Los Mitos del Computador Cuántico

El sueño de construir un poderoso computador no se ha desvanecido. En los cinco últimos años, los avances que se han producido en los laboratorios de física (fotones atrapados en trampas electromagnéticas, iluminación selectiva con luz láser, entre otros) han levantado una notable expectativa de la que se han hecho eco los medios de comunicación, tanto científicos como divulgativos. Sin embargo, todavía nadie es capaz de pronunciarse con seguridad sobre el futuro de tan formidable máquina.

En este momento ya hay trabajando más de un centenar de científicos de todo el mundo en el computador cuántico, no sólo bajo el paraguas financiero de los estamentos universitarios, sino también con el apoyo económico de importantes compañías comerciales. Pero, de momento, parece ser que el proyecto sigue desarrollándose entre los papeles de los teóricos y que los avances prácticos se encuentran con dificultades muy graves. "Ha habido un importante avance en cuanto a las teorías en torno al poder potencial de la computación cuántica y en cómo esta puede superar a la computación clásica -dice Di Vicenzo-, y también se ha progresado mucho en la comprensión teórica de las condiciones experimentales necesarias para que la computación cuántica llegue a ser una realidad. Por ejemplo, actualmente ya existen amplias teorías para saber cómo llevar a cabo la corrección de errores en la computación cuántica. En diversas áreas de la óptica cuántica, física atómica, superconductividad y magnetismo se valoran las posibilidades de efectuar experimentos para poner a prueba estas ideas".

En el ámbito del sadomasoquismo consumista en que nos ha sumido el mercado informático hay quien se atreve a decir que el computador cuántico pronto dejará fuera de servicio a las viejas máquinas que estamos utilizando actualmente. Si alguien se acaba de comprar un Pentium o está ahorrando para cuando salga el primer Power PC, puede hacer oídos sordos a esta banal agresión, ya que, de momento, el computador cuántico sólo existe en la mente de los físicos y nadie sabe a ciencia cierta cuando será una realidad, si es que llega a serlo algún día "Es absolutamente imposible saberlo -opina Di Vicenzo-, ya que las actuales posibilidades experimentales sólo nos permiten hacer computadores cuánticos pequeños, con no más de una pareja de bits. Es posible, de acuerdo con estos resultados, que la próxima generación de experimentos nos permita acceder a la computación cuántica. Pero no es predecible. El actual estado de la experimentación, en mi opinión, tardará todavía varios años en llegar a realizarse". Es muy posible que lo que haya confundido a un amplio sector de público sea el haber llamado computadora clásica a la que utilizamos actualmente. La palabra clásico tiene ciertas connotaciones de antiguo. Pero aquí, el calificativo de clásico se utiliza como contraposición al de cuántico y hace referencia a dos diferentes esquemas físicos de entender la realidad.

Carrera de miniaturización

Desde las lámparas de diodo hasta los microcircuitos integrados, los componentes básicos de los ordenadores se han ido reduciendo de tamaño de forma espectacular. Pero en esta carrera de miniaturización se empieza a vislumbrar la línea de meta. Esto es debido a que el mundo microscópico se rige por leyes distintas a las del macroscópico. La mecánica clásica deja de tener validez y el comportamiento de las partículas elementales hay que describirlo por medio de la física cuántica. Una teoría que con frecuencia hace tambalear nuestra lógica habitual. Es por esta razón que las todavía incipientes "tripas" del computador cuántico no son fáciles de entender y menos de explicar. "Cuando el estudiante de física se enfrenta por primera vez a la mecánica cuántica sufre una crisis que puede durarle de uno a tres años -dice Rolf Tarrach-, por esto no podemos esperar que hablar del computador cuántico sea una asunto fácil, ya que se adentra en los aspectos más sutiles de la mecánica cuántica".

El "qubit" (quantum bit)

El bit es la unidad fundamental en la arquitectura de un ordenador. Es un elemento físico capaz de almacenar una información tan simple como un 0 o un 1, y que puede materializarse en el hecho de que un condensador esté cargado o descargado. Algunos estados físicos de las partículas elementales también pueden ser utilizados para este fin. Por ejemplo, en un átomo, el electrón que se mueve alrededor de una órbita de mínima energía puede ser excitado por un fotón emitido por un láser y pasar a una órbita superior. Estos dos estados del electrón representan el 0 y el 1. Pero así como en el computador clásico los estados 0 y 1 son valores discretos, alternativos, en el sentido de que es uno u otro, en el mundo microscópico el estado de la partícula puede estar en los dos estados simultáneamente, en una especie de estado borroso entre 0 y 1. Es más, teóricamente es posible preparar a la partícula en cualquiera de los infinitos estados que van del 0 al 1. Este "quantum bit" o "qubit" (término acuñado por Schumacher en 1995) tendría así una capacidad potencial de información abrumadora, capacidad que puede verse incrementada por otro de los fenómenos no menos extraño de la mecánica cuántica: el llamado "entanglement".

El "entanglement" es uno de los conceptos más escurridizos de la física cuántica y ni siquiera vamos a intentar definirlo, pero sí vale la pena hablar de él, aunque sea dando una visión muy superficial. Cuando dos partículas se han generado en un mismo proceso (como en la desintegración en un positrón y un electrón) quedan indefectiblemente relacionadas entre sí formando subsistemas que no pueden describirse separadamente. No es posible hablar de uno sin hablar del otro. "Son como hermanos gemelos -explica Anna Sanperal-, aunque uno esté en Japón y el otro en la Argentina; sabemos que si al primero le ha crecido el pelo de color negro, al otro también, aunque no lo veamos. De hecho, no adquiere este carácter hasta que no hacemos una medición sobre él. Esta propiedad permite poner a trabajar a los "qubits"

como ordenadores masivamente en paralelo, aumentando así su capacidad computacional hasta límites que serían impensables con los ordenadores actuales."

Sin embargo, todo este maravilloso sueño computacional, sucede en intervalos de tiempo que, en el mejor de los casos, no exceden de la millonésima de segundo, lo que plantea algunos problemas, que son sólo el inicio de la pesadilla en la que acaba por convertirse el sueño del computador cuántico.

El drama del "qubit"

En mecánica cuántica no es posible hacer una observación sin alterar el estado cuántico de aquello que queremos observar. Además, esa alteración no está determinada, sino que depende ya de un cierto cálculo de probabilidades. Si sabemos que, a una hora determinada, un coche ha salido de Barcelona y se dirige por la autopista en dirección a Girona a 100 km por hora, podemos predecir a qué altura del recorrido se encuentra al cabo de media hora. Si tratamos de comprobarlo, ya sea mediante un telescopio o sobrevolándolo con un helicóptero, esperamos encontrarlo a una determinada distancia de su lugar de partida. Cuánticamente hablando, tendríamos la increíble sorpresa de que existe una cierta probabilidad de que el coche en cuestión se encuentre, en ese momento, en una carretera vecinal de las cercanías de Guadalajara, sólo por el hecho de haber intentado comprobar dónde estaba. Esto, en mecánica cuántica, sucede de golpe, sin solución de continuidad. Cuando el mundo macroscópico interacciona con el microscópico se produce lo que en términos técnicos se llama colapso o pérdida de coherencia. Es importante recalcar el hecho de que este fenómeno forma parte de la misma naturaleza de las cosas. Pretender perfeccionar los aparatos de medida para evitar la pérdida de la coherencia sería como prepararse físicamente en un gimnasio para conseguir la suficiente velocidad para alcanzar nuestra propia sombra.

Es en este punto donde el maravilloso "qubit" vive su primer drama. Cuando hacemos una medición para conocer la información que guarda, nos da el esquinazo. El "qubit" no sólo no quiere relacionarse con el usuario, sino que tampoco quiere saber nada con su entorno más inmediato, con su mera ubicación física. En conclusión, ha de permanecer en un total aislamiento del mundo macroscópico que le rodea. Esta es una de las grandes pesadillas de la ingeniería de la computación cuántica, aunque no la única. Si el "qubit" no se deja mirar, tampoco se deja copiar, operación esta que, como todo el mundo sabe, es vital en los diferentes manejos informáticos.

¿Una entelequia sin esperanza?

Diseñar el hardware del computador cuántico parece una tarea tan difícil como conseguir que un elefante aprenda a colocar la cristalería fina en el lavavajillas. Ante tantas dificultades cabe preguntarse si merece la pena el esfuerzo que una masa, ya

crítica, de científicos está llevando a cabo en todo el mundo para algo que, en ciertos aspectos, es casi como buscar la piedra filosofal. ¿Es el ordenador cuántico una moda en cuya implantación están jugando un papel clave los medios de comunicación? "Lo ideal sería que la prensa informase sin prometer tantas cosas fantásticas, la mayoría de las cuales son meras hipótesis, aun a riesgo de que esto suponga vender menos -afirma Rolf Tarrach-. Aunque probablemente sea una entelequia, alrededor del computador cuántico se están haciendo cosas muy interesantes. A veces se puede hacer un trabajo serio partiendo de una idea descabellada; en cualquier caso, hay que saber distinguir siempre entre fantasía y realidad".

Quizá el aspecto más interesante, incluso a escala filosófica, que encierra esta investigación es la posibilidad de conocer las leyes que rigen el brusco salto entre los dos mundos, el macroscópico y el microscópico, entre la teoría clásica y la cuántica. "Para construir un computador cuántico que sea útil tenemos que tener muchos 'qubits', es decir, nos tenemos que acercar al límite en donde se encuentran estas teorías -dice Ignacio Cirac-. Por otro lado, la computación cuántica está relacionada con otros fenómenos 'raros' de la mecánica cuántica como el teletransporte; los avances producidos en este terreno pueden ser trasladados a otras áreas".

Criptografía cuántica

Bancos, estamentos militares, y compañías telefónicas son las entidades no universitarias que financian la investigación del computador cuántico. Y todos ellos con un mismo objetivo: romper el sistema criptográfico del RSA.

Actualmente, la criptografía de clave pública basa su fuerza en la imposibilidad de factorizar grandes números como producto de números primos. Por ejemplo, el número 15 se hace público y las claves secretas son los números primos 3 y 5 cuyo producto es 15. Las claves públicas utilizadas son del orden de 65, 150 o hasta 1.024 bits, esta última en criptografía militar. La única manera de factorizar un número es mediante el algoritmo de la división, para el que los computadores actuales son tan lentos que se calcula que para factorizar uno solo de estos grandes números se tardaría un tiempo equivalente a la edad del Universo. Peter Shor, de AT&T Bell Laboratories, ha creado un algoritmo, teóricamente implementable en un computador cuántico, que utiliza la superposición de estados y que posibilita a los "qubits" trabajar masivamente en paralelo. Pecando de imprecisión, pero intentando ganar en claridad, podríamos decir que esto sería como convertir a los "qubits" del ordenador cuántico en pequeños ordenadores capaces de trabajar en equipo. Entonces, la factorización de números se llevaría a cabo en un tiempo más que razonable.

Si el ordenador cuántico llegar a ser una realidad algún día, los sistemas criptográficos actuales perderían dramáticamente su fuerza, y las grandes compañías quieren ser las primeras en enterarse, para lo cual no hay nada mejor que financiar ellos mismos la investigación.

¿Qué sistema criptográfico habría que utilizar entonces para hacer seguras nuestras comunicaciones? Probablemente ninguno. Si el espía "pincha" el cable de comunicaciones para hacer una observación, no sólo se pierde la información, sino que además, queda detectada inmediatamente su presencia. (La pérdida de esta información es algo que la criptografía cuántica podría resolver.) Este tipo de comunicaciones se está investigando actualmente por medio del cable de fibra óptica. El grupo de N. Gisin, de la Universidad de Ginebra, ha conseguido transmitir un dato cuántico (mediante fotones) a una distancia de 23 kilómetros, a lo largo de un cable submarino bajo las aguas de un lago. El que la transmisión se tenga que llevar a cabo a través de un medio material con la fibra óptica puede suponer algún tipo de limitación, especialmente para fines militares.

Los materiales

Es difícil predecir cuáles serán los componentes básicos de algo que todavía no existe. Aun así, hay ya varios candidatos, la mayoría de los cuales pertenecen al mundo microscópico. "Por el momento existen varias propuestas para realizar computación cuántica -asegura Ignacio Cirac-, aunque sólo una de ellas ha sido demostrada experimentalmente: es la de un conjunto de iones atrapados en una trampa electromagnética".

"Cada uno de los iones almacena 1 bit cuántico ("qubit"). Las operaciones aritméticas se producen iluminando selectivamente los iones con luz láser. Los elementos básicos de esta propuesta han sido demostrados experimentalmente por un grupo del Nist (Boulder, Estados Unidos). Otra propuesta se basa en la utilización de átomos, láseres y cavidades resonantes. Esta propuesta no se ha realizado experimentalmente, y parece "órdenes de magnitud" más complicada que la anterior. Existe otra propuesta que se basa en la utilización de "quantum dots" y luz láser, sin embargo, la tecnología actual no permite, al menos por el momento, poder realizar operación básica alguna (puerta lógica) entre dos "qubits".

Existe una tercera propuesta en la que se utilizarían propiedades magnéticas de los espines nucleares de los átomos de una molécula. Por el momento no se ha realizado experimento alguno al respecto, y no está claro que se pueda llevar a cabo una operación (al menos, con la tecnología actual). Por otra parte, existen propuestas para realizar una puerta lógica con fotones. Aunque ha habido algunos experimentos prometedores en esta dirección, esta propuesta no permite realizar más que una sola puerta, y, por lo tanto, es inútil para cualquier tipo de aplicación.

Los matemáticos y los físicos teóricos determinan, sobre el papel, lo que es y lo que no es posible hacer en la práctica. En el terreno puramente experimental, en la física de laboratorios, seguramente la última palabra la tenga la física del estado sólido. En los últimos años se han producido algunos descubrimientos considerados como muy importantes en una zona de tamaños intermedia, la de las "partículas mesoscópicas".

Un mundo fronterizo en el que se puede manipular la materia para escuchar los ecos misteriosos del microcosmos. En este orden de cosas, los físicos y teóricos experimentales opinan que el Mn-12-acetato puede llegar a convertirse en uno de los mejores candidatos para el computador cuántico.

La física cuántica ha "soñado" con precisión matemática cómo debe ser el mundo del microcosmos en el que estamos inmersos. Todos los experimentos encaminados a manipular, a hacer tangible ese mundo (y el computador cuántico puede ser uno de ellos) suponen convertir en realidad ese sueño.

Enrique Gracián <lsalas@lander.es>