Nuevas aplicaciones de la Física Cuántica cien años después de su creación

Pedro J. Salas
Depto. Tecnologías Especiales Aplicadas a la Telecomunicación
E.T.S.I. Telecomunicación, U.P.M.

Desde antiguo el hombre se ha sentido atraído por la posibilidad de predecir el comportamiento de la naturaleza. Le han guiado las ansias de conocer y dominar sus entresijos. Aún estamos lejos de comprenderla completamente, pero ya disponemos de algunas teorías y modelos físicos que nos ayudan a hacernos una imagen de ella. La Mecánica Cuántica (MC) es, sin duda, la teoría que ha cosechado los mayores éxitos en cuanto a describir y predecir nuevos fenómenos. Con ella se describe tanto la materia (partículas elementales, átomos, moléculas, sólidos y agregados) así como los campos electromagnéticos que constituyen la luz. La base matemática de su formalismo está perfectamente establecida, sin embargo, algunas de sus implicaciones filosóficas y de interpretación son las que dan lugar a ciertos "misterios". En alguna ocasión se califica a la MC como una teoría que atenta contra la intuición humana, pero ¿por qué una teoría surgida para explicar comportamientos *microscópicos* debe ser intuitiva? Después de todo, nuestra intuición se ha desarrollado en un mundo *macroscópico*.

Ya desde sus inicios surgieron numerosas e importantes críticas a la interpretación de la MC, acaudilladas por los propios físicos que la crearon como Bohr, Schrödinger, de Broglie, Einstein y otros, utilizándose "experimentos pensados" que trataban de poner en aprietos la descripción cuántica de la naturaleza. Tales intentos quedaron durante unos cincuenta años como paradojas académicas sin posibilidad de comprobación. Los actuales desarrollos tecnológicos son los que han propiciado el estudio experimental. Los físicos han preguntado a la naturaleza y ésta ha respondido, aunque no siempre del modo esperado.

Dualismo onda-partícula. Situación histórica[1].

Para apreciar la ruptura que la MC iba a plantear respecto a las teorías clásicas, mencionaremos algunos de los hitos más importantes de su desarrollo. Clásicamente, la naturaleza está formada por dos tipos distintos y bien diferenciados de entidades: luz (radiación) y partículas (materia).

En los siglos XVII y XVIII existió una división entre los partidarios de que luz tuviera una naturaleza corpuscular defendida por Newton, y aquellos que creían en una naturaleza ondulatoria, como Christian Huyghens. Sin embargo, no se realizaron demasiados esfuerzos hasta que Thomas Young retomó la explicación seria de estos fenómenos. El 24 de noviembre 1803, Young expuso su trabajo ante la Real Sociedad de Londres, mostrando los diagramas de difracción obtenidos haciendo pasar luz a través de rendijas muy próximas. La explicación de los máximos y mínimos que aparecían se podía realizar fácilmente mediante un modelo ondulatorio.

Por otra parte, la materia parecía bien descrita mediante la mecánica de Newton, gozando de las típicas propiedades de partícula (posición, trayectorias, etc.). Ambos entes, ondas y partículas parecían clásicamente *bien diferenciados*.

En el año 1900, los físicos tenían una confianza casi infinita en el poder de la física clásica para describir la naturaleza. A pesar de todo, existían algunos problemas "triviales" por resolver. El 27 de abril de 1900 (viernes por la tarde), Lord Kelvin lee en la Royal Institution de Gran Bretaña en Londres, una conferencia titulada *"Las nubes del siglo XIX en la teoría dinámica del calor y la luz"* (publicada en julio de 1901 en Philosophical Magazine). En palabras de Lord Kelvin

William Thomson
(Lord Kelvin)

"La física es un conjunto perfectamente armonioso y en lo esencial acabado, en el que sólo veo dos pequeñas nubes oscuras: el resultado negativo de la experiencia de Michelson - Morley y la catástrofe ultravioleta de la ley de Rayleigh-Jeans"

Afortunadamente, las cosas iban a cambiar rápidamente y de forma inesperada. La solución del experimento de Michelson-Morley daría lugar a la Teoría Especial de la Relatividad, formulada por Albert Einstein en 1905. Su aparición modificó la idea que tenían los físicos acerca del espacio y del tiempo. Con la intención de solventar los problemas surgidos en la emisión de radiación por un cuerpo negro, Max Planck indujo en 1900, la discretización de los niveles vibracionales de las partículas cargadas, cuya oscilación producía la radiación de cuerpo negro. Presentó su ecuación en la reunión de la Sociedad de Física Alemana que se celebró en Berlín el 19 de octubre de 1900, impartiendo una conferencia cuyo título fue "*Sobre una mejora de la ecuación de Wien para el espectro*". Según Planck, la radiación (luz) tenía una naturaleza ondulatoria, pero era absorbida y emitida en forma discontinua cuando los citados osciladores realizaban "saltos" energéticos entre niveles discretos permitidos, cuya energía venía por $E_n = nh\upsilon$ con $n = 0,1,2\ldots$, υ era la frecuencia del oscilador y h era la (llamada desde entonces) constante de Planck. Hacia 1905, Einstein se enfrentó con la búsqueda de una explicación para el efecto fotoeléctrico (emisión de electrones cuando un metal era iluminado con luz de frecuencia adecuada). Para ello extendió la discretización del proceso de absorción-emisión de la luz, a su propia naturaleza. La luz de frecuencia υ estaba formada por pequeños "paquetes" o cuantos, cuya energía era $E = h\upsilon$. Tal consideración fue sumamente fructífera, permitiendo explicar una gran variedad de fenómenos relacionados con los efectos mecánicos de la luz como el efecto Compton (dispersión de la luz por electrones). A partir de 1926, esos paquetes o cuantos de luz, G. N. Lewis los llamaría *fotones*. Después de todo, parece que la naturaleza ondulatoria de la luz, tan firmemente establecida desde los experimentos de interferencia de Thomas Young hacia 1803, no estaba tan clara. Dependiendo del experimento, la luz se muestra como si fuera una onda (electromagnética) y otras veces como un partícula (fotón). Tal comportamiento (no clásico) se le denominó *dualidad* entre onda y partícula.

A principios de los años veinte, el príncipe Louis de Broglie se preguntó acerca de la posibilidad de la existencia de una simetría entre la materia y la luz. Si la luz muestra un comportamiento dual, ¿por qué no lo presenta también la materia? En su tesis doctoral (titulada *Recherches sur la théorie des quanta*, que defendió en la Sorbona el 25 de noviembre de 1924) desarrolló tal idea, asociando a una partícula libre de masa m y velocidad v, una cierta onda "de materia", cuya longitud de onda vendría dada por $\lambda = h/mv$. Relación que liga las características de onda (λ) con las de partícula (m). Era

evidente que, si tal movimiento ondulatorio era real, debía de poder evidenciarse, por ejemplo, mediante la obtención de diagramas de interferencia para haces de partículas.

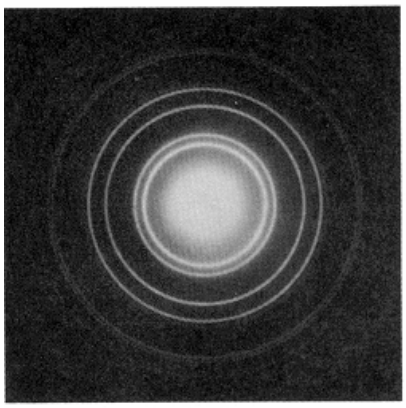


Diagrama de difracción obtenido con un haz de electrones al atravesar una lámina delgada de Al.

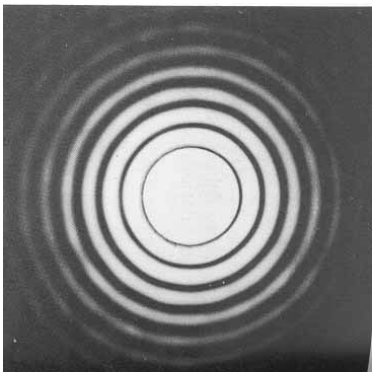
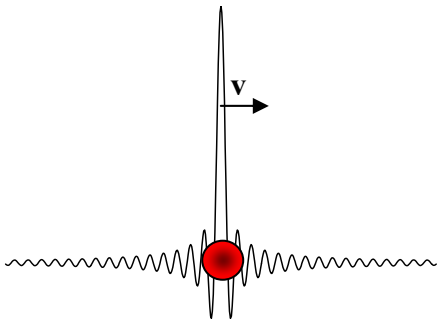


Diagrama de difracción de la luz obtenido al atravesar un orificio

Los electrones son partículas por excelencia, no en vano, en 1897 J.J. Thomson había determinado su relación carga/masa = 1.7 10^{11} C/Kg ¿Se podrían comportar los electrones como ondas? En 1927, G.P. Thomson (hijo de J.J. Thomson) y A. Reid dirigieron un haz de electrones a través de láminas de aluminio de unos 1000 Å de espesor. Los diagramas obtenidos se pueden comparar con los producidos cuando la luz atraviesa un orifico. La similitud entre ambos es sorprendente. Experimentalmente se concluye que los electrones (típicamente partículas) presentan cierto tipo de comportamiento solo explicable mediante el concepto clásico de onda.

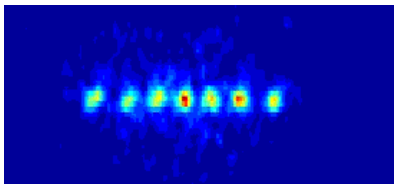
La conclusión parece ahora más clara. Tanto luz como materia tienen una naturaleza *dual* y la manifestación particular depende del tipo de experimento realizado. Hacia finales de 1925 y principios de 1926, Erwin Schrödinger ya se había planteado encontrar la ecuación general que gobierna la evolución de las ondas de materia, obteniendo la llamada ecuación de ondas de Schrödinger. Su solución es una función compleja, llamada *función de onda* Ψ, que depende de las coordenadas espaciales y del tiempo. Esta función es la generalización del aspecto ondulatorio de cualquier sistema, incluso si está sometido a un cierto potencial. La conexión entre el comportamiento de partícula y el de su onda de materia asociada, se establece a través de la densidad de probabilidad de presencia de una partícula en un volumen dV, alrededor del punto (x,y,z) y en el instante t, dada por $|\Psi(x,y,z,t)|^2$. Puesto que la ecuación de Schrödinger es lineal, admite soluciones del tipo pulso, lo que permite describir pictóricamente a un ente cuántico como el electrón, por medio de un pulso extenso en el espacio (presentando las características de onda) y cuyo máximo se desplaza con la velocidad de la partícula v.



Representación de la naturaleza dual de una partícula de masa m y velocidad **v**

Bien, quizás los electrones sean demasiado pequeños, y por ello presenten ese comportamiento dual no clásico ¿Mostrarán los átomos también un comportamiento

dual? Los átomos son varias miles de veces más pesados que los electrones y son entes que se comportan como partículas. Su observación individual no se ha conseguido hasta tiempos recientes. Un ejemplo de ello son las trampas de iones[2]. Los iones se enfrían con haces láser y se atrapan mediante un sistema de geometría apropiada de campos magnéticos y eléctricos. En su interior, los iones se mueven bajo la repulsión mutua y las interacciones creadas por los campos externos, realizando oscilaciones del tipo armónico. Cada ión se puede visualizar a través de la luz de fluorescencia reemitida después de su excitación previa.



Fluorescencia de átomos de Ca^{2+} en una trampa lineal de iones

Diagrama de interferencia obtenido con átomos de Ne

Muchas son ya las manifestaciones ondulatorias de los átomos. En 1995, Takuma[3] obtuvo diagramas de interferencia con átomos de Ne. En el año 1999, Anton Zeilinger obtuvo diagramas de interferencia con moléculas del tipo fulereno (C_{60})[4], que empiezan a tener ciertas características que las acercan al mundo macroscópico.

La conclusión parece clara, tanto materia como luz tienen una naturaleza dual. La descripción de su comportamiento requiere los modelos ondulatorio y corpuscular. Este es el mayor misterio de la física cuántica, que se manifiesta en el experimento de la doble rendija. Si enviamos un haz de luz o de partículas sobre un sistema de dos rendijas, su detección sobre una pantalla se realiza como si incidieran pequeñas partículas, pero su localización concreta se describe mediante un modelo ondulatorio. Tal como manifestaba Richard Feynman[5] (Premio Novel de física en 1965):

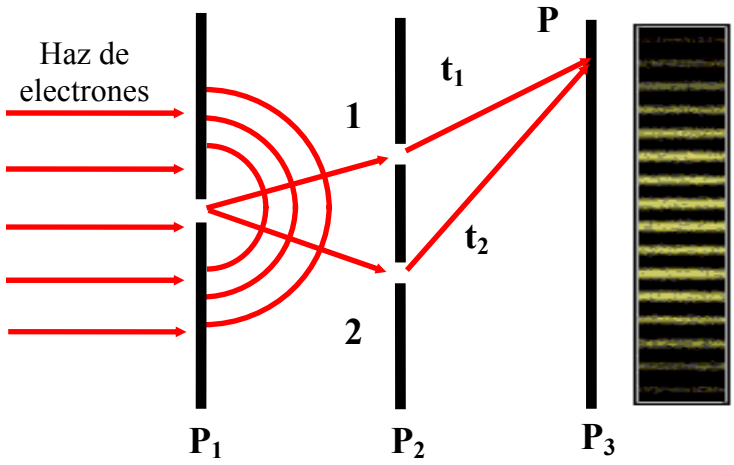
> *"el experimento de la doble rendija es un fenómeno que es imposible, absolutamente imposible de explicarse clásicamente, y que está en el corazón de la mecánica cuántica. En realidad, contiene el único misterio"*

Experimentos de doble rendija con electrones

El dualismo onda-partícula de los entes cuánticos, conduce a ciertas paradojas si pretendemos seguir manteniendo los conceptos clásicos. Los electrones muestran un comportamiento claramente de partícula, por ejemplo cuando su paso se detecta a través del rastro que dejan en una cámara de niebla. Sin embargo, en un experimento de difracción, cuando los electrones atraviesan un sistema de dos rendijas, su trayectoria no está tan clara. Al detectarse un electrón en el punto P de la pantalla P_3, no podemos saber por qué rendija ha pasado. Existen dos trayectorias compatibles, la t_1 y la t_2. Según Feynman[5], es este desconocimiento de la trayectoria seguida lo que permite justificar la aparición del diagrama de interferencia. Si tapamos una de las rendijas (lo que equivale a conocer la rendija por la que pasan los electrones), el diagrama de interferencia desaparece.

Los electrones "detectan" de alguna forma si ambas rendijas están abiertas (produciendo interferencia) o bien si sólo una de ellas lo está (no aparece interferencia).

Ahora podemos preguntarnos ¿cómo puede producirse el diagrama de interferencia con los electrones, si son partículas que atraviesan sólo una rendija? Quizás la respuesta podría estar relacionada con la existencia de interacciones entre los distintos electrones del haz, es decir surgiendo de un fenómeno *colectivo*. Un sencillo experimento nos permite comprobar la anterior consideración. Si realmente la interferencia de un haz de

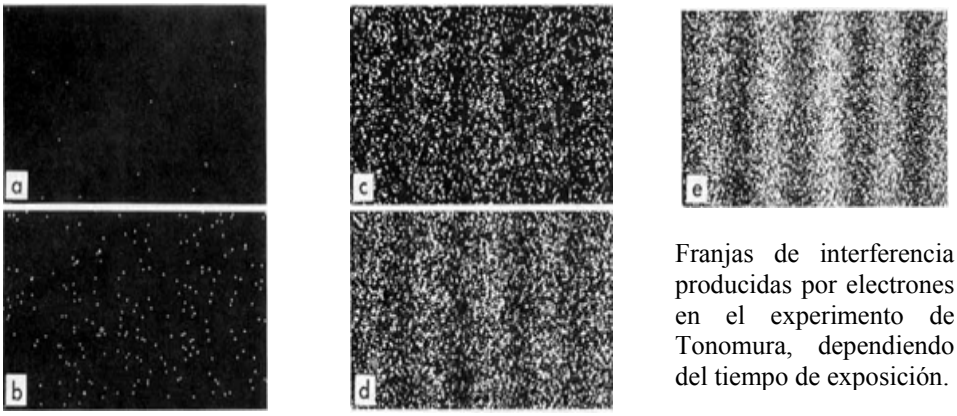


Difracción por dos rendijas 1 y 2 de un haz de electrones. El diagrama de interferencia se origina en la indistinguibilidad de las dos posibles trayectorias t_1 y t_2.

electrones se debe a sus interacciones mutuas, ¿qué pasaría si en lugar de enviar un haz formado por muchos electrones, los enviamos *uno a uno*? Es decir, sólo una partícula se encuentra, por término medio, dentro del aparato de doble rendija. Cada electrón ya no tiene con quien interaccionar, ¿aparecerá interferencia? La respuesta se adivina desconcertante.

En 1989, A. Tonomura[6] (trabajando en Hitachi Advanced Research Laboratory de Japón) realizó un experimento de doble rendija con electrones que incidían de forma consecutiva sobre una pantalla. En este experimento se dirigía un haz de electrones de $\lambda = 0.054$ Å con un flujo de 1000 electrones/s a una velocidad de 10^8 m/s, sobre un biprisma que consiste en dos placas paralelas con un filamento en el centro. El filamento se mantiene a un potencial positivo respecto a las placas. Los electrones son desviados al pasar entre el filamento y las placas, añadiéndole una fase a la onda de materia, dependiendo de por qué lado pasan. Los dos haces se focalizan y se les permite interferir. Sobre una pantalla (a 1.5 m de la fuente), se forma un diagrama de interferencia (en unos 20 minutos) con bandas separadas 7000 Å, que después de aumentarse convenientemente aparecen separadas unos 1.4 mm. La novedad del experimento radica en que el promedio de espacio entre dos electrones consecutivos, lanzados sobre el dispositivo de difracción, es de unos 100 Km. El paquete de ondas que describe a cada electrón tiene un tamaño del orden de 1 μm, lo que nos indica que hay una pequeña probabilidad de que dos electrones estén presentes simultáneamente entre el emisor y la pantalla, y mucho menor todavía, de que dos paquetes de onda solapen y los electrones puedan interferir entre sí. Los resultados muestran la aparición de puntos brillantes donde inciden los electrones sobre una pantalla del tipo de TV. Al principio, los puntos parecen situados aleatoriamente, pero con el tiempo van apareciendo regiones claras y regiones oscuras análogas a las de un diagrama de interferencia de la luz. La situación es parecida a los experimentos con radiación. Si colocamos detectores en distintos lugares de la pantalla, sólo se detecta un electrón al mismo tiempo, y los electrones llegan enteros y sin dividirse ¿Qué interfiere en este experimento?

La interpretación ortodoxa de la mecánica cuántica considera que cada electrón *interfiere consigo mismo*, dando lugar a una *autointerferencia* de electrones. La materia presenta un dualismo intrínseco que se manifiesta en el experimento de doble rendija con partículas como los electrones. Se puede interpretar que si la función de onda de un electrón atravesando la rendija 1 es ϕ_1 y es ϕ_2 si atraviesa la rendija 2, al enviar un solo electrón, su función de onda es $(\phi_1+\phi_2)$, lo que significa que *atraviesa ambas rendijas a la vez*. Si se tapa una de las rendijas, por ejemplo la 2, desaparece el término ϕ_2 (colapso de la función de onda) y con él la interferencia. Por lo tanto, trayectoria y diagrama de interferencia son aspectos *mutuamente excluyentes*.



Franjas de interferencia producidas por electrones en el experimento de Tonomura, dependiendo del tiempo de exposición.

Este comportamiento no es exclusivo de los electrones, sino que se manifiesta en partículas materiales de mayor tamaño, así como en la luz. En el caso de la radiación la autointerferencia no parece algo tan extraño, debido a su carácter disperso en el espacio. Sin embargo, si se emplea la descripción de la luz mediante fotones, la autointerferencia sigue teniendo un halo misterioso.

Medidas sin interacción

Según la mitología griega, el héroe Perseo tuvo que luchar contra la temida Medusa; monstruo con serpientes por cabellos y tan horrible que una sola mirada convertía al observador en piedra. Si Perseo la hubiera mirado, aunque sólo fuera ligeramente, se habría convertido en piedra. Por otra parte, si no hubiera mirado, le sería casi imposible acertar con su espada a la Medusa. Según el mito, Perseo escapó de tan espantoso destino usando hábilmente su escudo como espejo para reflejar la imagen de la propia Medusa, convirtiéndose ésta en piedra. Si Perseo hubiera tenido algunos conocimientos de Mecánica Cuántica, podría haber visto a la Medusa sin la presencia de luz, y destruirla de certero golpe.

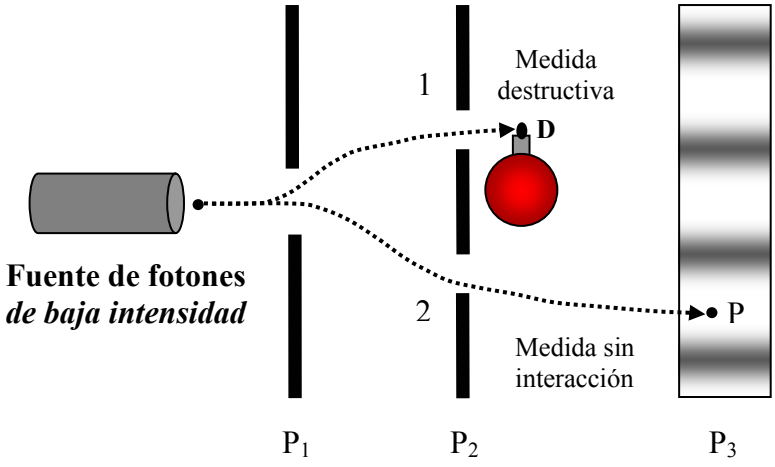
Parece que cualquier observación lleva asociada algún tipo de interacción entre el observador y el objeto observado. Dennis Gabor (Premio Nobel de Física en 1971 por inventar la holografía) manifestó en 1961 que *"no puede realizarse observación alguna a menos que un fotón dé en el objeto observado"*, aserción que parece lógica e ineludible.

Una consecuencia del dualismo de las partículas son las medidas sin interacción. A continuación expondremos dos métodos. En primer lugar usando el dualismo intrínseco de partículas *individuales* a través de un dispositivo de doble rendija, y a continuación por medio del comportamiento dual de *dos* partículas correlacionadas en estados especiales, llamados enredados.

a) Experimento de doble rendija.

La posibilidad de usar experimentos de resultado negativo para realizar medidas sin interacción, es conocida en física clásica. Por ejemplo, supongamos que disponemos de dos cajas cerradas en cuyo interior hay sendas bombas. Una de ellas tiene un dispositivo detonador constituido por una célula fotoeléctrica que es sensible, incluso a la incidencia de un solo fotón; mientras que la otra, carece de detonador. El problema consiste en realizar un experimento al final del cual tengamos una caja que contenga la bomba con detonador. El proceso es abrir una de las cajas elegida al azar. Si tenemos suerte y no explota, es que la bomba con detonador está en la otra caja, con la que no hemos interaccionado. Evidentemente, sólo la mitad de las veces (probabilidad de acertar = 0.5) tendremos éxito con el experimento, ya que en la otra mitad habremos elegido la caja que contiene la bomba con detonador y estallará. Ahora podemos modificar ligeramente el problema, y considerar que disponemos de una sola caja en cuyo interior hay una bomba, de la que desconocemos si tiene o no detonador fotoeléctrico. No podemos abrir sin más la caja, pues la bomba estallaría. En realidad, no existe ningún experimento clásico que nos permita saber, ni siquiera con cierta probabilidad, si la bomba contenida en la caja tiene o no detonador.

La solución al problema de detectar la presencia de un objeto, sin que éste sea perturbado ni por un solo fotón, fue propuesta en 1993, por Avshalom C. Elitzur y Lev Vaidman[7] de la Universidad de Tell-Aviv y se la denominó *visión cuántica en la oscuridad*. Supongamos que disponemos de un dispositivo de doble rendija sobre el que se envían fotones uno a uno, tal como en el experimento de Tonomura se hacía con



Medida sin interacción de la presencia de un objeto (detonador D en una bomba) obstruyendo la rendija 1. La detección de un fotón en P implica que su trayectoria es la indicada por una línea discontinua, representado una medida sin interacción. Suponemos que todo el dispositivo de doble rendija y la bomba están en absoluta oscuridad.

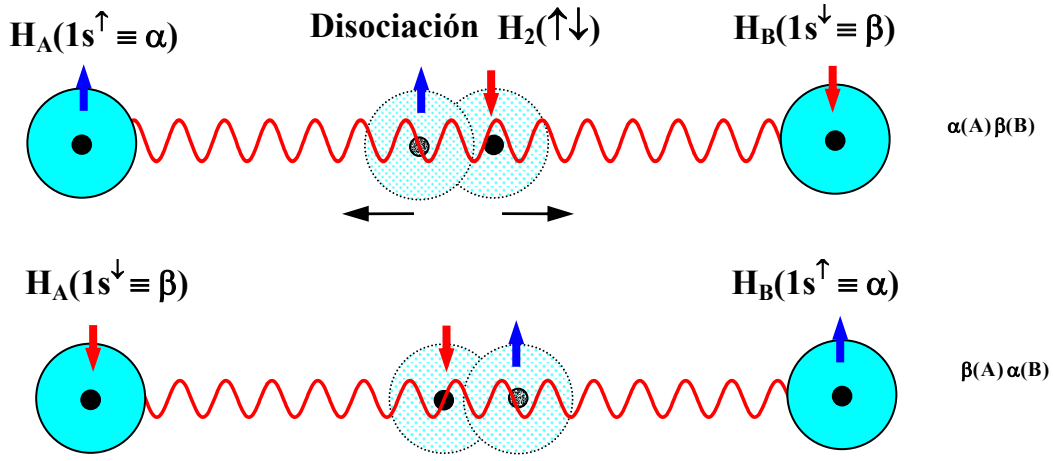
electrones. Cuando ambas rendijas están abiertas, se obtiene un diagrama de interferencia con bandas claras y oscuras. Supongamos que queremos detectar la presencia de un objeto que obstruye la rendija 1, representado por el detonador D de la bomba. Enviemos un fotón a través del dispositivo, cuya función de onda será del tipo $(\phi_1 + \phi_2)$. Al detectar la trayectoria de los fotones pueden aparecer dos resultados distintos. Puede suceder que el fotón incida sobre el detonador y la bomba explote. En tal caso, el fotón se habrá detectado atravesando la rendija 1 (ϕ_2=0), y produciéndose

una medida destructiva no deseada, la bomba explotará. Existe otra posibilidad, y es que el fotón se detecte en un punto P de la pantalla P_3 (situada detrás de las dos rendijas) sobre la región de un *mínimo* de interferencia. En estas zonas no inciden nunca fotones si *ambas* rendijas están abiertas, sólo lo hacen cuando una de ellas está obstruida (la rendija 1 en este caso). Pero la detección implica que el fotón ha pasado por rendija no obstruida 2, luego no ha interaccionado con el objeto (detonador D). Se trata de una *medida sin interacción*, pues se ha detectado la presencia del detonador sin que incida sobre él ningún fotón.

Además de la importancia fundamental en física cuántica de este resultado, la visión cuántica en la oscuridad abre la posibilidad de realizar fotografías en la más absoluta oscuridad. Ventaja inestimable en el caso de que la interacción con el objeto a fotografiar sea crucial. También es concebible la creación de imágenes de rayos-X sin exposición a la radiación de los pacientes.

b) Medidas sin interacción mediante *estados enredados*.

En primer lugar vamos a introducir el concepto de estado enredado, como un cierto tipo de estados que involucran de forma íntima a *varias* partículas. El caso más simple consta de *dos* partículas. Supongamos que partimos de una molécula de hidrógeno formada por dos núcleos (sin importancia en nuestro planteamiento) y dos electrones. Ambos electrones tienen un spin o momento angular intrínseco que puede adquirir únicamente dos direcciones que llamaremos arriba (o α) y abajo (o β). En el estado de menor energía de la molécula, los dos electrones tienen sus spines apareados,



Disociaciones posibles de una molécula de hidrógeno dependiendo del spin de los electrones. La línea ondulada indica la existencia de un tipo de relación no clásica entre los spines de ambos electrones.

es decir uno hacia arriba y el otro hacia abajo: $H_2(\uparrow\downarrow)$. Consideremos su disociación en dos átomos de hidrógeno en su estado fundamental, cada uno formado por un núcleo (positivo) y un electrón (negativo). Si nombramos a los dos núcleos que componen la molécula de hidrógeno como H_A y H_B, la disociación se puede realizar de dos formas distintas (con igual energía total), dependiendo del spin de los electrones. Se puede producir un estado $H_A(1s^{\uparrow}) + H_B(1s^{\downarrow})$, donde el núcleo A tiene un electrón en un orbital atómico 1s con spin hacia arriba (α) y el B lo tiene hacia abajo o bien a la inversa, $H_A(1s^{\downarrow}) + H_B(1s^{\uparrow})$. Tales posibilidades se describen con las funciones de onda para los electrones $\alpha(A)\beta(B)$ y $\beta(A)\alpha(B)$, respectivamente. Puesto que ambas situaciones son

indistinguibles (ya que los electrones son partículas cuánticas y gozan de tal propiedad), la función de onda que describe la disociación es:

$$\Psi(A,B) = \frac{1}{\sqrt{2}}\{\alpha(A)\beta(B) - \beta(A)\alpha(B)\} \neq \Phi(A)\Phi(B)$$

Dicha función describe un estado enredado con la característica de que su función de onda no se puede expresar como producto de dos factores Φ, cada uno de los cuales caracterice a un solo electrón. En cierto sentido los dos electrones están interrelacionados de una forma que no tiene análogo clásico, tal como exponemos a continuación.

Dados dos electrones en un estado enredado del tipo anterior, si medimos el spin del electrón del átomo A y obtenemos un resultado hacia arriba (α(A)), necesariamente el spin del electrón en B será hacia abajo (β(B)) incluso si no lo medimos, y a la inversa. En la primera medida se dice que la función de onda Ψ(A,B) ha *colapsado* en el término α(A)β(B), desapareciendo el β(A)α(B). Si en la medida se obtiene β(A), el estado del electrón en B es α(B), y Ψ(A,B) colapsa sobre el término β(A)α(B). Tal correlación negativa (arriba-abajo) entre spines es lo que se indica mediante una línea ondulada que une a ambos átomos de hidrógeno. Según la MC tal proceso de correlación de espines es ¡instantáneo! Además, el spin de las partículas en un estado Ψ(A,B), no está predeterminado, ya que en sucesivas medidas se obtienen los resultados aleatorios de spin hacia arriba y hacia abajo.

Este tipo de estados enredados fueron introducidos por Schrödinger y usados por A. Einstein B. Podolsky y N. Rosen[8] en 1935 para plantear medidas sin interacción (por lo que se llaman estados EPR) que parecían atentar contra el Principio de Incertidumbre de Heisenberg. Es posible usar los estados enredados de spin de los electrones para realizar medidas sin interacción. Supongamos dos interlocutores, habitualmente llamados Alicia y Roberto, que comparten dos partículas (electrones) en un estado enredado. Alicia está en la tierra mientras que Roberto puede estar en Andrómeda, a 4.5 años luz de distancia de la tierra. Si Alicia realiza una medida del spin de su electrón obteniendo el resultado hacia arriba (α(A)), *sabe* (aún sin medirlo) que el spin del electrón de Roberto es necesariamente opuesto (β(B)), debido a la correlación negativa de estos estados enredados. Ya que Alicia realiza su medida en, digamos una hora, al final de la cual ya sabe que el spin de Roberto es β(B) y que una señal a la velocidad de la luz tarda 4.5 años en afectar al spin del electrón de Roberto, la medida de Alicia no afecta al spin de Roberto. Concluimos que Alicia, tras su medida, sabe el spin del electrón de Roberto sin mediar interacción que viaje a la velocidad de la luz, lo que constituye una medida del spin de Roberto *sin interacción*.

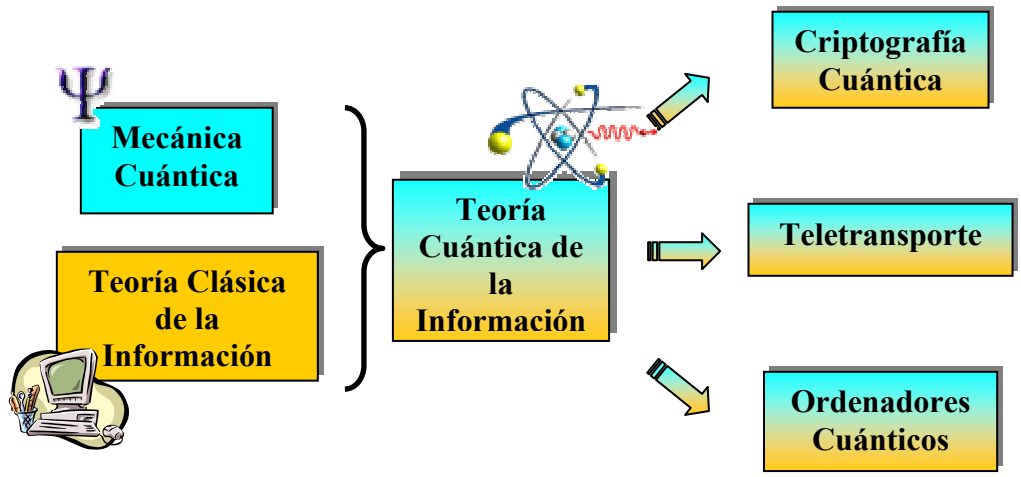
Usando otros estados enredados distintos, se pueden realizar medidas sin interacción de diversas magnitudes físicas.

Aplicaciones de los estados enredados

La existencia de los estados enredados es una de las características más distintivas de la física cuántica respecto a la clásica. En la actualidad, se están empezando a desarrollar aplicaciones que aprovechan el anterior tipo de correlaciones, llamas *no-locales*, entre partículas. Tienen especial importancia en la Teoría Cuántica de la Información, disciplina que está desarrollándose activamente en la actualidad.

La teoría de la información era un campo, hasta ahora, relacionado únicamente con las matemáticas, dando lugar a la Teoría Clásica de la Información. Durante mucho tiempo se creyó que esta teoría no dependía en absoluto de la representación de la información, ni de su puesta en práctica en dispositivos físicos. La situación empezó a cambiar cuando, hacia 1982, Richard Feynman (de nuevo) se percató de que cierto tipo de algoritmos, que clásicamente sufrían una ralentización exponencial cuando aumentaba el tamaño de los datos, al representarlos cuánticamente tal comportamiento se aceleraba. A partir de este trabajo se produjo un desarrollo vertiginoso que culminó con la unión entre la Teoría de la Información y la Mecánica Cuántica, naciendo la Teoría Cuántica de la Información[9].

A continuación vamos a revisar algunos de los avances dentro de este campo, relacionados con los estados enredados introducidos anteriormente.



a) Criptografía Cuántica

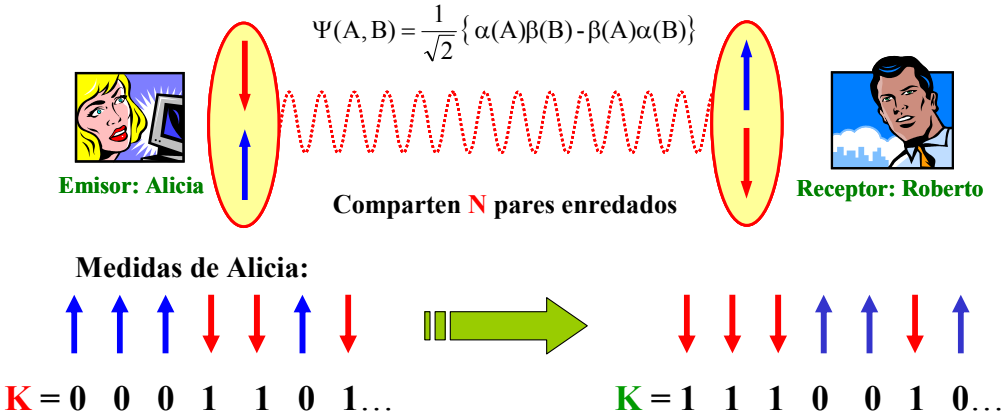
Para apreciar la aportación de la MC a la criptografía, comentemos los aspectos fundamentales de la criptografía clásica.

El objetivo de la criptografía es codificar los mensajes con la intención de ocultar su información a terceros. El esquema habitual es que el emisor Alicia, quiere enviar cierta información secreta (mensaje) al receptor Roberto. Para ello Alicia y Roberto deben compartir, previamente a la comunicación, cierta información secreta constituida por una clave K. Alicia codifica el mensaje usando la clave y obteniendo un mensaje encriptado o criptograma que envía a Roberto. Este, usando la clave secreta K, descifra el criptograma para recuperar en mensaje original. Desde un punto de vista clásico existe lo que se llaman *cifrados de secreto perfecto*, que tienen la propiedad de que el proceso de encriptar borra por completo la información relacionada con el mensaje original. Uno de estos cifrados es el de Vernam (introducido por Gilbert S. Vernam, de la compañía American Telephone and Telegraph y el comandante Joseph O. Mauborgne, del Cuerpo de Señaleros del Ejército estadounidense, en 1917). El mensaje a enviar se transforma en una secuencia de bits 0 y 1 al que se le suma módulo 2, una clave binaria K. Esta clave es una cadena aleatoria de ceros y unos, de longitud mayor o igual a la del mensaje a enviar. La aleatoriedad de K asegura que se borra cualquier información del mensaje original.

El principal inconveniente de este esquema clásico es el llamado *problema de distribución de la clave*. Los interlocutores deben comunicarse previamente al envío de información, mediante un canal seguro y secreto para distribuir la clave que usarán. Si

por algún motivo un espía (llamado genéricamente Eva) "pincha" la línea de comunicación y accede a la clave, podrá descifrar los mensajes intercambiados por Alicia y Roberto. Además, ninguna técnica clásica permite detectar la presencia de Eva.

Existe una solución matemática al problema de distribución de la clave dentro de un esquema clásico; es lo que se llama un *criptosistema de clave pública*. Un ejemplo son las claves RSA (introducidas en 1978 por Ronald L. Rivest, Adi Shamir y Leonard M. Adleman del MIT). Sin embargo, la seguridad de estos métodos se basa (generalmente) en suposiciones matemáticas no demostradas. En el caso de las RSA, la suposición es la ausencia de algoritmos suficientemente rápidos para factorizar números

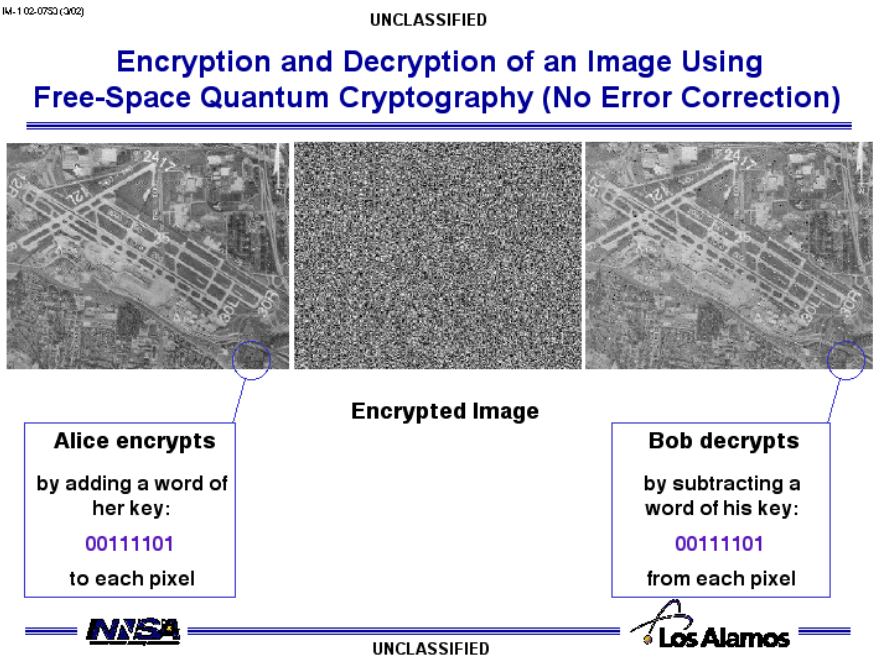


enteros grandes. Por otra parte, aunque parece que solucionan la distribución segura de la clave, si Eva "pincha" la línea de comunicación no es posible detectar su presencia.

La aportación cuántica al problema está relacionada con la seguridad que proporciona saber que una escucha no autorizada destruiría los estados usados en la comunicación. Existen varias estrategias que permiten la distribución segura de la clave, aquí expondremos la que emplea estados enredados. Supongamos que Alicia y Roberto quieren compartir una clave segura. Para ello comparten un conjunto de pares de partículas en estados enredados del tipo anterior $\Psi(A,B)$. Si Alicia realiza una medida en su partícula del par y obtiene un spin hacia arriba, sabe que la de Roberto tiene el spin hacia abajo. Si realiza varias medidas, cada una sobre una partícula de un par compartido distinto, obtendrá una secuencia del tipo ↑↑↑↓↑↓…, lo que implica que la secuencia detectada por Roberto será la complementaria ↓↓↓↑↓↑…. Si un spin hacia arriba significa un 0 y un spin hacia abajo un 1, Roberto sólo tiene que invertir los spines detectados y asignar los ceros y unos. Notemos que la clave secreta no existe previamente a la comunicación, sino que se crea durante la misma. La seguridad del protocolo descansa en que si Eva "pincha" la línea de comunicación, perturba y destruye el estado enredado compartido por Alicia y Roberto. Hecho que los interlocutores pueden detectar a través de la desigualdad de Bell[10], que los estados enredados cuánticos deben de violar. Esta posibilidad es nueva y no es posible en ningún protocolo criptográfico clásico.

La criptografía en la que la clave se ha distribuido cuánticamente, ha sido usada con éxito en varias aplicaciones prototipo. En la figura se muestra una fotografía aérea en la que la escala de grises se codifica con palabras binarias de longitud ocho. Alicia encripta los datos sumando la clave 00111101 a cada palabra, mientras que Roberto la descifra sumando la misma clave. La comunicación se realiza a través de la atmósfera y a pesar de que no hay corrección de errores, la fidelidad de la información recuperada es

bastante buena. En 1996, Muller usó una fibra óptica estándar (empleada en conversaciones telefónicas) de 23 Km bajo el lago Ginebra que conecta las ciudades de Ginebra y Nyon, para realizar la primera transmisión fuera de un laboratorio. En la actualidad ya existen empresas como Swisscom, que comercializan dispositivos criptográficos cuánticos con una comunicación a través de fibra óptica.



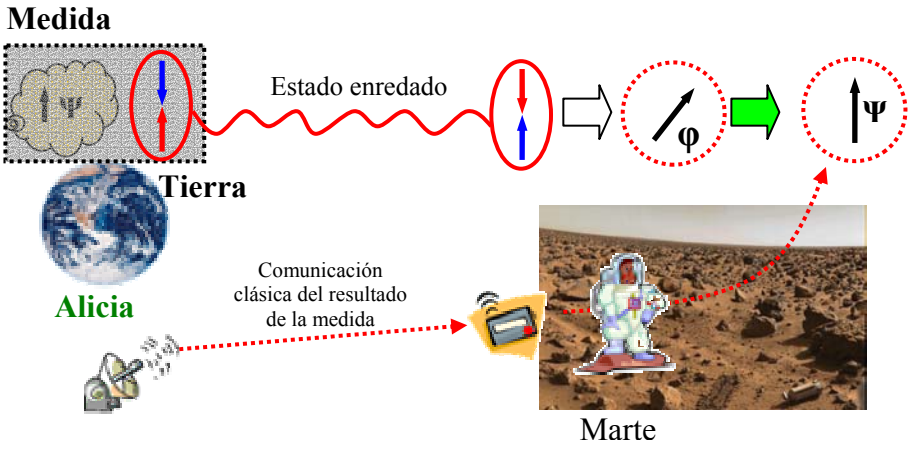
b) Teleportación

La utilización del fax está ampliamente extendida en la actualidad. La información (clásica) escrita en una hoja de papel se codifica y se envía a través de una conexión telefónica, reproduciéndose en el aparato receptor. En el proceso, tanto Alicia (emisor) como Roberto (receptor) mantienen una copia de la información.

Podríamos preguntarnos si podemos enviar información cuántica con un proceso similar al anterior, es decir ¿existe un fax cuántico? La información cuántica se expresa mediante la función de onda de algún sistema físico. Para copiarla necesitamos conocer esta función de onda, por ejemplo, realizando alguna medida. Sin embargo, durante el proceso de medida, el estado, así como la información que contiene se destruiría, perdiéndose irreversiblemente la información (colapso de la función de onda). En 1982, Wotters y Zurek[11] demostraron que (en general) la información cuántica no se puede copiar, demostrando el *teorema de no-clonación* de un estado cuántico desconocido. Por lo tanto, el fax cuántico no existe ¿Qué se puede hacer para que Alicia envíe una función de onda (información cuántica) a Roberto? La repuesta la proporcionaron en 1993, un grupo de investigadores, Charles Bennett, Giles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres y William Wootters[12], que establecieron las bases físicas de la teleportación. Para ello, usaron un canal de información clásico, y uno cuántico basado en el empleo de estados enredados. A continuación planteamos las ideas básicas que subyacen al protocolo de teleportación de información cuántica.

Supongamos que Alicia está en la Tierra y quiere comunicarle a Roberto, que está en Marte, la información cuántica contenida en la función de onda *desconocida* Ψ de cierta partícula. Como paso previo a la comunicación, los interlocutores comparten un par de partículas en un estado enredado (del tipo EPR). Alicia realiza una medida conjunta del sistema formado por su partícula descrita por Ψ y una de las partículas del

par EPR. El proceso afecta al estado de la partícula de Roberto en Marte transformándolo en el φ, además de romper la correlación (desenredo) entre ambas partículas del par, que a partir de ahora son independientes. Si entre los interlocutores existe una línea de comunicación clásica, Alicia puede comunicar a Roberto el resultado de su medida realizada en la Tierra. Esta información le permite a Roberto modificar el estado φ de su partícula para recuperar el estado Ψ.



Teleportación del estado Ψ desde la Tierra hasta Marte. La medida de Alicia deja la partícula de Roberto ene estado φ, que permite recuperar el Ψ cuando Alicia comunica a Roberto el resultado de su medida conjunta.

Como consecuencia de la medida que Alicia realiza sobre el sistema de dos partículas, borra la información del estado inicial Ψ, por lo que en el proceso de teleportación se destruye el original, a diferencia de lo que ocurre en un fax clásico. Notemos que, a pesar de que la correlación que existe en un par EPR permitiría que el efecto de la medida de Alicia se propagara a velocidad infinita, Roberto no recupera el estado Ψ hasta después de una comunicación clásica. Este es el motivo por el cual, en conjunto, el proceso de teleportación no implica una comunicación a velocidad superior a la de la luz. Otra característica es que ninguno de los interlocutores conoce el estado comunicado Ψ; ya que si éste fuera conocido se podría, simplemente, enviar la información por un canal clásico (teléfono).

La teleportación implica la "absorción" de la información que caracteriza a un estado Ψ de un sistema cuántico, su transmisión y finalmente la "materialización" sobre *otro* sistema o partícula distinta. El estado del sistema original se destruye. Realmente no es el objeto original lo que se transmite, sino *sólo su información*.

La primera demostración de la posibilidad de producir teleportación se llevó a cabo en 1997, en la Universidad de Innsbruck, por el grupo de Anton Zeilinger[13]. En este experimento se teleportó el estado de polarización de un fotón, usando un par EPR de fotones en un estado enredado de polarización.

A pesar de que estamos en el umbral de nuevas e intrigantes posibilidades a la hora de transmitir información, todavía estamos lejos de conseguir algo parecido a lo que se muestra en películas como Star Treck, en las que cuerpos humanos se teleportan (o teletransportan) de un lugar a otro.

c) Ordenadores cuánticos[14]

El concepto de ordenador ha ido evolucionando a lo largo de la historia. Uno de los primeros "ordenadores" se puede encontrar en Stonehenge (2800 aC). Es un

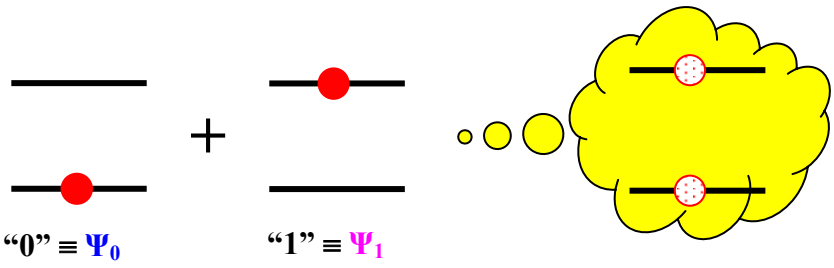
conjunto circular de grandes piedras que servía al hombre primitivo para predecir eventos astronómicos. Evidentemente, si hubiera que calcular otro tipo de acontecimientos habría que reprogramar el dispositivo lo que implicaría cambiar las piedras de lugar. No era un ordenador muy versátil.

La tendencia actual es la de miniaturizar cada vez más los componentes de los ordenadores. Lo apreciamos en nuestros ordenadores personales, cada vez más pequeños y rápidos. La primera ley de Moore asegura que el número de transistores que se pueden introducir en un chip se incrementa de forma exponencial con el tiempo, concretamente cada 3.4 años este número se multiplica por cuatro. Es evidente que el límite no está lejos. Llegará un momento en que los dispositivos sean de tamaño atómico y las leyes cuánticas empezarán a plantear limitaciones tecnológicas ¿Será un callejón sin salida? ¿Se detendrá el progreso de los ordenadores?

A pesar de que los ordenadores actuales funcionan de acuerdo con las leyes de la física cuántica, la representación de la información sigue siendo clásica, mediante cadenas de bits. Un bit es la unidad fundamental de información clásica representada por un sistema que puede situarse en *dos* posiciones distintas, llamadas 0 y 1. Cualquier computación consiste en la evolución de sistemas físicos en los que se ha codificado la información inicial o datos. Si la evolución es clásica, tenemos los ordenadores clásicos. Si la evolución de los sistemas es cuántica, tendremos un nuevo tipo de computación que dará lugar a los ordenadores cuánticos.

En estos ordenadores cuánticos, no solo la evolución es cuántica sino que la propia representación de la información también lo será. Si representamos un 0 por una función de onda Ψ_0 y un 1 por Ψ_1, dado que la MC es una teoría lineal, cualquier combinación de estas funciones del tipo $\Psi_Q = a\,\Psi_0 + b\,\Psi_1$ será otra posible función de onda. Además de un 0 y un 1 tenemos todas las posibilidades intermedias dependiendo del valor de los coeficientes a y b. La función Ψ_Q representa la unidad básica de información cuántica y se denomina *qubit* (quantum bit).

Una computación cuántica implicará la evolución temporal de estos qubits, existiendo una mayor riqueza de posibles estados a usar respecto a los de una



Representación de la unidad cuántica de información o qubit.

computación clásica. Las superposiciones de estados y los estados enredados son genuinamente cuánticos, sin análogo clásico. Su presencia en el contexto de la computación cuántica es ineludible.

Para atisbar las ventajas que puede aportar la computación cuántica frente a la clásica, planteémonos calcular el valor de una función f(x) para los valores x = 0,1,…7. Un ordenador clásico debe realizar 8 evaluaciones de f. Supongamos ahora que pudiéramos construir el estado de un sistema representado por la función de onda $\Psi = c_0\varphi_0 + c_1\varphi_1 + \ldots + c_7\varphi_7$, donde cada término del tipo φ_k (k = 0,..,7) lleva la información

acerca de uno de los 8 primeros números enteros x. Realizando una aplicación sobre Ψ de la operación (unitaria) cuántica U, definida como $U\{\varphi_k\} = \varphi_{f(k)}$, obtendríamos $U\Psi = c_0\varphi_{f(0)} + \ldots + c_7\varphi_{f(7)}$. La función UΨ contiene la información de *todos* los valores de f(x) y se ha obtenido mediante *una única aplicación de U*. En general, cualquier operación U realizada sobre una función de onda Ψ, se transforma en la acción sobre todas sus componentes $\{\varphi_k\}$:

$$U\Psi = U\left(\sum_{i=1}^{N} c_i\varphi_i\right) = \sum_{i=1}^{N} c_i\left(U\varphi_i\right)$$

De ahí la ventaja de la computación cuántica frente a la clásica. Desgraciadamente, todavía existe un problema. Puesto que la extracción de la información de UΨ implica realizar una medida, ésta destruye la superposición obteniéndose *un solo resultado*. Parece que no hemos ganado nada. El problema de la medida es el causante de que los algoritmos que aprovechan la representación cuántica de la información, sean escasos. El caso más interesante es el algoritmo de Shor[14] (1994), que factoriza números enteros en un tiempo que escala polinómicamente con el tamaño del número. Ningún algoritmo clásico consigue esta ley de escalaje tan lenta respecto a los recursos (tiempo de cálculo) necesarios para realizar una factorización. Las claves criptográficas actuales del tipo RSA-2048 (cuya ruptura implica la obtención de los factores primos de un número representado mediante 2048 bits), requieren, usando los medios actuales, unos 10^{15} años. Ahí radica su seguridad. Sin embargo, usando la potencia de un hipotético ordenador cuántico que empleara el algoritmo de Shor, tardaría tan solo unos ¡36 minutos! Por lo tanto, quién dispusiera de tal dispositivo cuántico sería capaz de romper todas las claves en uso actualmente en bancos, ejército, comunicaciones por internet, etc.

Un segundo algoritmo cuántico que merece nuestra atención es el algoritmo de búsqueda, planteado por Grover en 1998, así como un conjunto de adaptaciones del mismo a otros problemas. Clásicamente, si queremos encontrar un cierto ítem de una base de datos que cumpla cierta condición, por ejemplo, dado el nombre de un abonado de telefónica encontrar su número de teléfono, es fácil ya que los nombres de los abonados están ordenados alfabéticamente. Sin embargo el problema opuesto, el de dado un teléfono encontrar el nombre del abonado al que pertenece, es un problema difícil. Si nuestra lista tuviera $N = 10^6$ números, deberíamos buscar (en promedio) $N/2 = 5\ 10^5$ veces antes de encontrar el abonado buscado. El problema clásico escala como O(N). Grover demostró que usando un determinado algoritmo de búsqueda en un ordenador cuántico, el problema escalaría como $O(N^{1/2})$, es decir que para $N = 10^6$ números, deberíamos realizar sólo unas ¡1000 búsquedas! antes de encontrar la solución. La ganancia es evidente. Tal posibilidad se podría emplear también para romper claves, simplemente por búsqueda exhaustiva.

Existen otros algoritmos similares o que emplean las mismas técnicas que los dos anteriores y que amplían el espectro de utilidad. Sin embargo, por el momento son pocos los conocidos.

No todo son ventajas en estos dispositivos. La necesidad de utilizar superposiciones de estados representa un problema grave, ya que su coherencia se pierde con gran facilidad. Para evitarlo se han diseñado complejos métodos de control de posibles errores, que (en teoría) permitirían la ejecución de cualquier algoritmo cuántico el tiempo necesario para obtener una solución.

Mención especial merecen los grandes esfuerzos tecnológicos que se están poniendo en práctica para la construcción de los ordenadores cuánticos. A pesar de la

dificultad, ya se ha conseguido realizar puertas cuánticas simples y ejecutar pequeños algoritmos que, por el momento, sólo tienen un interés académico. Las estimaciones actuales parecen situar la construcción de un ordenador cuántico en unos 20 ó 30 años. Quizás entonces seamos capaces de realizar simulaciones de procesos físicos que por el momento son imposibles, como por ejemplo predecir la evolución del tiempo atmosférico mediante un modelo matemático.

El horizonte de las posibilidades abiertas en la física por la utilización de estados enredados, cuyo origen está en el dualismo onda-partícula, parece todavía lejano. Relativo a este dualismo decía Einstein *"si la mecánica cuántica fuese correcta, el mundo estaría loco"*. A lo que Daniel Greenberger (City College de Nueva York) responde *"Einstein tenía razón. El mundo está loco"*. Transcurridos cien años desde la creación de la física cuántica, sus aportaciones, tanto respecto a la precisión con la que describe la naturaleza, como por las nuevas ideas que proporciona, nos siguen sorprendiendo e intrigando.

---

[1] J. M. Sánchez Ron; *Historia de la física cuántica.* Ed. Dracontos (2001).

[2] C. J. Foot; *Laser cooling and trapping of atoms,* Contemporary Physics **32** 369 1991.
A. Aspect y J. Dalibard, *El enfriamiento de átomos por láser,* Mundo Científico Nº 144 vol 14 p 216.

[3] H. Takuma, K. Shimizu y F. Shimizu; *Fundamental Problems in Quantum Theory*, *N. York* p217 1995

[4] C. Brukner y A. Zeilinger; *Young's experiment and finiteness of information*, Phil. Trans. R. Soc. London A **360** 1061 (2002).
L. Hackermüller, S. Uttenthaler, K. Hornberger, E. Reiger, B. Brezger, A. Zeilinger y M. Arndt; *The wave nature of biomolecules and fluorofullerenes*, Phys. Rev. Lett. **91** 090408 (2003).

[5] R. P. Feynman; *Mecánica cuántica vol III*. Ed. Fondo Educativo Interamericano, S.A. (1971).

[6] A. Tonomura, J. Endo, T. Matsuda, T Kawasaki y H. Exawa; *Demonstration of single-electron buildup of an interference pattern*, Am. J. Phys. **57**(2) 117 (1989).

[7] A.C. Elitzur y L. Vaidman; *Quantum mechanical interaction-free measurements*, Found. of Phys. **23** 987 (1993).
P. Kwiat, H. Weinfurter y A. Zeilinger; *Visión cuántica en la oscuridad*, Investigación y Ciencia (enero 1997, p54).

[8] A. Einstein, B. Podolsky y N. Rosen; *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev. **47** 777 (1935).

[9] A. Zeilinger; *Fundamentals of quantum information*, Physics World p35 (marzo 1998).

[10] F. Selleri; *El debate de la teoría cuántica*, Ed. Alianza Universidad 453.

[11] W. K. Wootters y W. H. Zurek; *A single quantum cannot be cloned*, Nature **299** 802 (1982).

[12] Charles H. Bennett, Giles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres y William Wootters; *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70** 1895 (1993).
A. Zelinger, *Teletransporte cuántico*, Invest. y Ciencia p58 (junio 2000).

[13] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter y A. Zeilinger; *Experimental quantum teleportation*, Nature **390** 575 (1997)

[14] A. Barenco; *Quantum physics and computers*, Contemporary Physics **37** 375 (1996).
P. J. Salas y A. L. Sanz; *Computación cuántica: una revolución en el tratamiento de la información*, Rev. Española de Física **15**(3) 20 (2001).