Recibido: martes, 18 diciembre 2007

comunicación ::
matematicalia
revista digital de divulgación matemática
Vol. 3, nos. 4-5 (oct.-dic. 2007)

Computación y comunicación cuánticas

Jesús Clemente-Gallardo
Instituto de Biocomputación y Física de los Sistemas Complejos
Universidad de Zaragoza
e-mail: jcg@unizar.es, jesus.clementegallardo@gmail.com

Pinche sobre una fórmula para ampliarla. Vuelva a pinchar sobre ella para reducirla, o pinche manteniendo pulsada la tecla [shift] para reducir todas las que permanezcan ampliadas.

1. Introducción: ¿qué es la computación cuántica?

1.1. Un poco de historia: Hilbert, Church y Turing

Dejando a un lado el magnífico precedente de Charles Babbage (1791-1871) y sus dos soberbias invenciones (su Máquina de Diferencias y su Máquina Analítica) que nunca llegaron a construirse, podemos afirmar que la ciencia de la computación moderna, tal como la entendemos hoy en día, tiene sus orígenes en el primer tercio del siglo pasado. Su nacimiento se debe a un problema matemático: desde Gottingen, David Hilbert estructura en torno a él un grupo de trabajo para estudiar los fundamentos de la Matemática y la imbricación de sus diferentes ramas. La lógica estaba llamada a ser el nexo y fundamentación de todo el sistema. Sin embargo, en 1931 Kurt Gödel demuestra que los sistemas lógicos no pueden ser perfectos, es decir, en todo sistema lógico existirán proposiciones que no pueden ser establecidas como verdaderas o falsas. Aunque este resultado echa por tierra la búsqueda de una estructuración lógica global de la Matemática, Hilbert quiere seguir desarrollando esta línea y propone un nuevo problema, denominado *das Entscheidungsproblem* (el *problema de la decisión*):

Dado un sistema lógico y una proposición, ¿cómo podemos decidir si puede considerarse verdadera o falsa?

Este problema fue estudiado intensamente durante la década de los 30 del siglo pasado. En 1936, de manera independiente y con muy poco tiempo de diferencia, se propusieron dos soluciones que luego se demostraron equivalentes. En el año 1936, en Princeton, el matemático Alonzo Church introdujo un nuevo concepto, bautizado como λ*–calculus* que permitía predecir la decibilidad de una proposición dada. Paralelamente, el jovencísimo Alan Turing completaba su doctorado en Cambridge introduciendo el concepto de la máquina que posteriormente recibió el nombre de su creador. La respuesta al problema de decisión era sencilla de plantear: aquellos problemas para los cuales la máquina completase el proceso en un tiempo finito, eran las proposiciones cuya veracidad o falsedad podían decirse. Aquellos para los que no, no lo eran. Casi inmediatamente, en 1937, Turing demostró la equivalencia de su enfoque y el de Church, a partir de lo cual su esquema ha sido el más utilizado a lo largo de los años. Pero, a todo esto, ¿qué es una máquina de Turing?

Una máquina de Turing la forma el conjunto de componentes de la figura:

una cinta infinita, dividida en celdas, en las cuales aparecen los signos de un alfabeto finito (normalmente binario, pero eso no es imprescindible);

un mecanismo de entrada/salida que permite leer el contenido de cada una de las celdas de la cinta, y escribir en ellas;

un procesador, formado por una máquina de estados, consistente en un sistema que puede tomar un número finito de valores diferentes, y un conjunto de instrucciones de la forma:

$$(m_1, E_1) \rightarrow (m_2, E_2, D/I).$$

¿Cómo funciona? El proceso es simple:

el sistema lee de la lista el contenido m_1 de la celda donde se encuentra el mecanismo de entrada-salida y pasa esa información al procesador,

éste combina el dato obtenido desde la cinta y el valor de la máquina de estados E_1 y aplica la instrucción correspondiente:

sustituye el valor de la celdilla de la cinta por m_2,

pasa la máquina de estados a la posición E_2,

y finalmente hace avanzar la cinta una posición hacia la (D)erecha o la (I)zquierda para comenzar el proceso de nuevo.

Turing usó el término *computer* para designar al sujeto que hacía las funciones que la máquina describía. Evidentemente, dada la fecha, en ese contexto el término estaba representando a un ser humano que realizaba las operaciones con lápiz y papel. Sin embargo, este esquema ha sentado las bases para las Ciencias de la Computación modernas, y, hoy en día, la máquina descrita más arriba es el modelo teórico más utilizado para describir el funcionamiento de un programa de ordenador cualquiera. Para modelizar un comportamiento más complejo, como el de un ordenador actual, es necesario sofisticar ligeramente la construcción anterior, y definir lo que se conoce como una *máquina de Turing universal* (UTM, por sus siglas en inglés), que *grosso modo* permite simular cualquier máquina de Turing simple.

Esencialmente, lo que comporta el concepto de máquina de Turing es la sistematización de la algorítmica. Sobre una máquina de Turing implementamos algoritmos que proponemos para resolver un problema dado. En principio, podríamos implementar cualquier algoritmo que deseemos sobre una de ellas (algoritmo de la suma, del producto, de la división, etc.). Esta es, en esencia, y sin entrar en detalles técnicos, la conocida como *Hipótesis de Church-Turing*, formulada en la década de los 30, y que permanece aún hoy como uno de los grandes retos de la teoría de las Ciencias de la Computación.

En los años siguientes se experimentó un extraordinario desarrollo incentivado por las necesidades militares de la Segunda Guerra Mundial y el inicio de la Guerra Fría. Turing en Gran Bretaña y John von Neumann en Estados Unidos fueron los grandes nombres de ese periodo. En especial, éste último presenta el 30 de junio de 1945 el primer proyecto para la construcción de un *very high speed automatic digital computing system* (un sistema digital de computación automática de gran velocidad) conocido como EDVAC (Electronic Discrete Variable Automatic Computer). La diferencia fundamental con la propuesta de Turing consiste en la introducción de un mecanismo que permita incluir la tarea a calcular en la memoria del sistema, de manera que el centro de control pueda acceder a ella y proceder en consecuencia. Nótese la diferencia con la propuesta anterior, en la que la secuencia de instrucciones estaba incluida de manera permanente en el procesador. Este es el modelo teórico de referencia para un ordenador actual. Por supuesto, la tecnología ha permitido avances que von Neumann no podría haber anticipado pero, desde un punto de vista teórico, la estructura por él introducida se mantiene casi inalterada. Es importante destacar que desde un punto de vista lógico no hay diferencias entre esta propuesta y la de Turing; las diferencias son puramente a nivel de eficacia. Dado un problema para ser resuelto, una máquina de Turing será capaz de resolverlo de la misma forma en que lo haría una máquina de von Neumann. La diferencia está en que la máquina de von Neumann podrá, sin cambios, resolver otros problemas de la misma forma, mientras que la de Turing deberá ser rediseñada.

1.2. Computación y sistemas cuánticos

Daremos ahora un salto en el tiempo de unos 40 años para buscar las primeras referencias a la computación relacionada con sistemas cuánticos. Durante los años 70, con la llegada de las mejoras técnicas que propician la espectacular mejora en los ordenadores que aún hoy vivimos, comienzan a desarrollarse técnicas para la simulación en ordenador de sistemas físicos. El objetivo es el estudio numérico de sistemas demasiado complejos para permitir un estudio analítico. Durante la década de los 70 se desarrolló también la idea de reproducir con la evolución de sistemas cuánticos los procesos de las máquinas de Turing clásicas. Sin embargo, a partir de lo expuesto más arriba, parece una afirmación difícil de creer. Por ejemplo, es bien sabido que los operadores booleanos (AND, OR, etc.) no son reversibles, es decir, nos transforman dos bits en uno solo, y no existe ningún mecanismo inverso. En cambio, la evolución de un sistema cuántico es reversible. ¿Cómo compaginar ambas cosas? En 1973, Bennett demostró que las máquinas de Turing podían hacerse reversibles sin perder efectividad, y construyendo sobre ello, Paul Benioff probó en los primeros años ochenta que la evolución de modelos cuánticos concretos podía reproducir el mismo proceso. En

este punto todavía no se disponía de una idea definida para diseñar un computador cuántico, pero sí que se sabía que la evolución de algunos sistemas ofrecía tanta potencia como las máquinas de Turing.

Aproximadamente en esos años Richard Feynman avanza un paso más, pero en una dirección diferente. En términos simples, en dos artículos diferentes, en 1982 y 1986, analizó la posibilidad de que un computador clásico simulara de manera fidedigna el comportamiento de un sistema físico cuántico. Justificó que tal cosa era imposible, basándose en la imposibilidad de reproducir la distribución de probabilidad cuántica de una manera clásica, y, por consiguiente, declarando la limitación que existía en el paradigma de computación de que se disponía, a la hora de realizar los cálculos necesarios para el estudio de un sistema físico. Su idea era la de conseguir un simulador cuántico, esto es, diseñar un sistema cuántico cuya evolución permitiese inferir el resultado de la evolución de otro (cualquiera) sistema físico. De nuevo, su propuesta carecía del detalle necesario, pues la descripción de cómo debía conseguirse adecuar la interacción de un sistema dado para que su evolución describiese el comportamiento de otro sistema era muy poco precisa.

En 1985, un físico británico de Oxford, David Deutsch, se planteó el problema propuesto por Feynman y su relación con las máquinas de Turing. Deutsch propuso la construcción de una máquina de Turing similar a la propuesta en 1937, pero donde todos los componentes fuesen de naturaleza cuántica, es decir, la cinta, el procesador y el sistema de entrada y salida estarían formados por sistemas que se regirían, no por las leyes de la mecánica clásica, sino por las de la mecánica cuántica. Hasta el final de las década de los ochenta (su otro artículo de referencia data de 1989), diseñó en detalle el análogo cuántico de la computación clásica a base de puertas lógicas. Ahora ya sí, por fin, se disponía de un mecanismo detallado para obligar al sistema cuántico a reproducir los pasos de los algoritmos que se quería implementar en las máquinas de Turing. Podemos considerar que Deutsch fue el primero en formular el concepto de ordenador cuántico tal como lo entendemos en la actualidad.

Finalmente, durante la década de los 90 el nuevo paradigma cristalizó, y los investigadores comenzaron a explorar las nuevas posibilidades que ofrecía. A primera vista esta idea no parece aportar nada nuevo a la idea de Turing, pero vamos a ver en la sección siguiente cómo el comportamiento cuántico va a proporcionar al sistema características completamente nuevas. La diferencia fundamental está en la posibilidad de considerar estados del sistema que sean una combinación lineal de estados. Pensemos, por ejemplo, en una máquina de Turing clásica ejecutando una operación AND (de la lógica booleana). Se trata de una operación que actúa sobre dos entradas de la cinta y devuelve como resultado el AND lógico de las mismas. Evidentemente el resultado depende de las entradas iniciales: si tenemos un 0 o tenemos un 1. En ellas, el resultado final será diferente. Para obtener todos los posibles resultados debemos considerar todas las posibles entradas (esto es, cuatro diferentes situaciones). En el mundo cuántico, sin embargo, tiene perfecto sentido considerar un estado del sistema cuántico que sea combinación lineal de los estados a los que asociamos el equivalente del valor 0 y el valor 1 en el mundo clásico. Supongamos un sistema cuántico de dos partículas, de las que sólo consideramos su espín. Éste puede tomar dos valores, por lo que habrá dos estados en el espacio de Hilbert, que vamos a etiquetar como $|0\rangle$ y $|1\rangle$, para los cuales el operador de espín tomará precisamente ese valor. Si hacemos operar la transformación AND sobre el producto de esos estados para el primer y el segundo espín, recuperamos los resultados que conocemos

En el caso del algoritmo de Grover, la ganancia no es tan espectacular, ni tiene tantas implicaciones como el caso anterior, pero es también notable. Lev Grover propuso un algoritmo para la búsqueda en una base de datos. Simplemente, se trata del problema de determinar si un determinado dato se encuentra o no en la base de datos, y dónde. El tiempo empleado en el mejor algoritmo clásico conocido escala con el tamaño de la base de datos, mientras que en el caso del algoritmo de Grover este escalado es con la raíz cuadrada de ese tamaño.

1.4. El status actual

¿Qué ha ocurrido en los últimos años? Durante la última década el crecimiento del área ha sido espectacular, tanto a nivel teórico como a nivel experimental y tecnológico. Se han propuesto varias plataformas donde desarrollar implementaciones de ordenadores cuánticos, siendo las más conocidas las de resonancia magnético-nuclear (NMR), las de trampas de iones, las de uniones Josephson y los sistemas ópticos. Aunque se hacen progresos continuamente, tener un ordenador cuántico operativo a un nivel de interés práctico se encuentra aún a varias décadas de distancia.

Como hechos más relevantes debemos destacar sin duda, desde un punto de vista experimental, la implementación del algoritmo de Schor que consiguieron científicos de IBM en el laboratorio de Alamaden (USA) en 2001. Para ello emplearon un sistema de resonancia magnético-nuclear con una molécula de 7 átomos, lo que supone que el mayor número que se podía factorizar era 15. Por poco significativo que pueda parecer el logro, significó el espaldarazo definitivo para el área.

El hecho de que se manejen sólo unos pocos qubits es una limitación inherente al uso de técnicas NMR, dado que se pueden manejar únicamente moléculas simples, normalmente con un reducido número de átomos. Es por esto que, aún habiendo sido la primera técnica empleada, dado que la tecnología NMR se ha estado usando en espectroscopía desde hace varios años y por consiguiente se conoce muy bien, poco a poco esté cediendo su lugar de privilegio a las otras técnicas mencionadas más arriba. Falta un largo camino por recorrer, estribando la dificultad principal en dos factores:

El principal es el fenómeno conocido como *decoherencia. Grosso modo* podemos explicarlo como sigue: cuando se diseña la forma de implementar el algoritmo cuántico en el sistema, es necesario suponer, en principio, que dicho

sistema se encuentra aislado del entorno. Sin embargo, esto nunca ocurre así, y, el entorno acaba finalmente por interaccionar con él en mayor o menor medida, y modificar el comportamiento que nuestro modelo le supone. Combatir estos efectos es uno de los grandes desafíos, sobre todo tecnológicos, a los que se enfrenta la disciplina.

Además, aún suponiendo que estamos trabajando en escalas de tiempo lo suficientemente pequeñas para que un buen montaje experimental nos permita trabajar controlando la decoherencia, es también fundamental poder interaccionar con el sistema de forma controlada con la suficiente precisión. Por expresarlo de forma simple, es necesario que desde el exterior podamos "mover" los qubits a voluntad, para obligar que su dinámica describa los pasos del algoritmo que queremos implementar. Esto implica ser capaces de colocar al sistema en el estado inicial para iniciar el algoritmo, ser capaz de llevarlo al punto final del mismo y finalmente extraer del estado final la información deseada.

2. ¿Qué tiene el mundo cuántico para conseguir esto?

Como hemos dicho más arriba, la gran revolución de la computación cuántica consiste en considerar como cuánticos los componentes de una máquina de Turing. ¿En qué consiste la revolución entonces? Si la máquina va a operar de la misma forma, ¿qué ganamos? Para responder a esta pregunta vamos a hacer una pequeña digresión y explicar algunas propiedades de la teoría cuántica.

2.1. La Mecánica Cuántica

Es bien sabido que la mayoría de los fenómenos físicos de escala macroscópica pueden ser descritos con las leyes de la Mecánica Clásica. Las leyes de Newton (o alternativamente los principios variacionales) dan cuenta con bastante exactitud del comportamiento de la materia con la que podemos interaccionar en nuestra vida diaria. Sin embargo, a escala molecular, atómica y subatómica esto deja de ser cierto.

¿Qué ocurre desde el punto de vista matemático? En el caso de la mecánica clásica, los estados de un sistema se modelizan como puntos de un espacio de estados, que normalmente tiene una estructura de variedad diferenciable (con frecuencia, un espacio vectorial de dimensión finita). La dinámica de las partículas de nuestro sistema físico pasan a ser descritas como curvas en el espacio de estados, y los problemas consisten, normalmente, en ser capaz de obtener las curvas que son soluciones de alguna ecuación diferencial: Por ejemplo, en el caso más simple en que consideramos el movimiento de una partícula en el espacio, sabemos que

$$\vec{F} = \frac{d\vec{p}}{dt} = m\frac{d^2\vec{x}}{dt^2},$$

donde $\vec{F}$ representa la fuerza y $\vec{p}$ el momento lineal de nuestra partícula, que asumimos puntual y de masa m. Las magnitudes físicas pasan a ser funciones sobre el espacio de estados, y por consiguiente puede conocerse el valor de cualquier magnitud (por ejemplo, la energía o el momento angular de una partícula) evaluando la función que lo representa en el punto donde se encuentra dicha partícula.

En el mundo cuántico, la situación es muy diferente. Los estados de un sistema cuántico van a estar definidos como vectores ψ de un espacio de Hilbert H, complejo y de dimensión infinita. Estos vectores, normalmente elementos de un espacio de funciones, no tienen una interpretación física directa. Sólo el módulo al cuadrado de esa función (recordemos que aunque es compleja, este módulo al cuadrado será una función real) va a tener un sentido físico bien definido: en términos simples podemos decir que su valor en un punto x del dominio representará la densidad de probabilidad de que un experimento detecte la partícula precisamente en ese punto. Por coherencia, pediremos entonces que la norma de las funciones que representan los estados del sistema sean la unidad. Esto traduce matemáticamente la propiedad de que si consideramos todos los posibles puntos del dominio (llamémoslo, por ejemplo, Ω) que estamos estudiando, la partícula debe encontrarse en él con una probabilidad del 100%.

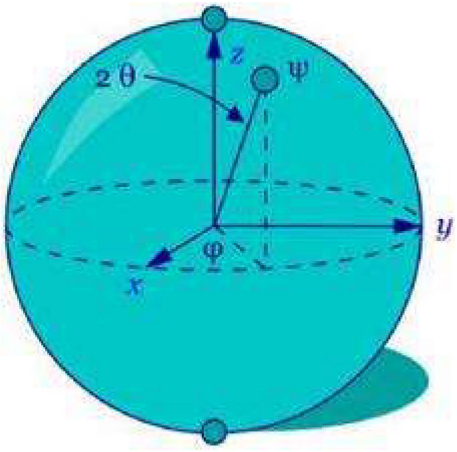
Las magnitudes físicas estarán ahora representadas, no por funciones, sino por operadores definidos sobre el espacio de Hilbert H. Tendremos así un operador que representará la energía, otro que representará el momento lineal, otro que representará la posición de la partícula, etc. En el laboratorio, lo que hacemos al medir la, digamos, energía de un sistema representado por el vector ψ, es en realidad evaluar la acción del operador que representa la energía (que se denomina *Hamiltoniano*) sobre el estado ψ (esto nos dará otro elemento del espacio de Hilbert) y luego calcular la proyección de este nuevo estado sobre el estado ψ. El número así obtenido (que siempre es real) es lo que consideramos la energía del sistema.

Es de esta forma que nuestra máquina de Turing cuántica opera: las transformaciones que definen el algoritmo corresponderán a actuar sobre los estados con operadores convenientemente escogidos. La implementación de un algoritmo corresponderá, pues, a una secuencia de estos operadores que llevan el estado inicial a un cierto estado final. La lectura del resultado es un proceso más complicado que en el caso clásico, pero podemos decir, *grosso modo*, que se hará proyectando sobre ciertos estados, como hemos comentado más arriba. Y un aspecto muy importante del proceso, es que el proceso de medida va a modificar el estado del sistema. Es un proceso complejo, pero se puede justificar bien desde el punto de vista estadístico. Imaginemos que tenemos una partícula cuya posición medimos en un

cierto instante de tiempo. Vamos a obtener un resultado concreto, digamos que x_p. Evidentemente, si medimos más veces obtendremos, en general, valores diferentes, pues ya hemos dicho que la partícula tiene una determinada probabilidad de estar en todos los puntos del dominio. Sin embargo, una vez que hemos medido, y asumiendo que la partícula no interacciona con nada, la partícula debe seguir estando en el punto x_p. Es decir, tenemos una probabilidad del 100% de encontrarlo en ese punto. Pero esto supone que la función que representaba el estado ha tenido que cambiar, pues sabemos que la probabilidad antes era diferente. Este hecho es una de las propiedades fundamentales de la mecánica cuántica, y veremos más tarde que tiene implicaciones importantes en los problemas que estamos analizando.

2.2. Los qubits: los bits cuánticos

Ahora que ya sabemos cómo describir un sistema cuántico en general y algunas de las peculiaridades que esa descripción presenta, vamos a ver rápidamente qué tipo de situaciones nos van a aparecer cuando trabajemos con un ordenador cuántico. Ya hemos visto que la propuesta de Deutsch consiste en la implementación de una máquina de Turing empleando para ello componentes de naturaleza cuántica. En una máquina de Turing clásica, la descripción de los estados del sistema se realiza usualmente empleando un sistema binario, formado por unidades que pueden tomar sólo valores 0 ó 1: los bits. Sobre ellos definiremos las transformaciones que implementarán el algoritmo que la máquina de Turing deba realizar. Por consiguiente, para trabajar con una máquina de Turing cuántica, debemos, en primer lugar, caracterizar los análogos cuánticos de estas unidades. En la jerga técnica, serán denominados de forma genérica *qubits* (aunque en caso de considerar sistemas no binarios, puedan aparecer otras denominaciones). Si queremos mantener el alfabeto del sistema como binario, vamos a tener que considerar lo que se denominan *sistemas cuánticos de dos niveles*. Se trata de sistemas en los cuales vamos a poder considerar dos estados bien definidos con respecto a alguna magnitud (la energía, el espín, etc.), que denotaremos como $|0\rangle$ y $|1\rangle$, y todas sus combinaciones lineales. Es, pues, un sistema de dimensión finita, a diferencia de los sistemas cuánticos usuales, y por consiguiente mucho más sencillo a la hora de trabajar con él. Si consideramos la ligadura ya comentada sobre el cuadrado de la función de onda (en este caso la función de onda no es más que un punto en un espacio vectorial complejo de dimensión 2) y la independencia de la fase global de la misma, es inmediato probar que los estados son en realidad puntos en una esfera real de dimensión dos. Esta es la llamada *esfera de Bloch*. Por consiguiente, tenemos un conjunto de estados que se corresponden con los puntos:



Vemos aquí, por tanto, una de las diferencias de la computación cuántica con respecto a su análogo clásico: donde en el marco clásico considerábamos sólo dos estados discretos (un bit puede tener dos valores, 0 ó 1, y sólo esos dos), en el mundo cuántico vamos a poder jugar con toda una esfera de posibles valores. Esta mayor riqueza de la descripción está en la base del paralelismo que antes mencionábamos.

2.3. Sistemas cuánticos compuestos y entrelazamiento

La característica más interesante para nosotros ahora es, sin embargo, la forma en que el espacio de estados formado por dos partículas se obtiene a partir de los espacios de estados de cada una de las partículas individuales. En el caso de la mecánica clásica, la composición de sistemas se traduce en el producto cartesiano de los espacios de estados de cada una de las partículas. En cambio, en el mundo cuántico la composición se traduce en el producto tensorial de los espacios de Hilbert de los factores. Esto tiene una implicación fundamental para el problema que nos ocupa: consideremos dos estados de cada uno de los subsistemas $\{\psi_1^A, \psi_1^B, \psi_2^A, \psi_2^B\}$ y los correspondientes estados

$$\psi^A = \psi_1^A \otimes \psi_2^A , \qquad \psi^B = \psi_1^B \otimes \psi_2^B .$$

Los vectores ψ^A y ψ^B representan estados del sistema de dos partículas. Pero son también estados donde se pueden leer (proyectando sobre el subespacio correspondiente) el estado de la partícula 1 y el de la partícula 2. Esto es lo que ocurre en el caso de un sistema de partículas clásico: en un sistema de partículas podemos reconocer el estado de las

partículas individuales. Sin embargo, en el espacio de Hilbert correspondiente al espacio de las dos partículas existen también estados como

$$\phi = \frac{1}{\sqrt{2}}(\psi^A + \psi^B) = \frac{1}{\sqrt{2}}(\psi_1^A \otimes \psi_2^A + \psi_1^B \otimes \psi_2^B).$$

Estos estados del sistema compuesto tienen perfecto sentido y cumplen con todas los requisitos para ser considerados tales. Sin embargo, en general no existirán estados del primer sistema y del segundo tales que ϕ sea un producto de ellos. Nótese que ϕ es un estado del sistema compuesto, en el que las dos partículas que lo componen han dejado de tener entidad. Podemos considerar el estado del compuesto, pero ya no de los constituyentes. Este fenómeno, inherente a la descripción cuántica de la Naturaleza, se conoce como *entrelazamiento* (*entanglement* en inglés), y es una de las características más importantes de los estados de un sistema cuántico.

En particular, la relevancia para el problema que nos ocupa es enorme. Quizá la aplicación más popular y simple es la conocida como *superdense coding*. Sin entrar en muchos detalles, podemos imaginar un estado entrelazado $\phi = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle$ compartido por dos personas. Imaginemos que una de las personas quiere comunicar dos bits de información a la otra. En el marco clásico, es necesario transmitir los dos valores, después de haberlos medido; sin embargo, en el marco cuántico es suficiente con trabajar con uno. ¿Cómo hacerlo? Evidentemente, queremos transmitir uno de los valores del conjunto $\{(00), (01), (10), (11)\}$. Si actuamos sobre el primer qubit del estado ϕ (el que suponemos pertenece a uno de las dos personas), podemos hacer que el estado resultante pueda tomar cuatro valores distintos haciendo lo siguiente:

- no actuar sobre el estado. Podemos considerar que esto transmite el estado (00).
- no actuar si tenemos un $|0\rangle$ y cambiar el signo si tenemos un $|1\rangle$. En este caso ϕ se convierte en $\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle$. Podemos considerar que esto transmite el estado (01).
- transformar el estado $|0\rangle$ al $|1\rangle$ y el $|1\rangle$ a $|0\rangle$. En este caso ϕ se convierte en $\frac{1}{\sqrt{2}}(|1\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle$. Podemos considerar que esto transmite el estado (10).
- transformar el estado $|0\rangle$ al $-|1\rangle$ y el $|1\rangle$ a $|0\rangle$. En este caso ϕ se convierte en $\frac{1}{\sqrt{2}}(|1\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle$. Podemos considerar que esto transmite el estado (11).

De esta manera, basta con que el emisor actúe sobre su qubit para que el receptor pueda recibir cuatro posibles valores, que evidentemente tendrá que detectar midiendo adecuadamente el sistema.

3. La comunicación cuántica

Es esta una disciplina que, si bien no está directamente relacionada con la computación, ha experimentado un enorme desarrollo durante los últimos años impulsada por el interés suscitado por ella. Como ocurre en el caso anterior, las bases de la teoría son relativamente similares a su análogo clásico, pero la naturaleza cuántica de los sistemas sobre los que se implementa va a dotar al proceso de comunicación de características enteramente nuevas.

Desde un punto de vista clásico, el proceso de comunicación es simple. Un emisor codifica cierta información en un conjunto de bits. Una vez hecho esto, la información es simplemente una secuencia de números en formato binario. ¿Cómo transmitir la información? Basta un mecanismo que permita enviar la secuencia de números. Este es el proceso empleado en cualquier comunicación en la actualidad: enviamos una señal de televisión, una página web por Internet, una llamada o un mensaje por el teléfono móvil, etc. Los distintos ejemplos difieren simplemente en el código empleado y en el protocolo que se emplea para acelerar el proceso y asegurarse de que la transmisión tiene éxito.

La comunicación cuántica consistirá, por tanto, en la transmisión de información entre dos puntos, a través de cualquier medio. Llamaremos *canales* a estos métodos de transmisión. Según su naturaleza, los clasificaremos en canales clásicos o cuánticos. En realidad, podemos considerar ambos como cuánticos, pero restringir el tipo de transformaciones asociados a cada uno. Desde este punto de vista parece que estamos ante un esquema equivalente al caso anterior; pero no es así, pues el hecho de trabajar con sistemas cuánticos va a hacer que presente peculiaridades interesantísimas. Veamos dos de las más conocidas para terminar este brevísimo resumen.

3.1. Primer ejemplo: teleportación

Sin duda una de las aplicaciones que recibe más interés público de la comunicación cuántica es la llamada *teleportación*. Por las fuertes connotaciones asociadas a la ciencia ficción, es necesario explicar en detalle en qué consiste este fenómeno. Supongamos que tenemos cierto estado de un qubit que, en principio, desconocemos. Al tratarse de un solo qubit, el estado desconocido será un elemento del espacio de Hilbert correspondiente H. La teleportación consiste en ser capaz de transmitir el valor de ese estado entre los dos puntos. Es relativamente sencillo

probar que si entre emisor y receptor se comparte un par de qubits en un estado entrelazado, y dicho par se acopla a un tercer qubit “libre”, forzando una interacción particular entre los qubits del par y el qubit libre se puede hacer que el estado del qubit libre del emisor pase al receptor; esto es, una secuencia de operaciones precisas hacen que uno de los qubits del receptor tome el mismo valor que el qubit libre del emisor. Para ello basta que el emisor envíe (por un canal clásico) el valor de dos medidas (dos bits, en realidad) y el receptor realice una operación concreta para cada uno de los posibles valores que puede recibir. Desde este punto de vista, hemos “teleportado” el estado del qubit de emisor a receptor. Aunque existen ejemplos más sofisticados, las imágenes que la ciencia ficción proporciona están muy alejadas de la realidad científica.

3.2. Segundo ejemplo: criptografía cuántica

Finalmente vamos a considerar otro tópico muy frecuente en la comunidad como es la *criptografía cuántica*. Esencialmente, las aplicaciones consideradas hasta ahora suponen la aplicación de técnicas similares a las comentadas más arriba al estudio de los procesos de comunicación. En éstos, uno de los problemas habituales es el de la seguridad. Sabemos por ejemplo que cuando accedemos a nuestro correo electrónico o, sobre todo, a nuestro banco por Internet, es muy importante el hecho de que cuando enviamos nuestras contraseñas estamos ante un potencial riesgo. Si alguien intercepta la comunicación, podría en principio acceder a datos confidenciales. Es por esto que en el marco de la computación clásica se ha desarrollado un amplio elenco de herramientas para garantizar la privacidad del proceso de comunicación. Sin embargo, siempre sabemos que existe un riesgo. Pero eso es únicamente en el marco de la teoría clásica.

En el mundo cuántico la situación es un poco más esperanzadora. Y de nuevo debido al uso del entrelazamiento y las propiedades de la medida en sistemas cuánticos que comentamos más arriba. En términos simples, la idea es la siguiente: consideraremos que el mensaje que queremos transmitir está codificado en un estado entrelazado, y que emisor y receptor tienen un protocolo de decodificación que es sensible al estado sobre el que actúa. Esto es, sólo codifica o decodifica la información si el estado es uno particular. Supongamos ahora que somos capaces de separar el emisor y el receptor, pero el estado entrelazado sigue existiendo. ¿Qué ocurriría ahora si alguien intercepta esa comunicación? La manera de interceptar la comunicación es, esencialmente, interaccionar con el estado (dado que se debe emplear alguna técnica para poder decodificar la información que contiene, pero para eso se debe tener acceso a él). Sin embargo, cuando se interaccione con el estado (midiendo sobre él el valor de alguna magnitud, por ejemplo) vamos a modificarlo: al medir algún observable la función de onda del estado se modificará y pasará a ser una en la que el valor del observable sea el obtenido con un 100% de probabilidad, tal como explicamos más arriba. Pero si esto ocurre, el receptor ya no podrá recuperar la información y sabrá que ésta ha sido interceptada.

Existen varios protocolos de comunicación segura, siendo los más conocidos los de Charles H. Bennett y Gilles Brassard (ejemplo de *quantum key distribution* conocido como BB84) y el de Arthur Ekert (conocido como Eckert91). A diferencia de la computación cuántica, las técnicas de criptografía cuántica se emplean ya de forma eficiente, incluso a nivel comercial. En marzo de 2007 se organizó un experimento para mantener una comunicación segura en Los Alamos (EEUU), empleando el algoritmo BB84 a lo largo de 148.7km de fibra óptica. Similares experimentos tuvieron lugar en 2006 en las Islas Canarias (sobre 144km entre La Palma y Tenerife, se implementó también la técnica de quantum key distribution empleando fotones polarizados y el algortimo Eckert91, y este mismo año se ha conseguido implementar también el BB84). Existen además tres empresas que comercializan sistemas de este tipo, usados sobre todo por entidades bancarias. Como dato curioso, en las últimas elecciones suizas, en octubre de 2007, se emplearon máquinas de una de esas empresas para el envío de los resultados de voto a la sede central de cómputo.

4. Conclusiones

A lo largo de estas pocas líneas hemos pretendido presentar el origen y las principales características de la computación y la comunicación cuánticas. Podemos resumir lo expuesto en los siguientes puntos:

Un ordenador cuántico consiste en la implementación, usando elementos de naturaleza cuántica, de los modelos de computación clásica.

La naturaleza cuántica de los componentes dota a estos elementos de propiedades completamente nuevas que permiten resolver problemas inabordables desde el punto de vista clásico. Podemos destacar entre estas propiedades:

primero, la superposición de estados. Donde un sistema clásico sólo tiene dos posibles estados (0 ó 1), un sistema cuántico presenta toda una esfera de posibles estados (la esfera de Bloch). Esto da lugar a sistemas de cómputo que son paralelos de manera natural.

segundo, el entrelazamiento. Esta propiedad, inherente a la descripción cuántica de la Naturaleza, tiene muy importantes consecuencias en la comunicación cuántica (hemos visto algunas), pero también en propiedades de computación.

La comunicación cuántica se define de manera análoga a la comunicación clásica, pero de nuevo la naturaleza cuántica de los componentes ofrece propiedades inaccesibles en el marco clásico, como la teleportación de estados, o la criptografía cuántica.

En cuanto al futuro, mientras que la comunicación cuántica es ya una disciplina madura con aplicaciones funcionales incluso a nivel comercial, la construcción de un ordenador cuántico que trabaje en un rango interesante desde el punto de vista práctico está todavía a varios años de distancia. No obstante, el vertiginoso crecimiento que ha experimentado la disciplina en las últimas dos décadas pueden traer sorpresas antes de lo que todos esperamos.

Referencias

Artículos de revisión e introducción:

A. Galindo, M.A. Martín-Delgado: Information and Computation: Classical and Quantum Aspects. *Rev. Mod. Phys.* **74** (2002), 347.

A. Galindo: *Del bit al qubit*. Conferencia inaugural del curso 2001-2002 en la UCM [Disponible en http://teorica.fis.ucm.es/~agt/conferencias/leccionweb.pdf].

Artículos clásicos:

A. Turing: On computable numbers, with an application to the Entscheidungs-problem. *Proc. London Math. Soc.* (2) 42 (1936), 230-265; correction ibid. 43 (1937), pp. 544-546.

P.A. Benioff: The computer as a physical system: a microscopic Hamiltonian model of computers as represented by Turing machines. *J. Stat. Phys.* 22 (1980), 563-591.

R. Feynman: Simulating physics with computers. *Int. J. Theor. Phys.* 21 (1982), 467-488.

D. Deutsch: Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Roy. Soc. London A* 400 (1985), 97-117.

D. Deutsch: Quantum computational networks. *Proc. Roy. Soc. London A* 425 (1989), 73-90.

P. W. Shor: *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. En *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science,* IEEE Computer Society Press, Los Alamitos, CA, 1994, pp. 124 [e-print quant-ph/9508027].

L. Grover: *A fast quantum mechanical algorithm for database search*. En *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, PA, 1996, pp. 212-221.

Libros introductorios:

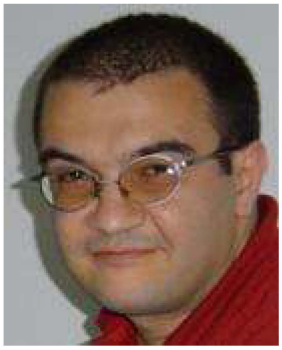
J. Stolze, D. Suter: *Quantum Computing. A short course from theory to experiment*. Wiley-VCH, 2004.

Libros más avanzados:

M. Hirvensalo: *Quantum computation* (2nd. edition). Springer, 2003.

A.Y. Kitaev, A.H. Shen, M.N. Vyalyi: *Classical and quantum computation*. Graduate Studies in Mathematics, vol. 47. AMS, 2002.

M.A. Nielsen, I.L. Chuang: *Quantum computation and quantum information*. Cambridge Univ. Press, 2000.



Sobre el autor

Jesús Clemente-Gallardo se doctoró en Física (especializado en Física Matemática) por la Universidad de Zaragoza en 1999. Tras cinco años en el extranjero (en universidades de Francia, Holanda y Portugal) se incorporó en 2004 al Instituto de Biocomputación y Física de los Sistemas Complejos de la Universidad de Zaragoza como Investigador Ramón y Cajal. Sus líneas de trabajo son la teoría de control geométrico, la formulación geométrica de la mecánica cuántica, la teoría de control de sistemas cuánticos y sus aplicaciones a computación cuántica.