¿Existirá algún día una computadora cuántica?

Yuri Rubo y Julia Tagüeña

La creación de una computadora cuántica promete revolucionar la ciencia y la tecnología. Sin embargo, hay muchos obstáculos que vencer para realizar este sueño.

Las computadoras se han vuelto parte de nuestra vida cotidiana. Están presentes no sólo en las universidades, oficinas y escuelas, sino en las casas de muchas personas. Las computadoras modernas almacenan nuestros datos, nos comunican con los amigos, sacan fotos y sirven para escuchar música. Sin embargo, no hay que olvidar su propósito original: hacer cálculos. Ha habido recientemente un enorme avance en la computación numérica. Cada año aparecen procesadores más rápidos y debemos tirar a la basura las computadoras que orgullosamente compramos hace poco tiempo. ¿Qué nos depara el futuro?

Ilustraciones: Aline Guevara

El aumento en la velocidad y la potencia de las computadoras en los últimos años y los efectos de esta tecnología son tan espectaculares, que uno podría pensar que no tienen límites. Y ni siquiera hace falta tomar en cuenta los cambios que las computadoras han producido en el comercio y la economía. Basta considerar el efecto de las computadoras en la ciencia para darse cuenta de que han cambiado nuestra manera de estudiar la naturaleza. Hoy en día las computadoras nos permiten simular, por ejemplo, colisiones de galaxias y la formación de las primeras estrellas. Así podemos estudiar y entender estos sucesos sin necesidad de que ocurran ante nuestros ojos. Podemos decir que los científicos cuentan con una nueva herramienta, además de las tradicionales (la teoría y la experimentación): la ciencia computacional.

El lenguaje natural de las computadoras

Básicamente, no hay diferencia entre las primeras computadoras y las modernas. Todas usan el sistema de numeración binario para codificar y manipular información. En la escuela aprendemos a contar con el sistema decimal. En este sistema, los números se construyen con 10 símbolos fundamentales (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) que, ubicados en distintas posiciones en el número, cuantifican las unidades, decenas, centenas… que contenga la cantidad en cuestión. Seguramente es el más común porque tenemos diez dedos. El sistema binario, en cambio, tiene sólo dos símbolos, el 0 y el 1, y es el más sencillo posible. En el sistema binario las posiciones no indican unidades, decenas, centenas, etecétera (que son las potencias de 10: 10^0, 10^1, 10^2…), sino potencias de 2: 2^0, 2^1, 2^2, 2^3…. Por ejemplo, en notación binaria los números 0, 1, 2, 3, 4 se escriben así: 0,1,10,11,100. Para hacer operaciones aritméticas en binario basta recordar que en esa notación 1 más 1 es igual a 10 y que 1 multiplicado por 1 es 1. En el sistema decimal, en cambio, tenemos que memorizar muchas sumas y multiplicaciones.

El elemento fundamental de todas las computadoras es una celda de memoria llamada *bit* (contracción de *binary digit*, o "dígito binario" en inglés), que puede exis-

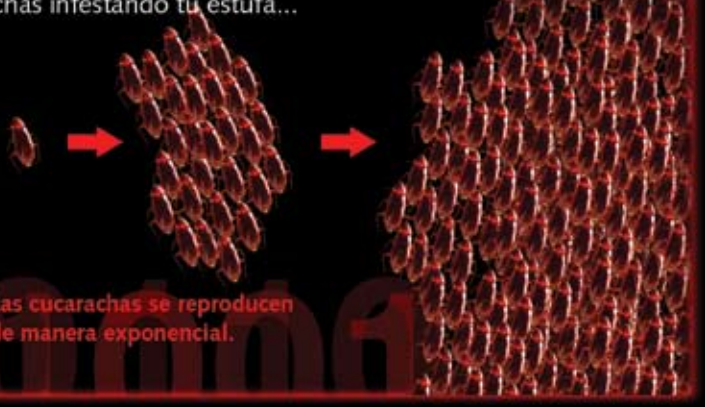
Aumento lineal

Cae una lluvia torrencial y en casa tienes goteras. Usas una cubeta para que el agua caiga en ella. Las gotas son idénticas, y oyes que caen a ritmo constante: tac, tac, tac, tac...

La cubeta se llena de manera lineal. En el aumento lineal la cantidad original de algo se incrementa en cantidades constantes, por unidad de tiempo.

Aumento exponencial

Sabemos que las cucarachas pueden invadir una cocina en poco tiempo. Si una cucaracha tiene 30 hijas, y a su vez cada una de ellas tiene 30 más, serán 900 cucarachas nuevas; si cada una de éstas tiene otras 30, el crecimiento será de 27 mil hijas. Si éstas continúan como sus madres, tendrán 810 mil descendientes... El crecimiento es de 30^1 cucarachas, 30^2 cucarachas, 30^3 cucarachas, 30^4 cucarachas, ¡etc! En poco tiempo, tendrás miles y miles de cucarachas infestando tu estufa...



Las cucarachas se reproducen de manera exponencial.

tir en dos estados, normalmente denotados por 0 y 1. Técnicamente estos bits se relacionan con unos dispositivos electrónicos (transistores) que representan los estados 0 y 1 interrumpiendo o dejando pasar una corriente eléctrica. La notación binaria es el lenguaje natural de las computadoras. Pero tiene un problema: que los números, salvo los más pequeños, son muy largos (por ejemplo, el número 40 en binario se escribe 101000). Para manipular la información con más facilidad se define el *byte*, un grupo de ocho bits.

El proceso de computación en general consiste en aplicar una secuencia de operaciones a ciertos bits. La regla que dice qué bits intervienen y en qué orden se llama *algoritmo*. Cada cálculo particular tiene un algoritmo, definido por el programador usando un lenguaje computacional. Las computadoras que funcionan aplicando algoritmos a información codificada en bits se llaman *computadoras clásicas*. Las computadoras clásicas (todas las que existen hoy, por rápidas o complejas que sean) son equivalentes a una *máquina de Turing*, modelo teórico de computadora descrito por Alan Turing en 1936 y perfeccionado por John von Neumann en 1940.

Límites de las computadoras clásicas

La máquina de Turing, y por lo tanto todas las computadoras de hoy, funcionan de acuerdo con las leyes de la llamada *física clásica*. Ésta prescribe que los bits tengan uno de dos valores bien definidos, es decir, que los transistores operen como puertas que se abren o se cierran, dejando pasar o interrumpiendo la corriente, sin ambigüedades. Pero la mecánica cuántica, teoría que describe el comportamiento de la materia en la escala de los átomos y las partículas subatómicas como el electrón, ha demostrado que nuestro mundo es más complicado.

Richard Feynman, uno de los físicos teóricos más brillantes del siglo pasado, reflexionó en 1982 acerca de las limitaciones de las computadoras clásicas. Le interesaba, en particular, el problema de hacer simulaciones del mundo real, que es cuántico a fin de cuentas, por medio de computadoras clásicas. ¿Se puede?

Simular un fenómeno por medio de una computadora exige que le proporcionemos a ésta las ecuaciones matemáticas que describen el fenómeno. La descripción matemática de los fenómenos cuánticos es la ecuación de Schrödinger. Se trata de una ecuación diferencial que una computadora clásica puede manipular. En otras palabras, nada impide resolver ecuaciones de movimiento cuántico con una computadora clásica. Pero la dificultad, como indicó Feynman, es que sólo podríamos resolver problemas muy simples y de poco interés, en los que intervienen sólo unas cuantas partículas (en un sistema cuántico de interés hay miles de millones de partículas). Si el número de partículas aumenta, la capacidad de la máquina debe aumentar exponencialmente. Para simular procesos cuánticos no triviales la computadora clásica tendría que ser gigantesca, porque su capacidad aumenta en forma lineal.

Además de plantear esta crítica de la física computacional clásica, Richard Feynman propuso

la utilización de sistemas cuánticos sencillos, llamados *qubits* (de *quantum bits*), como elementos estructurales básicos de una nueva computadora. Así nace el sueño de una computadora cuántica.

Bits cuánticos

La descripción cuántica tiene varias peculiaridades. Por ejemplo, cuando se lanza al aire una moneda la mecánica clásica nos permitiría saber de qué lado caerá si tuviéramos todos los datos acerca de la posición y la velocidad de la moneda al salir de nuestra mano. Si no tenemos los datos, decimos que hay una probabilidad de 50% de que caiga de un lado o del otro. En cambio, la probabilidad en mecánica cuántica es otra cosa. En los experimentos cuánticos no podemos predecir el resultado, sólo la probabilidad de que ocurra cierto resultado.

Pero la peculiaridad cuántica más importante para nuestros propósitos es el llamado *principio de superposición*. Si en el mundo clásico un objeto puede estar en uno de varios estados distintos (por ejemplo, en distintas posiciones, o con distintos valores de la energía), en mecánica cuántica puede estar, además, en combinaciones de todos los estados posibles. Esta superposición de estados perdura mientras el objeto permanezca aislado. En cuanto interactúa con su entorno (por ejemplo, cuando alguien trata de determinar con una medición en qué estado se encuentra), la superposición se destruye y el objeto cae en uno de sus estados. Por ejemplo, un electrón confinado en cierto volumen puede ocupar al mismo tiempo muchas posiciones. Pero cuando uno trata de localizarlo con una medición, el electrón se manifiesta en una sola posición. La destrucción de los estados de superposición al interactuar un sistema cuántico con su entorno se llama *decoherencia*.

Las computadoras cuánticas aprovechan el principio de superposición para sacarles más partido a los bits. Un bit cuántico, o *qubit*, tiene más posibilidades de almacenar información porque, además de los dos estados clásicos 1 y 0, puede encontrarse en una superposición de éstos. Dicho de otro modo, puede estar parcialmente en uno y otro al mismo tiempo. La gama de posibilidades varía continuamente del 0 al 1, con superposiciones que contienen más o menos de los dos estados clásicos. El qubit lleva una vida mucho más rica que el bit clásico. Esto finalmente define la importancia de los sistemas cuánticos para la informática y la computación. Es cómodo imaginar al qubit como un vector. La longitud de este vector es fija, pero puede apuntar en cualquier dirección, a diferencia del bit clásico, que sólo puede apuntar, digamos, hacia arriba y hacia abajo.

Los números primos y la criptografía

Los números primos son los que sólo se pueden dividir entre 1 y entre sí mismos. No hay algoritmos sencillos para generar números primos, comprobar si un número dado es primo ni descomponer un número en un producto de números primos (o sea, factorizarlo). Las computadoras clásicas usan el método de ensayo y error. La dificultad del cálculo aumenta exponencialmente con el valor de los números por generar o examinar. Por eso es fácil imaginar el entusiasmo que se dio en la comunidad científica cuando, en 1986, Peter W. Shor demostró que una computadora cuántica podría descomponer un número en factores primos en forma eficiente.

La factorización de números, aparte de ser un problema importante para la ciencia computacional, es también la clave de la criptografía moderna. Por ejemplo, el método PGP (*Pretty Good Privacy*, "Muy Buena Privacidad") depende de poder generar dos números primos grandes. Cada usuario del mensaje en clave genera su propio par de números. Un número (llamado la llave derecha o la llave pública) se distribuye en una forma abierta a todos. El segundo (la llave izquierda o la llave privada) lo guarda en secreto cada usuario. Si, digamos, Alicia quiere mandar un mensaje a Beto, ella "cierra" su mensaje con la llave pública de Beto. El mensaje queda revuelto o encriptado. Una vez cerrado con la llave derecha el mensaje sólo puede ser abierto (ordenado y descifrado) con la llave izquierda, y sólo Beto la tiene en secreto. Sólo él puede abrir el mensaje y leerlo, si tiene instalado desde luego el paquete de computación adecuado llamado PGP que se ofrece gratuitamente en la red. Si alguien más quiere saber lo que está escrito, va a tener que generar números primos grandes y comprobar cuál de ellos sirve.

Con los métodos de factorización de las computadoras clásicas el proceso puede durar un lapso equivalente a la antigüedad del Universo (que se mide en miles de millones de años).

Por eso no es sorprendente que después del descubrimiento de Shor el desarrollo de la computación cuántica haya recibido apoyo económico fuerte de parte de las agencias militares.

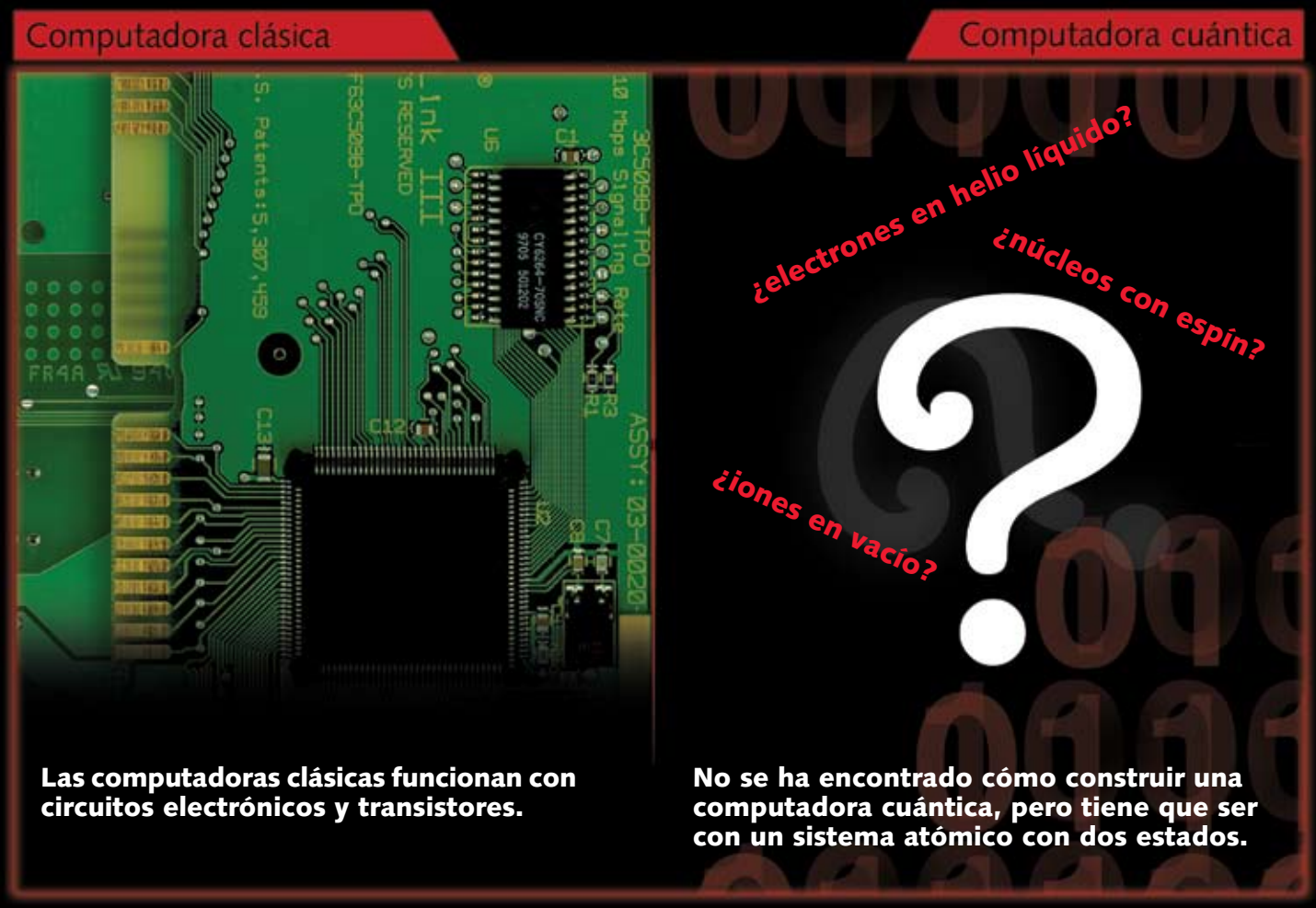
La computadora cuántica

En 1985 David Deutsch dio una base matemática sólida a la propuesta de Feynman. Deutsch explicó cómo podría funcionar una computadora cuántica universal y describió su funcionamiento como secuencias de operaciones elementales sobre qubits. La computadora cuántica de Deutsch es muy parecida a la máquina universal de Turing, pero con qubits en el lugar de bits clásicos. Sin embargo, la operación de una computadora cuántica es muy distinta de la operación de la máquina de Turing. Había que formular algoritmos computacionales cuánticos.

Los algoritmos cuánticos hacen uso de las peculiaridades de los qubits. Para iniciar un proceso de cómputo cuántico, podríamos, por ejemplo, poner para empezar todos los qubits que representan la información inicial en una superposición de 0 y 1. El estado inicial de esta computadora contendrá así todos los datos iniciales posibles. Ahora sólo falta hacer un cálculo adecuado (aplicar el algoritmo). Operando sobre los qubits en superposiciones de 1 y 0, el algoritmo cuántico resuelve, en cierta forma, todos los cálculos posibles al mismo tiempo. Uno puede imaginar (muy aproximadamente) una computadora cuántica como un conjunto muy grande de computadoras clásicas que funcionan en paralelo. Esta riqueza de la información se llama *paralelismo cuántico*, y disminuye drásticamente el número de pasos necesarios para resolver un problema en una computadora cuántica. Pensemos en la siguiente analogía. Supongamos que queremos comunicar información sobre una figura geométrica tridimensional muy complicada por medio de fotografías. La computadora clásica funcionaría entonces como una cámara que sólo maneja fotos en blanco y negro. En cambio una computadora cuántica podría transmitir todos los tonos de gris además del blanco y negro. Es claro que necesitaremos muchas menos fotos para representar el objeto debido a la riqueza de la descripción cuántica.

Obstáculos a vencer

El obstáculo principal para la construcción de una computadora cuántica es la fragilidad de los estados superpuestos



necesarios para que opere. La interacción de los qubits con el mundo exterior debe disminuirse al nivel más bajo posible para evitar la decoherencia de los estados superpuestos. Las influencias no controlables destruirían por completo la delicada superposición y el "enredamiento" de los qubits, propiedades que son la base de todos los algoritmos computacionales cuánticos. Aislar unos cuantos qubits de influencias incontrolables es relativamente fácil y ya se han hecho algunos experimentos. Pero cuanto más grande es un sistema cuántico (cuantos más elementos contiene, o en este caso, más qubits), más probable es que alguno de ellos interactúe con el exterior, y eso basta para producir la decoherencia de todo el sistema.

Claro que el problema de aparición de errores por influencias externas también existe en las computadoras clásicas. Por ejemplo, si guardamos un bit de información en el disco duro de una computadora clásica, con el tiempo este bit puede invertirse. Una manera de prevenir este error es guardar copias de cada bit. Después se compara periódicamente el valor de este bit con el de las copias, y si uno de ellos no coincide con los otros, se invierte.

Desgraciadamente este método no sirve en una computadora cuántica. Para determinar en qué estado se encuentra un qubit hay que interactuar con él, lo que destruye su estado y afecta el resultado del cálculo. Aunque ya existe un progreso importante en el desarrollo de métodos cuánticos no-destructivos de corrección de errores, todavía falta mucho para la construcción de una computadora cuántica suficientemente grande.

Por el momento no está claro todavía si podremos sortear estos obstáculos y construir una computadora cuántica con un gran número de qubits. ¿Vale la pena la lucha para construirla? Si dejamos aparte el problema de la criptografía, cuya importancia es temporal, el único motivo fundamental que queda para construir computadoras cuánticas es el estudio de los problemas del mundo cuántico. Sin embargo, el propio mundo cuántico nos impone un reto: ¿habrá una ley de la naturaleza que no permita que existan objetos cuánticos suficientemente grandes? Es probable que la respuesta sea afirmativa.

Independientemente del resultado de estas investigaciones, esperamos que estos estudios nos proporcionen una mejor interpretación de la naturaleza. Además, sólo se puede averiguar más intentando.

Yuri Rubo y Julia Tagüeña son investigadores del Centro de Investigación de Energía de la UNAM. La doctora Tagüeña es además titular de la Dirección General de Divulgación de la Ciencia, también de la UNAM.