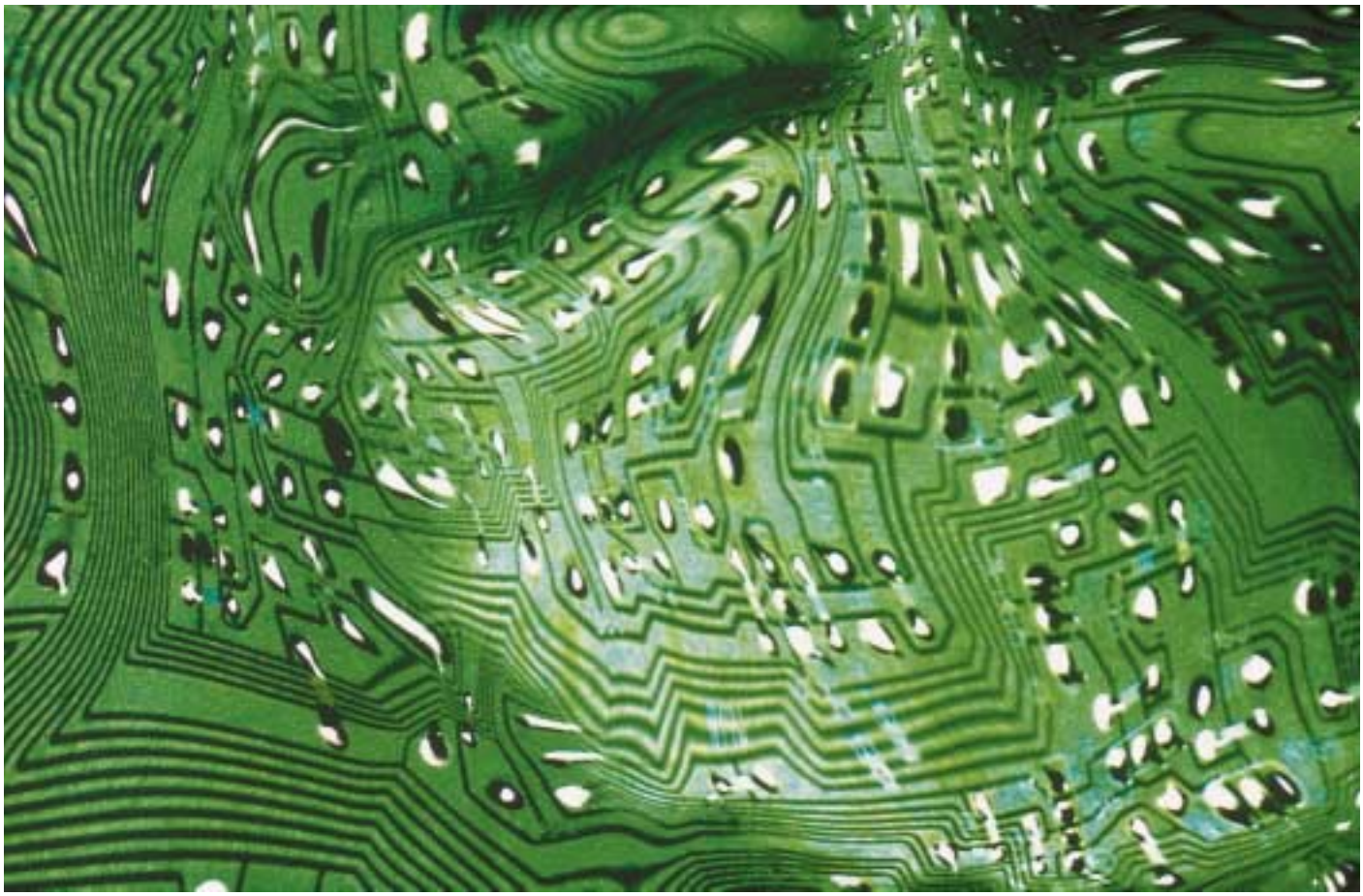
Desde los años cuarenta, los ordenadores no han dejado de evolucionar. Los enormes mastodontes del pasado abrieron las puertas a otros equipos más livianos. Tras la eclosión de los portátiles, ahora le llega el turno a los ordenadores cuyas piezas sean átomos o moléculas.

Los ordenadores cuánticos

Luis Miguel Lorenzo Saldaña,
Ingeniero Técnico de Telecomunicación



En el año 1958, Jack S. Kilby, Nobel de Física en el 2000, sacó a la luz el primer circuito integrado, base esencial de los computadores modernos.

La capacidad de procesamiento actual está basada en un aumento de la densidad de los transitores y de la miniaturización.

IBM dearrolló en el año 2000 un supercomputador con tecnología punta de ASCI White que ya logra 100 billones de cálculos por segundo (100 *teraflops*).

Sin embargo, esta carrera basada en el silicio, incluso el transistor de silicón, anunciado por Intel, que medirá unos 20 nanómetros, con el cual piensa alcanzar velocidades superiores a 20 Ghz para el año 2010, *está llegando el límite de las posibilidades de esta tecnología.*

Ante esta perspectiva de agotamiento de prestaciones, surge una posibilidad: *La computación cuántica.*

El ordenador cuántico más avanzado del mundo ha sido desarrollado por IBM en su Centro de Investigación de Almadén, California, (EE.UU.) Los investigadores a cargo del proyecto han realizado una prueba para mostrar cómo los ordenadores cuánticos son capaces de resolver problemas que resultan imposibles para los ordenadores convencionales.

Es bien conocido que los transistores con los cuales se construyen los ordenadores actuales son cada día más pequeños. La progresiva miniaturización de los chips se está acercando al límite de las leyes físicas clásicas.

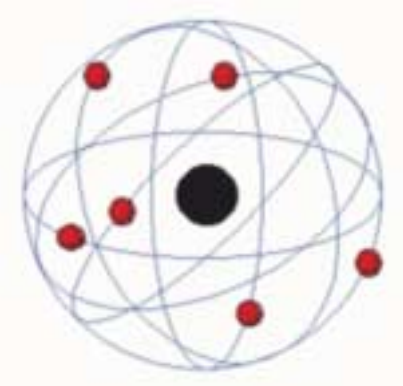
Los nanocircuitos actuales no podrán continuar disminuyendo porque entrarían en el campo de las partículas subatómicas, según informes de IBM, esto ocurrirá sobre el año 2015; en este momento, podría comenzar de manera clara la era de la computación cuántica ya que a estos niveles dominan las leyes de la mecánica cuántica y no las de la física clásica.

La computación actual busca nuevos caminos, y se presenta como *una alternativa diferente y revolucionaria*. La cuántica aplicada a los ordenadores no ha hecho más que comenzar y ya ha producido resultados sorprendentes.

PRINCIPIO DE INCERTIDUMBRE

Los sistemas atómicos incluyendo las partículas elementales no siguen las leyes de la Física clásica, esto se debe a un hecho fundamental, que consiste en la imposibilidad de medir todas sus propiedades simultáneamente de una manera exacta; es imposible, por ejemplo, conocer la posición y velocidad exacta de una partícula al mismo tiempo. Es lo que se conoce como *Principio de Incertidumbre de Heisemberg.*

Según la teoría clásica del electromagnetismo la radiación de un cuerpo caliente sería infinita, siendo imposible en un mundo real; la explicación la dio el físico Max Plank creando la *Mecánica Cuántica.*



BASE DE LOS ORDENADORES ACTUALES

Están basados en la Física Clásica, todas las variables se pueden medir directamente, de forma secuencial y sobre un conjunto *finito de estado internos.* En definitiva, están basados en la *Máquina de Turing* que brevemente describimos a continuación:

La máquina de Turing

Una máquina de Turing es un dispositivo que transforma un INPUT en un OUTPUT después de algunos pasos. Tanto el INPUT como el OUPUT constan de números en código binario.

Para llevar a cabo algún algoritmo, la máquina se inicializa en algún estado interno arbitrario. A continuación, se pone en marcha y la máquina lee el bit que se encuentra en ese momento en su interior y ejecuta alguna operación con ese bit (lo cambia o no, dependiendo de su estado interno). Después se mueve en un sentido, y vuelve a procesar el siguiente bit de la misma manera. Al final se para, dejando el resultado en uno de los lados.

La máquina de Turing, como modelo matemático, está formado por un cabezal lectura/escritura y una cinta infinita en lo que el cabezal lee el contenido, borra el contenido anterior y escribe un nuevo valor. Las operaciones que se pueden realizar en esta máquina se limitan a:

— avanzar el cabezal lector/escritor para la derecha;

— avanzar el cabezal lector/escritor para la izquierda.

La computación es determinada a partir de una tabla de estados de la forma:

(estado,valor) → (\nuevo estado, \nuevo valor, dirección)

No se puede simular un sistema cuántico con una máquina de Turing.

FENÓMEMOS CUÁNTICOS

Para entender «un poco» la base de funcionamiento de un ordenador cuántico de este tipo, debemos tener en cuenta la Mecánica Cuántica. Mencionaremos, para hacerlo más ameno, algunos fenómenos cuanticos.

El gato de Schrödinger

Sabemos que la física cuántica es muy rara y simplemente lo aceptamos.

Cuanto entramos en detalles, la cosa cambia. Imaginemos que alguien nos dice: «Un átomo puede girar a derecha y a la izquierda *a la vez*» nos quedamos descolocados.

«Los sistemas atómicos, incluyendo las partículas elementales, no siguen las leyes de la Física clásica»

Allá por el año 1935, Erwin Schrödinger, ideó el siguiente experimento mental que se ha hecho famoso:

Construir una caja cerrada, aislada completamente del exterior, es decir, que nada que ocurra en el interior sea detec-

table desde el exterior, incluso ruido, vibraciones, etc.

Introducimos dentro de la caja una muestra radiactiva que tenga un 50% de probabilidades de que se desintegre en un tiempo T.

Se instala un dispositivo en el interior de la caja de tal forma que si la muestra radiactiva se desintegra, el dispositivo romperá un frasco en el que hay gas cianuro suficiente para matar al gato. Una vez todo preparado metemos al gato en la caja y cerramos esta. Desde el exterior no sabemos nada del gato, ni movimientos, ni aullidos... nada.

Transcurrido el tiempo T, no sabremos desde fuera si el gato esta vivo o muerto.

La física cuántica nos da la siguiente respuesta: *No está ni vivo ni muerto.*

El gato no estará ni vivo ni muerto hasta que abramos la caja y observemos. Mientras tanto el estado real del gato será diferente a «realmente vivo» o «realmente muerto». Existe un estado de superposición cuántica. Al abrir la caja, la función de onda se colapsa y ante el observador aparece únicamente uno de los dos fenómenos.

¿Puede un gato estar vivo y muerto a la vez? En los años ochenta, Leggett y sus colaboradores propusieron que, bajo determinadas condiciones, *un objeto macroscópico* con varios grados de libertad microscópicos podía tener un comportamiento cuántico si se encontraba convenientemente aislado de su entorno.

Algunos para resolver la paradoja, les ha llevado a suponer «universos paralelos».

En los últimos años se han llevado a cabo experimentos que ponen de manifiesto la existencia de partículas subatómicas en estados de superposición aunque nunca gatos.

El squid

Friedman realizó el siguiente experimento cuántico: aplicó a un squid (dispositivo superconductor de interferencia cuántica) un flujo magnético. Observó una superposición cuántica al evidenciar dos corrientes simultáneas circulando en sentidos contrarios en el anillo del squid.

Supongamos un anillo superconductor, es decir, que a muy bajas temperaturas su resistencia es prácticamente cero. Intercalamos una delgada capa de material aislante, lo que se conoce como unión *Josephson.*

En este dispositivo es posible que circule corriente sin aplicar tensión, ¿es raro? Pues si, pero ocurre. Los electrones pasan de un extremo a otro del anillo por un fenómeno que en física cuántica se denomina «efecto túnel».

Pero es que además los electrones circulaban en ambos sentidos (estado de superposición cuántica). Los autores del experimento hablan de que unos mil millones de electrones están involucrados en el experimento, ya no se puede hablar de «partícula subatómica» sino de un objeto.

Teletransportación

La magia del teletransporte, es que una estructura va de un punto a otro, sin pasar por medio.

En el periódico *Tribune* de Ginebra, apareció la noticia de que un equipo de investigadores de la Universidad de esa

ciudad habían logrado reproducir un fotón a una distancia de dos kilómetros de distancia aun en sus más mínimos detalles. El teletransporte en cuanto a su concepción existe desde la década de los años 90. La importancia de este experimento reside en la distancia cubierta, según comenta la revista *Nature*.

El jefe de este grupo de investigadores ginebrinos comenta: «Si un mensaje codificado no existe mientras dura su transmisión, será imposible interceptarlo».

Para el experimento comentado se creó una línea de fibra óptica, una vez establecida la línea, se pueden retirar los cables y *la línea seguirá existiendo.* Otro de los misterios de la mecánica cuántica.

CARA Y CRUZ

La computación cuántica ofrece dos caras:

— Por un lado tiene una altísima capacidad de cálculo, *la cara*.

— Por otro maneja principios cuánticos, *la cruz*.

Un ordenador cuántico podría descrifrar una clave de 1.024 bits, en cuestión de minutos, mientras que usando el potencial de 8.000 ordenadores actuales a la vez podríamos tardar más de 800 millones de años.

Desaparecería la criptografía actual y surgiría la criptografía cuántica, mucho más segura.

En un ordenador actual la información se guarda en forma de bits cada uno de los cuales puede valer 0 o 1. En un ordenador cuántico la información se procesa y se guarda en qubits, del inglés *quantum bits* (bits cuánticos). Un qubit se encuentra en superposición de estados, puede ser un 1 o un cero. Haciendo comparación un bit es a un gato como un qubit es al gato de Schrödinger, pero claro está, antes de abrir la caja.

Como sabemos un 0 representa un voltaje entre 0 y 2 voltios, un 1 representa un voltaje entre 4 y 6. Los detalles de exactamente cómo funcionan todas estas cosas no son demasiado importantes; en los años 40 se usaban válvulas de vacío, luego vinieron los transistores, los circuitos integrados y los microchips, y sin embargo los ordenadores no cambiaron esencialmente.

En las memorias clásicas se guardan los 1 y los 0, como voltajes, operando con «puertas lógicas». En un ordenador cuántico se usarán «puertas cuánticas».

Para representar, guardar, copiar, etc, con los *qubits* se usarán tecnologías que sería hablar de futurible. Concretando ideas a este respecto, en unos casos se han utilizado iones atrapados en campos de vacío en campos eléctricos dentro de cámaras de vacío a temperaturas bajísimas; estos iones se pueden manipular con láseres. En otros casos, cada qubit se ha representado con el spin de un electrón atrapado en un pozo cuántico, de forma que si «giraba» en un sentido representaba un 1 y si giraba en el sentido contrario representaba un 0. En estos casos el valor del qubit se puede manipular

«La computación cuántica tiene tal capacidad de cálculo que la criptografía actual no serviría para nada»

con campos magnéticos. Se opera con los qubits en las puertas cuánticas, cuyo funcionamiento tiende a ser muy complicado de explicar.

Hay dos diferencias importantes entre un ordenador cuántico y uno clásico.

La primera está en que al operar con qubits se pueden hacer muchas operaciones a la vez. Por ejemplo, supongamos que en un ordenador cuántico tenemos dos registros de 8 qubits; el primero vale 7 y 8 y el segundo vale 1.000 y 2.000 (en rigor tendríamos que decir que cada registro está en una superposición de dos estados en vez de tener ambos valores) Bueno, pues podríamos sumar estos dos registros, de la misma forma en que los ordenadores han hecho sumas toda la vida, pero el resultado sería una superposición de cuatro estados con valores 1.007, 1.008, 2.007 y 2.008.

Con un único «circuito» y con una única operación podemos hacer simultáneamente cantidades enormes de sumas.

La segunda diferencia fundamental en un ordenador cuántico es que este realiza una operación nueva: *observar un registro, equivalente a abrir la caja del gato.*

En el caso de la operación anterior, si observásemos la suma, veríamos que su valor es alguno de los indicados, escogido al azar con las probabilidades imaginables; por ejemplo, la probabilidad de que al observar la suma viésemos 1.007 sería la probabilidad de que al observar el primer sumando viésemos 7 multiplicado por la probabilidad de que al observar el segundo sumando viésemos 1.000.

Señalaremos que esta tecnología incluye muchos campos de la ciencia, como las matemáticas, las comunicaciones, la criptografía, la microelectrónica, la nanotecnología, etc.

EL FUTURO

Curiosamente los ordenadores cuánticos serían capaces de demostrar teoremas matemáticos pero quizás las demostraciones serían tan *fabulosamente extensas* que llenarían un «universo de papel» por lo que tendríamos que creer sin más esa demostración. Manejarían inmensas bases de datos, a la «velocidad de la luz».

El número de investigadores inmersos en este nuevo y apasionante mundo es cada vez mayor.

El camino hacia la construcción del ordenador cuántico ya está produciendo grandes beneficios por el mejor conocimiento del funcionamiento de este tipo de sistemas moleculares.

El nacimiento del ordenador cuántico destruiría la criptografía actual, pero también el nacimiento de la criptografía cuántica, mucho más segura y prácticamente inviolable.

Agencias gubernamentales, agencias de seguridad, bancos, institutos de investigación, centros de control, etc., ya están interesados por esta técnica.

En este momento, se están desarrollando nuevas investigaciones para conseguir un bit cuántico por combinación de los ingredientes básicos existentes.

Koppens sostiene que el camino ya ha sido allanado para comenzar a ejecutar cálculos cuánticos elementales. Según su opinión, gracias a estos avances, descubrir las peculiares propiedades de la física cuántica podría resultar más atractivo, por ejemplo, revelando el enredo o entrelazado de los dos electrones. El entrelazado es también el tema central del grupo de investigación del FOM sobre Procesamiento de Información Cuántica del Estado Sólido de la Universidad de Delft, que cuenta con el apoyo de la Universidad de Leiden y del que forma parte el equipo de Vandersypen.

«Los ordenadores cuánticos manejarían inmensas bases de datos a la velocidad de la luz»

Entre la fantasia y la realidad... los ordenadores cuánticos... tienen un futuro... que según los expertos... dentro de 20, 30, o más años estarían operativos.

Quizá más tiempo para tenerlos en nuestras mesas, al igual que hoy día disponemos del familiar PC, *quizás menos tiempo*, si alguien descubre «algo» que sea el fundamento de la computación e informática cuántica y acelere su puesta en marcha, como ha ocurrido en muchos campos de la ciencia.