2^n estados cuánticos mutuamente ortogonales. En las referencias [8] y [5] se demuestra que el qubit es una medida útil de información y se define también el concepto de fidelidad, que es análogo al termino clásico. El qubit cumple los requisitos definidos en las teorías de la información.

Para simplificar la notación y hacerla más parecida al código binario, se puede escribir los dos estados ortogonales de un qubit de forma: {|0>, |1>}

Las sutilezas de la mecánica cuántica, dan lugar a unas propiedades diferentes a la mecánica clásica:

-Teorema de la no-clonación: las fotocopiadoras pueden fácilmente copiar cualquier tipo de información clásica que se les envía, sin embargo, en la mecánica cuántica eso no es siempre posible. Vamos a suponer un estado:

$\psi = c_1\phi_1 + c_2\phi_2$

Suponiendo una máquina capaz de realizar copias cuánticas, dicha máquina deberá leer el estado ψ para poder hacer una copia. Durante la lectura del estado ψ se va a producir el ya conocido efecto del colapso de la función de onda. Dicho de otro modo: a no ser que ψ, ya se encuentre en ϕ_1 o en ϕ_2, no podremos obtener un estado copia ψ'.

- Codificación de Alta Densidad: Gracias al entrelazamiento cuántico, se pueden enviar dos bits de información clásica mediante el uso de un solo qubit. Supongamos que los personajes anteriormente presentados Alice y Bob están en posesión de un par entrelazado de qubits, en el estado |00> + |11>, de esta forma, cada uno de ellos posee un qubit, pero el estado de uno

está absolutamente relacionado con el otro. En este caso, Alice podrá actuar sobre su qubit mediante la acción de una puerta cuántica escogida adecuadamente y simultáneamente alterar el estado del qubit en posesión de Bob. De esta forma, Alice y Bob obtendrían uno de los 4 estados posibles de Bell: |00> + |11>, |00> - |11>, |01> + |10>, |01> - |10>. Además, en el caso de que un observador malintencionado, llamémosle 'Eve' a partir de ahora, pudiera interceptar el qubit enviado por Alice, no podría obtener la información contenida en el mensaje a menos que también pudiera acceder al qubit de Bob.

-Teleportación cuántica: Se pueden transmitir qubits sin enviar qubits[9]!

Supongamos que Alice ha recibido un fotón en un estado $|\psi>$, desconocido para ella, y quiere comunicarle a Bob suficiente información del sistema como para poder hacer un copia exacta. En el caso de que Alice conociera de antemano que su estado $|\psi>$ pertenece a un set ortonormal de estados, podría hacer una copia exacta de su sistema (teorema de no-clonación). En el caso opuesto, que su estado $|\psi>$ incluya la posibilidad de encontrarse en 2 o más estados ($\psi = c_1\phi_1+c_2\phi_2$), Alice no podrá realizar ninguna copia exacta. Ésta última opción es la que se trata en este caso.

Una opción trivial para Alice seria enviar la partícula original directamente a Bob. En el caso de que no quiera o no pueda hacerlo, podrá hacerlo de la siguiente manera: Primero de todo, hacemos interactuar la partícula de Alice (subíndice 1) con otro sistema inicialmente en un estado conocido ψ_0:

Este sistema ψ_0 consiste en un estado singlete de dos fotones (subíndices 2 i 3) entrelazados: (voy a obviar los coeficientes de normalización de ahora en adelante)

$|\Psi_{23}^{(-)}> = |\uparrow_2>|\downarrow_3> - |\downarrow_2>|\uparrow_3>$

Alice recibe una de estas dos partículas, mientras que la otra la recibe Bob:

Partícula 1 → Alice
Partícula 2 → Alice
Partícula 3 → Bob

Las partículas 1 y 2 en poder de Alice se encontraran en los cuatro posibles estados de Bell:

- $|\Psi_{12}^{(-)}> = |\uparrow_1>|\downarrow_2> - |\downarrow_1>|\uparrow_2>$
- $|\Psi_{12}^{(+)}> = |\uparrow_1>|\downarrow_2> + |\downarrow_1>|\uparrow_2>$
- $|\phi_{12}^{(-)}> = |\uparrow_1>|\uparrow_2> - |\downarrow_1>|\downarrow_2>$
- $|\phi_{12}^{(+)}> = |\uparrow_1>|\uparrow_2> + |\downarrow_1>|\downarrow_2>$

Puesto que la partícula 2 y la 3 se van a encontrar por definición en el estado singlete, el estado de las 3 partículas se podrá escribir:

$|\Psi_{123}> = [|\uparrow_1>|\uparrow_2>|\downarrow_3> - |\uparrow_1>|\downarrow_2>|\uparrow_3>] + [|\uparrow_1>|\uparrow_2>|\downarrow_3> - |\uparrow_1>|\downarrow_2>|\uparrow_3>]$

Este estado representa las posibilidades de que las partículas 1 y 2 se encuentren con espín paralelo o antiparalelo teniendo siempre a la partícula 3 con espín antiparalelo a 2.

Expresando el estando mediante los estados de Bell, obtenemos:

$|\Psi_{123}\rangle = |\Psi_{12}^{(-)}\rangle (|\uparrow_3\rangle - |\downarrow_3\rangle) + |\Psi_{12}^{(+)}\rangle (|\uparrow_3\rangle + |\downarrow_3\rangle) + |\phi_{12}^{(-)}\rangle (|\downarrow_3\rangle - |\uparrow_3\rangle) + |\phi_{12}^{(+)}\rangle (|\downarrow_3\rangle + |\uparrow_3\rangle)$

Los cuatro posibles resultados tienen la misma probabilidad de ocurrir, por lo tanto, una medida de Alice sobre el sistema proyectara la tercera partícula en uno de los cuatro posibles estados presentados. Cada uno de estos cuatro estados estará relacionado con el estado $|\psi\rangle$ que Alice pretende transportar y entre ellos, los estados se podrán relacionar mediante una rotación del espín. Al final del proceso, Alice conocerá el estado de la partícula 1 (ha realizado una medida) y Bob tendrá a su disposición la partícula 3, sólo necesitará que Alice le transmita la información obtenida en su medida mediante un canal clásico, para que Bob aplique la rotación correspondiente y pueda obtener un fotón idéntico a 1.

TEORÍA CUÁNTICA DE LA COMPUTACIÓN (TQC)

Para empezar este capítulo, y para poder continuar más adelante, es necesario comentar brevemente las puertas cuánticas (Quantum Gates). Se trata, ni más ni menos de los análogos quánticos a las puertas lógicas. Por lo tanto, son las encargadas de modificar qubits, individualmente o secuencias de ellos. Existen infinitas puertas cuánticas, algunos ejemplos:

(Nomenclatura = $\underbrace{|\text{estado final}\rangle\langle\text{estado inicial}|}$ + $\underbrace{|\text{estado final}\rangle\langle\text{estado inicial}|}$)

Primer posible valor del qubit Segundo posible valor del qubit

Puerta identidad: $I = |0\rangle\langle 0| + |1\rangle\langle 1|$
Puerta NOT: $X=|0\rangle\langle 1| + |1\rangle\langle 0|$

De las puertas que actúan sobre pares de qubits, una de las más interesantes es la CNOT (Controlled-Not) ya que actúa sobre un qubit dependiendo del estado del otro, por ejemplo:

$|00| \rightarrow |00|$
$|01| \rightarrow |01|$
$|10| \rightarrow |11|$
$|11| \rightarrow |10|$

Se puede ver, que solo se produce variación en el par de qubits en el caso que el primero se encuentre en $|1\rangle$.

La Operación AND es otro caso peculiar puesto que involucra a 3 qubits en lo que a la práctica es una “Controlled-Controlled-Not”: Se invierte el estado del tercer qubit sólo (y sólo si) los 2

primeros se encuentran en |1>. En general, se podrá emular el efecto de cualquier puerta cuántica mediante la combinación de rotaciones de un solo qubit y puertas CNOT.

Ahora ya tenemos suficiente comprender el propósito final de la teoría, la computadora cuántica (QC). Los requisitos que debe cumplir una QC [6] [10] son:
- Cada qubit debe poder ser preparado en un estado conocido
- Cada qubit debe poder ser medido en la base de los estados |0> y |1>
- Se deben poder aplicar cualquier combinación de puertas cuánticas a discreción a un conjunto de qubits
- Los qubits no evolucionarán de cualquier forma no controlada.

A diferencia de la computación clásica, un usuario no podrá saber en qué momento la QC ha terminado un proceso. Por lo tanto, se diseñarán procesos que consistan en un número previamente conocido de pasos o se destinará un qubit no involucrado en la computación para que señalice que la QC ha terminado de procesar.

COMPUTADORAS CUÁNTICAS (QC en inglés)

Todos los procesos llevados a cabo por una computadora clásica pueden ser ejecutados por una QC. Los algoritmos para las QC exigen la preparación de estados entrelazados de qubits que son extremadamente sensibles a fenómenos externos no deseados. Por supuesto, a nadie se le ocurriría desarrollar toda una nueva tecnología para poder seguir haciendo lo mismo que una computadora clásica. El gran interés de las QC es que hay determinados procesos que pueden ser abordados de forma mucho más eficiente. Algunos de estos casos se presentan más adelante.

La aplicación a priori más obvia de una QC es la de simular otros sistemas cuánticos. Para simular un vector de estado en un espacio de Hilbert 2^n-dimensional, una computadora clásica necesita manipular vectores que contienen 2^n números complejos mientras que una QC 'sólo' necesitará n qubits, necesitando por tanto mucha menos memoria. Para simular la evolución de este sistema, ambos tipos de computación van a mostrar ser ineficientes puesto que el número de operaciones necesarias va a crecer exponencialmente con n en ambos casos (complejidad de clase NP). Por lo tanto, una QC tampoco va a permitir simular cualquier sistema físico eficientemente pero en algunos casos puede representar una mejora sustancial en recursos.

Una de las grandes ventajas de la computación quántica es el paralelismo cuántico, que en su versión más simple se puede explicar mediante el uso de una puerta NOT. En la versión clásica esta puerta tiene la propiedad de cambiar el estado de un bit de 0 a 1 y de 1 a 0. Para pasar de [01] a [10] será necesario aplicar la puerta NOT 2 veces. En la versión cuántica actúa sobre los qubits para pasarlos de α a β o de β a α. Supongamos ahora que aplicamos una puerta NOT a un estado que no es propio de S_z (componente z del momento angular de Spin) y que es combinación lineal de α_z y β_z, omitiré los subíndices z a partir de ahora. Lo que tenemos al aplicar una puerta NOT es (el cambio de signo no es relevante ahora):

$A\alpha + B\beta \rightarrow A\beta - B\alpha$

Se puede ver que esta simple operación contiene las 2 operaciones $\alpha \rightarrow \beta$ y $\beta \rightarrow -\alpha$. Es decir, hemos actuado sobre 2 qubits en un solo paso computacional. Desde otro punto de vista, con un solo procesador cuántico podemos emular el efecto de 2 procesadores clásicos. El paralelismo cuántico no es siempre posible de aplicar, los dos algoritmos siguientes son casos en que esta propiedad de la computación cuántica juega un papel muy importante.

Supongamos una función f(x) que es periódica tal que f(x)=f(x+r). Asumiendo que no hay ninguna técnica analítica para ello, lo mejor que puede hacer una computadora clásica es calcular f(x) en tantos puntos como sea necesario hasta encontrar el periodo de la función, lo que puede llegar a representar un coste muy alto en recursos.

En 1994, Peter Shor [(11)] basándose en Simon [(12)] presenta una forma elegante de resolver este problema gracias al paralelismo cuántico presentado anteriormente. La QC va a requerir de 2n qubits (n depende del tamaño del input), estos qubits estarán divididos en 2 registros diferentes y mediante el uso de transformadas de Fourier cuánticas se logra calcular, en un solo paso, la función para 2^n valores de x. Como si se tratara de una computadora clásica con 2^n procesadores. El proceso posterior para obtener el resultado no es trivial pero no lo detallare aquí. El algoritmo entero se puede consultar más detalladamente en la referencia [(13)] o en el propio artículo de Shor.

El otro algoritmo que presenta una mejora considerable es el de búsqueda en una base de datos (no-ordenada) construido por Grover en 1997 [(14)]. Los algoritmos clásicos consisten básicamente en leer la lista de N ítems para necesitar de media N/2 pasos mientras que al algoritmo de Grover le bastan $\sqrt{N}$ pasos. De nuevo, remito al lector a las referencias [(13)] y [(14)] para encontrar el algoritmo en detalle.

El número de algoritmos diseñados para la computación cuántica crece lentamente. Parece seguro predecir que existe un número muy limitado de casos específicos en los que una QC puede ser verdaderamente de ayuda. Por otro lado, un problema para el que encontrar una solución concreta es muy difícil, puede ser abordado de otra forma: testeando posibles soluciones candidatas, desde este punto de vista, el algoritmo de Grover resulta ser de gran ayuda y amplía el número de casos en los que, indirectamente, una QC podría ser útil.

DISPOSITIVOS EXPERIMENTALES

Las operaciones de lógica cuántica más elementales han sido demostradas en muchos experimentos durante los últimos 60 años. Sin embargo, si queremos contemplar una QC es necesario encontrar un sistema que permita la preparación, manipulación, evolución coherente y la medida de forma suficientemente controlable, tal y como anunciaba en el cuarto requisito de la TQC.

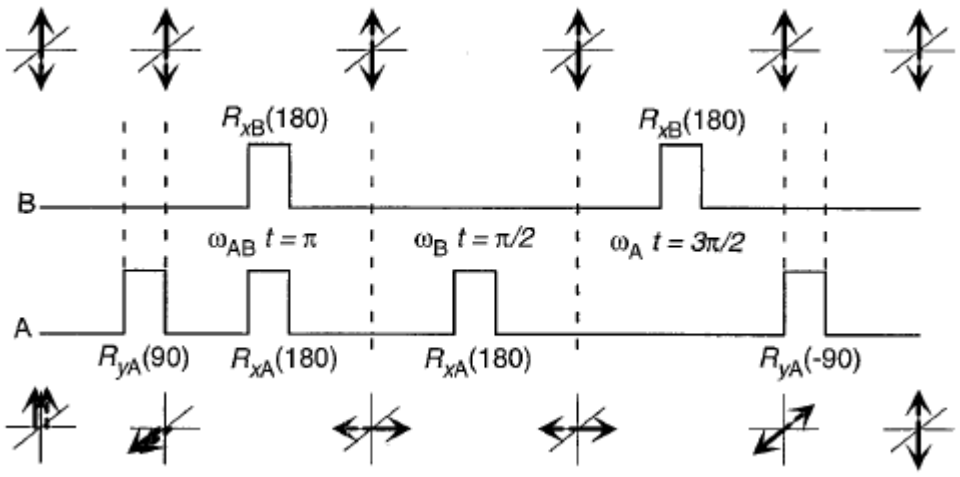
Encontrar este tipo de sistemas es extremadamente difícil. Uno podría esperar construir microchips, como si se tratara del procedimiento clásico que ha permitido de la computación sea hoy en día tan potente. Sin embargo, los sistemas cuánticos involucrados sufren

importantes procesos de interferencia que hacen que este proceder no esté permitido. No es posible con la tecnología actual poder aislar completamente un sistema cuántico, con lo que el acoplamiento de estos con el medio que los rodea produce un efecto llamado decoherencia que limita las posibilidades de la computación a unos pocos qubits.

Actualmente existen 2 tipos de sistemas particularmente interesantes para permitir la computación con entre 10 y 40 qubits. Por un lado Cirac y Zoller [15] en 1995 proponen un sistema llamado de trampa iónica y por otro lado Gershenfeld y Chuang [16] en 1997 y simultáneamente Cory, presentan un método basado en la RMN. El sistema de trampa iónico no va a ser tratado aquí así que remito al lector a las referencias en caso de interés. En cambio, el dispositivo basado en la resonancia magnética nuclear sí que va a ser descrito brevemente.

En el sistema que proponen Gershenfeld y Chuang, el procesador consiste en un líquido que contenga unas 10^{20} moléculas que deben tener un 'esqueleto' de unos 10 átomos sin insaturaciones (en su trabajo hablan del (2-3)-dibromotiofeno). Aunque el colectivo es claramente una mezcla estadística de estados, se demuestra que se va a comportar como un estado puro, de forma que podremos cumplir el requisito de 'preparación'.

Los qubits van a ser los estados de spin de cada molécula. El colectivo de moléculas se sitúa en un campo magnético y dichos estados de spin son manipulados mediante pulsos, de esta forma podremos acontecer las rotaciones de un solo qubit y las puertas CNOT, que como he comentado anteriormente son las dos únicas operaciones necesarias para emular cualquier puerta cuántica. La secuencia de pulsos aplicada para la puerta CNOT se describe en la siguiente imagen y es muy parecida a la secuencia INEPT (insensitive nuclei enhancement by polarization transfer) usada comúnmente en RMN.



En esta técnica, el resultado que mediremos será una media de resultados de todo el colectivo. Este hecho revienta los algoritmos originales pero se resuelve fácilmente aplicándoles ciertos cambios. La gran y definitiva ventaja de la RMN consiste en un tiempo de decoherencia suficientemente largo como para poder aplicar unos pocos miles de puertas cuánticas, permitiendo así el manejo de algoritmos realmente interesantes.

CONCLUSIÓN

La idea de computación cuántica ha suscitado mucha imaginación ya que sus propias palabras sugieren algo realmente potente y extraño, pero la realidad es que no va a reemplazar la computación clásica de la misma forma que la física cuántica no ha reemplazado la física clásica. Se trata simplemente de una nueva herramienta de computación que puede llevar a cabo algunas (pocas) tareas con mucha más eficiencia que las técnicas actuales.

El principal obstáculo a resolver en estos momentos es el diseño de los dispositivos experimentales adecuados, y no parece descabellado pensar que podemos necesitar toda una generación en desarrollar la tecnología necesaria para una computación cuántica a gran escala. Como mucho quizás nuestros nietos nos pidan para navidad un ordenador cuántico nuevo. En realidad, el objetivo final, mucho más modesto, parece que se va a centrar en el desarrollo de máquinas híbridas que consistan en un ordenador clásico con procesador cuántico acoplado al que sólo se recurriría en caso de necesidad.

En este trabajo se ha presentado un concepto tanto o más importante que la propia computación cuántica, el entrelazamiento cuántico. A parte de lo que supone de cara a la interpretación de las leyes de la naturaleza, los concepto en sí mismos de las interacciones no-locales y el colapso de la función de onda son suficientemente extravagantes como para que ciertos científicos especialmente creativos (algunos de ellos especialmente notables) hayan planteado teorías, a priori descabelladas, como la 'Computational Theory of Mind' que intenta explicar el funcionamiento del cerebro humano, la consciencia, el alma, lo que nos diferencia de los animales, guiados básicamente por instinto... En cualquier caso, parece que hemos descubierto otra de las herramientas que la naturaleza nos tiene preparadas para desvelar algún día la gran teoría del todo que incluya, porqué no, nuestro comportamiento.

BIBLIOGRAFÍA

(1) - Turing A. M. 1936 On computable numbers, with an aplication to the Entschneidungsproblem *Proc. Lond. Math. Soc. Ser.* **42** 230

(2) - Bell J. S. 1964 On the Einstein-Podolsky-Rosen paradox *Physics* **1** 195-200

(3) - Aspect A. 1991 Testing Bell's inequalities *Europhys. News* **22** 73-5

(4) - Aspect A. Dalibard J. and Roger G. 1982 Experimental test of Bell's inequalities usin time-varying analysers *Phys. Rev. Lett.* **49** 1804-7

(5) - Schumacher B. 1995 Quantum Coding *Phys. Rev.* A **51** 2738-47

(6) - Deutsch D. 1985 Quantum Theory, the Church-Turing principle and the universal quantum computer *Proc. R. Soc.* A **400** 97-117

(7) - Einstein A. Rosen N. and Podolsky B. 1935 *Phys. Rev.* **47** 777

(8) - Josza R. and Schumacher B. 1994 A new proof of the quantum noiseless coding theorem *J. Mod. Opt.* **41** 2343

(9) - Bennet C. H. 1995 Quantum Information and computation *Phys. Today* **48** (10) 24-30

(10) - Deutsch D. 1989 Quantum computational networks *Proc. R. Soc.* A **425** 73-90

(11) - Shor P. W. 1994 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *Proc. 35th Annual Symp. On foundations of Computer Science*

(12) - Simon D. 1994 On the power of quantum computation *Proc. 35th Annual Symp. On foundations of Computer Science*

(13) - Steane A. Quantum Computing *Rep. Prog. Phys.* **61** (1998)

(14) - Grover L. K. 1997 Quantum Mechanics helps in searching for a needle in a haystack *Phys. Rev. Lett.* **79** 325-8

(15) - Cirac J. I. and Zoller P. 1995 Quantum computations with cold trapped ions *Phys. Rev. Lett.* **74** 4091-4

(16) - Gershenfeld N. A. and Chuang I. L. 1997 Bulk spin-resonance quantum computation *Science* **275** 350-6