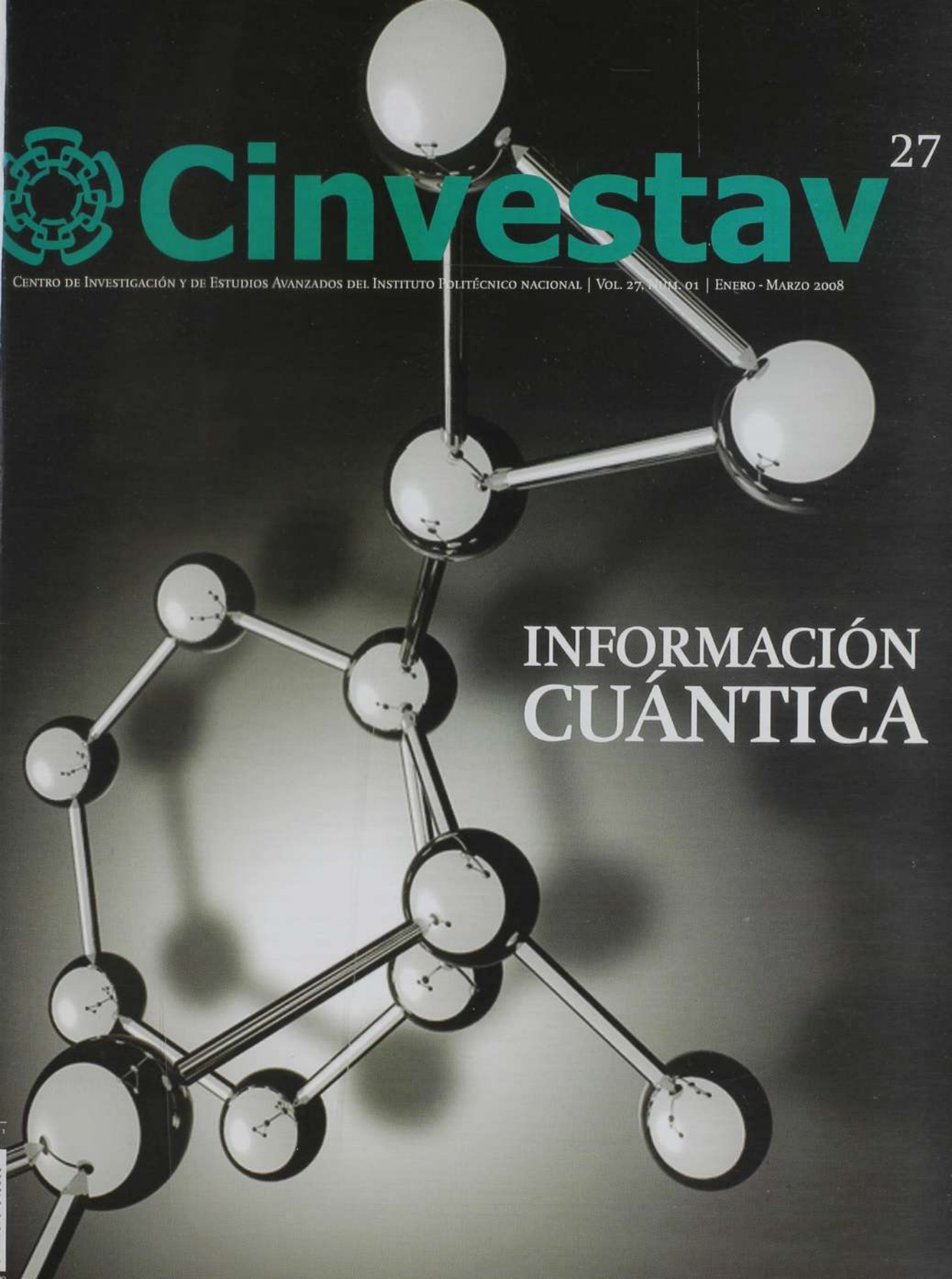

Cinvestav

27

Centro de Investigación y de Estudios Avanzados del Instituto Politécnico nacional | Vol. 27, núm. 01 | Enero - Marzo 2008

INFORMACIÓN CUÁNTICA

Editorial

Un tema recurrente en los contenidos publicados en la revista *Cinvestav* se relaciona con el reconocimiento de que el desarrollo de un país o de cualquier nación se sustenta a partir del desarrollo del conocimiento científico y tecnológico. En este contexto, las universidades y los centros de investigación son las instituciones donde se construyen las bases que permitirán a sus egresados realizar investigación en los diversos dominios científicos y tecnológicos.

La construcción de una agenda de investigación y los caminos de producir el conocimiento científico dependen de las herramientas o instrumentos disponibles para recabar y analizar información asociada con los fenómenos en estudio. Artefactos tecnológicos que van desde buscadores en Internet, hojas de cálculo, o procesadores de texto, hasta herramientas como el *software* Maple o Mathematica, o simuladores que se utilizan para realizar actividades asociadas con la investigación, no sólo facilitan la expresión de las ideas y los procesos de investigación, sino que también moldean y orientan las formas de desarrollar la ciencia y la tecnología. Además, el uso de las herramientas está influyendo en la forma de interactuar y fomentar el trabajo multidisciplinario en las comunidades científicas. Los trabajos que se publican en este número son un ejemplo de cómo diversas comunidades trabajan sobre un programa común relacionado con la información cuántica.

¿Cómo se construyen y se actualizan las agendas o los programas de investigación científica y tecnológica? ¿Cómo se desarrollan e incorporan los métodos o estrategias necesarias para realizar investigación frontera en las disciplinas? ¿Hasta qué punto los cambios en las programas de investigación se traducen en cambios o transformaciones en la formación de futuros investigadores? ¿Son consistentes los modelos tradicionales de generación del conocimiento científico y tecnológico con las prácticas que emergen del uso sistemático de diversas herramientas computacionales? ¿Qué ajustes en la estructura y organización de las instituciones son necesarios para crear áreas y programas de investigación multidisciplinaria? La discusión amplia y abierta de este tipo de preguntas puede orientar la reflexión acerca de la importancia y el compromiso de la comunidad científica de constantemente revisar y ajustar no sólo los programas de investigación, sino también las rutas en la formación de los investigadores.

La formación de los investigadores es un tema que se relaciona directamente con el funcionamiento y desarrollo del sistema educativo en su conjunto. La prensa ha destacado, recientemente, los bajos niveles de aprovechamiento que muestran los estudiantes de educación básica en ciencias, matemáticas y uso del lenguaje en las evaluaciones internacionales y nacionales. ¿Cuál es el papel de la comunidad científica en la formación de los profesores de esas disciplinas? ¿Qué concepción de ciencia y tipo de competencia científica se debe promover en la formación básica de los estudiantes? ¿Qué recursos, contenidos, estrategias y formas de razonamiento disciplinario hay que ofrecer para que los estudiantes obtengan las bases y desarrollen una cultura científica?

Con su experiencia en la generación de conocimiento, la comunidad académica del Cinvestav puede contribuir significativamente en la discusión de estas preguntas y así orientar el diseño del proyecto de educación del país. Finalmente agradezco al Dr. Oscar Rosas por la selección y coordinación del proceso de revisión de los artículos que se publican en este número de la revista.

Luz Manuel Santos Trigo
msantos@cinvestav.mx

Presentación

El vertiginoso avance que tuvo la tecnología durante el siglo XX permitió identificar a la generación y al manejo de la información como una disciplina científica. El diseño y la realización de dispositivos computacionales cada vez más pequeños y eficientes fueron posibles gracias a la miniaturización de la electrónica. Casi imperceptible para el público lego, la mecánica cuántica ha estado siempre presente en el desarrollo de la informática y telemática modernas: desde la sustitución de bulbos por transistores hasta el perfeccionamiento de la tecnología que dio origen a los dispositivos electrónicos portátiles como las *laptop*, el *iPod*, la telefonía celular y la Internet. Todos estos avances han repercutido, a su vez, en otras áreas del conocimiento humano como son la mecatrónica y la medicina, por mencionar algunas. Aceptando que la miniaturización de los dispositivos electrónicos obedece la célebre *Ley Moore*,[1] en un futuro no muy lejano se estarán diseñando y construyendo computadoras tan pequeñas que, para su funcionamiento, requerirán del control detallado de las propiedades cuánticas de sistemas físicos como la luz, los átomos y las moléculas.

Los países desarrollados han sido sensibles a esta posibilidad y, desde hace un par de décadas, fomentan e impulsan las investigaciones teóricas y experimentales orientadas al desarrollo e implementación de una *teoría cuántica de la información*. La realización de una computadora cuántica abriría opciones impensables de llevar a cabo con una computadora convencional.[2] México deberá participar en esta ambiciosa búsqueda si no queremos quedar, nuevamente, en el atraso y vernos únicamente como compradores de las tecnologías correspondientes.

Las instituciones científicas más importantes de nuestro país desarrollan investigación en alguno o varios de los rubros de la información cuántica. Teniendo intereses comunes en estos tópicos, nuestra comunidad se ha organizado para establecer una red nacional que incluya a todas y cada una de estas instituciones. Como resultado inmediato se ha creado la División de Información Cuántica de la Sociedad Mexicana de Física. Con este número de la revista *Cinvestav* presentamos un panorama muy general de algunos temas que son de interés en este ámbito. Cabe mencionar que por razones de espacio y tiempo editorial no están representadas todas las instituciones involucradas en la red nacional antes mencionada. Nuestro objetivo es llamar la atención de los jóvenes estudiantes de ciencias e ingenierías para que se entrenen como investigadores en esta disciplina del conocimiento científico.

Los 'objetos' microscópicos tienen propiedades físicas que contravienen nuestra experiencia cotidiana. Los estados cuánticos de dos átomos, por ejemplo, pueden estar correlacionados. Esto significa que lo que le ocurra a uno afecta al otro aun cuando los átomos estén separados espacialmente (digamos que uno está en China y otro en el D. F.) A esta propiedad se le conoce como *entrelazamiento cuántico*. Alfed U'Ren, junto con otros colegas de la Facultad de Ciencias de la UNAM y de la División de Física Aplicada del CICESE, nos introducen a este tema desde el punto de vista experimental con su artículo "Fotones enredados y desigualdades de Bell: explorando la no-localidad". El lector encontrará una buena exposición del famoso argumento de Einstein, Podolsky y Rosen (EPR) tanto como de las desigualdades de Bell, que han dado lugar a muchas discusiones en el ámbito de los fundamentos de la teoría cuántica. A manera de revisión, Andrei Klimov nos presenta el artículo "Información cuántica: ideas y perspectivas", donde también nos comenta acerca de la posibilidad de *teleportar* el estado cuántico de los sistemas microscópicos sin que éstos se desplacen espacialmente.

1 El número de componentes electrónicos por unidad de área se duplica aproximadamente cada dos años. Gordon E. Moore, *Cramming more components onto integrated circuits*, Electronics, Volume 38, Number 8, April 19, 1965.

2 Es pertinente mencionar que esta afirmación se refiere al tiempo de cálculo de ciertos algoritmos; en muchos otros aspectos, tal como lo menciona Scott Aaronson en su reciente artículo de *Scientific American* (2008, vol. 293, núm. 3, pp. 50), las computadoras cuánticas sólo proporcionarían una mejora modesta a las computadoras convencionales.

El entrelazamiento cuántico puede ser explotado para transmitir información en forma segura, tal y como lo expone Blas Rodríguez-Lara en su artículo "Alicia y Beto se comunican: introducción a la comunicación cuántica". El autor aclara también que la transmisión de información no está exenta de errores. La implementación de esta técnica debe incluir mecanismos que corrijan el 'ruido' generado, sobre todo si se trata de claves cifradas como las usadas por las instituciones bancarias. Kamil Bradler describe los pormenores de este procedimiento en su artículo "Distribución de claves cuánticas". La primera parte de este número especial se cierra con el artículo de Sara Cruz y Oscar Rosas-Ortiz, "Estados coherentes y gatos de Schrödinger". En él se muestra que usando luz coherente se pueden construir entrelazamientos cuánticos que son una buena alternativa para implementar operaciones en los algoritmos de cómputo cuántico.

En la segunda parte de este número, Eduardo Gómez nos habla de los pormenores experimentales de la implementación de operaciones cuánticas con átomos en su artículo "Procesadores cuánticos atómicos". El autor discute las complicaciones que surgen al intentar mantener atrapados a los rebeldes átomos, que siempre quieren 'escabullirse' por entre las paredes del 'recipiente' que los contiene. También en el ámbito experimental, a lo largo de su artículo Máximo López-López y Víctor H. Méndez-García nos explican qué son los puntos cuánticos y cómo pueden usarse en el diseño de computadoras cuánticas. Los algoritmos de cálculo cuántico explotan la superposición lineal de los estados cuánticos para mejorar el uso de recursos temporales y espaciales con respecto a sus contrapartes clásicas. Guillermo Morales nos explica los detalles matemáticos de este procedimiento en su artículo "Codificación superdensa: característica única del cómputo cuántico". Todas estas operaciones requieren de la manipulación y del control de los sistemas cuánticos. Francisco Delgado da cuenta de ello en su artículo "Control cuántico: dos enfoques". Por otro lado, en el artículo "Caminatas cuánticas: definiciones y algoritmos", Salvador E. Venegas Andraca nos muestra cómo pueden implementarse los algoritmos cuánticos con el uso de caminatas cuánticas, al tiempo que hace una exposición clara de los diferentes modelos computacionales. Por último, Octavio Castaños cierra el número especial de la revista presentándonos un breve panorama histórico de la "Creación de la División de Información Cuántica de la Sociedad Mexicana de Física", además de exponer las inquietudes de nuestra comunidad y algunas de las medidas que se piensan tomar para solventar algunos de los rezagos científicos que esta disciplina enfrenta en nuestro país. Están todos ustedes invitados a integrarse como miembros de nuestra nueva división en la Sociedad Mexicana de Física.

Agradecemos el apoyo secretarial de la Srita. Miriam Lomelí Cortés así como la colaboración de los revisores anónimos de los artículos que aquí se presentan. La participación de Karina Jiménez, estudiante del Departamento de Física del Cinvestav, fue de enorme ayuda en diversos aspectos del proceso editorial. La disposición del Dr. Manuel Santos, editor de la revista *Cinvestav*, permitió la materialización de este número especial. Finalmente, reconocemos el patrocinio del Centro de Investigación y de Estudios Avanzados (Cinvestav) y agradecemos las facilidades que se nos brindaron para usar este espacio como mecanismo de difusión de todos los artículos que integran este número.

Oscar Rosas-Ortiz (Departamento de Física, Cinvestav)
Rocío Jáuregui (Instituto de Física, UNAM)
Sara Cruz y Cruz (UPIITA-IPN)

Contenido

La revista *Cinvestav* antes *Avance y Perspectiva*, órgano oficial del **Cinvestav-IPN** (Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional) es una publicación trimestral dedicada a la difusión y divulgación de la actividad científica y de la vida académica del Centro. Los artículos publicados son responsabilidad de sus autores. Se autoriza la publicación parcial o total del material publicado con el requisito de que se cite la fuente. La edición correspondiente a enero-marzo 2008, volumen 27, número 1 se terminó de imprimir en junio de 2008. Tiraje: 5000 ejemplares. Certificado de Reserva de Derecho de Autor 04-2006-051210075200-102, expedido por la Dirección General de Derechos de Autor de la Secretaría de Educación Pública. Certificado de Licitud de Título 13538 y Certificado de Licitud de Contenidos 11111, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. ISSN 1870-5499. Negativos, impresión y encuadernación: Lito Laser S.A. de C.V., Primera Privada de Aquiles Serdán núm. 28, Col. Santo Domingo Azcapotzalco, CP 02160, Del. Gustavo A. Madero, México DF. Sede del **Cinvestav**: Av. Instituto Politécnico Nacional núm. 2508, Col. San Pedro Zacatenco, CP 07360, Del. Gustavo A. Madero, México DF. Web del **Cinvestav**: www.cinvestav.mx

Fotones enredados y desigualdades de Bell: explorando la no-localidad

EN EL TRANSCURSO DEL ÚLTIMO SIGLO, LA VALIDEZ DE LA MECÁNICA CUÁNTICA HA SIDO OBJETO DE ESCRUTINIO Y CUESTIONAMIENTO. A CONTINUACIÓN, LOS AUTORES EXAMINAN ESTE TEMA A PARTIR DE LOS ARGUMENTOS DE EINSTEIN, PODOLSKY Y ROSEN, ASÍ COMO DEL TEOREMA DE BELL, Y PRESENTAN RESULTADOS EXPERIMENTALES QUE CONFIRMAN LA VALIDEZ DE LA MECÁNICA CUÁNTICA COMO DESCRIPCIÓN CORRECTA DE LA NATURALEZA A MUY PEQUEÑA ESCALA.

Luis Edgar Vicent, Alfred B. U´Ren, Erick Barrios, Victor Velázquez, Enrique López-Moreno y Marcela Grether

Actualmente, nuestra descripción de los fenómenos físicos que ocurren a escala atómica está dada en términos de estadística y probabilidad. Al utilizar este tipo de descripción se predice que, a muy pequeña escala, cuando realicemos una medición sobre algún sistema físico, la medición misma alterará al sistema de tal manera que no será posible obtener un valor definido de la cantidad observada. La mecánica cuántica, que estudia la física de los fenómenos a pequeña escala, predice que si conocemos con gran precisión la posición, por ejemplo, de una partícula, no podremos determinar mediante una medición su velocidad. Este fenómeno cúantico se conoce como el principio de incertidumbre de Heisenberg.

En contraste con la mecánica cuántica, la física de sistemas macroscópicos, que es descrita por la mecánica clásica, nos permite obtener valores bien definidos de una medición simultánea de la posición y la velocidad de un objeto.

En los inicios de la mecánica cuántica se dieron acalorados debates acerca de la concepción estadística de los sistemas físicos. Albert Einstein, por ejemplo, pensaba que la mecánica cuántica era una teoría incompleta, dado que nos impide conocer simultáneamente y con precisión ciertas cantidades físicas asociadas con la dinámica de las partículas. Este fue el objeto de discusión en un artículo que publicó en colaboración con Boris Podolsky y Nathan Rosen [1] en 1935.

LUIS EDGAR VICENT Doctor en Ciencias por la Universidad Autónoma del Estado de Morelos (2007). Actualmente es investigador posdoctoral en el Departamento de Óptica del Centro de Investigación Científica y Educación Superior de Ensenada (CICESE). Sus principales áreas de interés son la óptica cuántica no-lineal y la óptica matemática orientada al procesamiento de señales discretas. lvicent@cicese.mx

ALFRED U'REN Licenciado en Física por la Universidad Autónoma Metropolitana (1997) y doctor en Óptica por la Universidad de Rochester (2004). Su tesis doctoral fue elaborada bajo la supervisión de Ian Walmsley, profesor de física experimental en la Universidad de Oxford (Reino Unido), lugar donde realizó una estancia académica entre 2001 y 2004. Actualmente es investigador titular en el Departamento de Óptica del CICESE. Pertenece al Sistema Nacional de Investigadores (nivel I). Sus temas de investigación incluyen óptica cuántica, pulsos ultra cortos y óptica no-lineal. auren@cicese.mx

ERICK BARRIOS BAROCIO. Realizó sus estudios de licenciatura en Física en la Facultad de Ciencias de la UNAM. Actualmente realiza experimentación en óptica cuántica.

VÍCTOR VELÁZQUEZ AGUILAR. Obtuvo su doctorado en el **Cinvestav** en el área de modelos nucleares y caos cuántico. Desempeña sus labores en los laboratorios de óptica cuántica de la Facultad de Ciencias de la UNAM. viva@fciencias.unam.mx

ENRIQUE LÓPEZ-MORENO. Doctor por la Facultad de Ciencias de la UNAM. Actualmente coordina los laboratorios de óptica de esta facultad. Su campo de trabajo abarca la óptica clásica y la óptica cuántica. elm@fciencias.unam.mx

MARCELA GRETHER GONZÁLEZ. Se doctoró en la Universidad Autónoma Metropolitana en temas de condensación de Bose-Einstein. Su trabajo actual está orientado a dicho tema, así como al campo de la óptica clásica y la óptica cuántica. mdgg@fciencias.unam.mx

El argumento de Einstein-Podolsky-Rosen (EPR)

Dicho artículo llevaba por nombre "¿La descripción de la realidad por parte de la mecánica cuántica puede ser considerada completa?"[1] y representó un formidable catalizador en el estudio del *enredamiento cuántico*, quizá la propiedad clave que distingue a los sistemas cuánticos de los clásicos, y que se refiere al hecho de que la medición de una primera partícula puede determinar el resultado en una medición futura de una segunda partícula. El argumento presentado por EPR pretende demostrar que la mecánica cuántica es una teoría incompleta, partiendo de ciertas afirmaciones que, en su opinión, toda teoría física debería cumplir, y llegando a una inconsistencia con el principio de incertidumbre de Heisenberg, el cual constituye una piedra angular de la teoría cuántica. El argumento de EPR parte de suponer la validez de lo que ellos llamaron *localidad* y *realismo*: la localidad es la postura filosófica según la cual los efectos físicos se propagan a una velocidad finita, mientras que el realismo sostiene que un objeto debe poseer un estado físico determinado, independientemente de si es o no observado. David Bohm reformuló estas ideas en 1952 [12], a través de un experimento pensado (*gedanken experiment*) haciendo uso de variables discretas –espines (del inglés *spin*: giro, girar)– en lugar de usar variables continuas, como la posición y el momento, como se hizo en el argumento original de EPR. A continuación delineamos este experimento pensado.

Supongamos que tenemos una partícula sin espín, la cual podemos imaginar como una partícula que no gira sobre su propio eje. Supongamos, ahora, que nuestra partícula se separa o, equivalentemente, que decae en dos partículas independientes, con espines opuestos y emitidas en direcciones opuestas, descritas por lo que se conoce como un estado singulete anti-correlacionado en espín. Supongamos que Alicia y Beto observan el experimento y Alicia recibe a una de las partículas, mientras que Beto recibe a su contraparte. Una pareja de partículas con estas propiedades es tal que si Alicia determina el sentido de giro de su partícula mediante una medición, sabrá con certeza que el sentido de giro de la partícula de Beto es el opuesto a la suya, aun sin medirlo. Ahora, dado que las partículas son tridimensionales, su movimiento rotacional se descompone también en tres dimensiones, que llamaremos como los ejes cartesianos X,Y,Z. Si Alicia determina el espín de su partícula en la dirección X, entonces la mecánica cuántica le impide conocer simultáneamente el espín en las direcciones Y o Z, como consecuencia directa del principio de incertidumbre de Heisenberg. Sin embargo, supongamos que Beto mide la componente Y del espín de su partícula, y que Alicia le comunica por un canal de comunicación usual (por ejemplo, vía telefónica) el resultado de su medición. De esta manera Beto podría conocer simultáneamente el espín en las direcciones X y Y, en conflicto con el principio de incertidumbre de Heisenberg y, por lo tanto, con la teoría cuántica misma.

Inspirado en el experimento pensado de Bohm, en 1964 John Bell [2] formuló un teorema en la forma de una desigualdad, aplicable a cualquier sistema físico que cumpla con los principios de realismo y de localidad. Para entender en qué consiste esta desigualdad (en una de sus variantes), supongamos que a,b y c son tres propiedades dicotómicas, es decir que admiten únicamente dos posibles valores, que caracterizan a una colección de objetos. Entonces, si $N(a,\neg b)$ representa el número de objetos que tiene la propiedad a pero que no tiene la propiedad b, Bell nos dice que debe cumplirse que

$$N(a,\neg b) + N(b,\neg c) \geq N(a,\neg c), \qquad (1)$$

es decir, que el número de elementos del conjunto con la propiedad a pero no la b, más el número de elementos con la propiedad b pero no la c es mayor o igual que el número de elementos con la propiedad a pero no la c.

Para demostrar la validez de esta desigualdad de Bell partimos de que la suma

$N(a,\neg b,c) + N(\neg a,b,\neg c) \geq 0$, lo cual es evidentemente cierto, dado que cada número de objetos es cero o un número entero positivo. Sumando $N(a,\neg b,\neg c) + N(a,b,\neg c) = N(a,\neg c)$ a cada lado de la desigualdad anterior (donde la igualdad proviene del supuesto que las propiedades c y $\neg c$ cubren el espectro completo de posibilidades), llegamos a la ecuación 1. Para un sistema como el supuesto para el experimento pensado de Bohm, a, b y c pueden representar la observación de espín hacia arriba, medido en tres direcciones distintas, en cuyo caso $\neg a,\neg b$, y $\neg c$ representan las correspondientes mediciones de espín hacia abajo.

Sorprendentemente, parejas de partículas con enredamiento cuántico pueden violar la desigualdad de Bell (ecuación 1). Esto implica que al menos alguna de las siguientes afirmaciones es falsa: 1. la naturaleza está constreñida por la *localidad*, y 2. existen *elementos de realidad* en la naturaleza. Notemos que una forma de intentar salvar las nociones de realismo y localidad, ante la aparición de la "acción a distancia" aparente en sistemas cuánticos enredados, es suponer la existencia de *variables ocultas*. En el contexto del experimento pensado de Bohm, podríamos suponer que estas variables ocultas caracterizan tanto a la partícula de Alicia como a la de Beto, y determinan el resultado de una medición conjunta sobre ambas partículas. Bajo esta línea de argumentación, la mecánica cuántica representa entonces una teoría incompleta, implicando la

existencia de una teoría más fundamental, donde las aparentes correlaciones no-locales son descritas por variables ocultas aún no reconocidas. La importancia de la demostración experimental de la violación de las desigualdades de Bell es que refuta este argumento manteniendo, por ahora, a la mecánica cuántica como descripción correcta de la naturaleza.

Experimentalmente, resulta más práctico el uso de parejas de fotones enredados en polarización, en lugar de parejas de partículas con enredamiento en espines, y resulta más conveniente utilizar ciertas variantes de la desigualdad de Bell presentada en la ecuación 1, como por ejemplo la desigualdad de Clauser, Horne, Shimony, Holt (CHSH) [4]. Esta variante, en contraste a la ecuación 1, puede ser probada experimentalmente aun con detectores no ideales (caracterizados por una eficiencia de detección menor a la unidad), recurriendo al supuesto de muestreo fiel; esto es, suponer que el subconjunto de fotones detectados forma una muestra representativa del total.

A continuación describimos un experimento realizado por Erick Barrios, Víctor Velázquez, Enrique López-Moreno y Marcela Grether en la Facultad de Ciencias de la UNAM, que demuestra la violación de la desigualdad de Bell (en su variante de CHSH), utilizando parejas de fotones emitidos por conversión paramétrica descendente.

Experimento

La parte central del experimento aquí descrito consiste en la producción de parejas de fotones emitidos de forma esencialmente simultánea. Al utilizar parejas de fotones con enredamiento en su estado de polarización, podemos conocer el valor de dicha propiedad en uno de los fotones de la pareja tras una medición en su contraparte; esto representa una manifestación de no-localidad. Elegimos utilizar el enredamiento en polarización como la propiedad a medir, dada la disponibilidad de elementos ópticos que permiten la manipulación del estado de polarización de la luz (en contraste, la manipulación de otros grados de libertad como el espectral, es decir, el color de la luz, es menos accesible). Entre los primeros estudios experimentales en esta dirección tenemos el trabajo de Alain Aspect y colaboradores en 1982 [3], quienes idearon una forma de obtener fotones correlacionados en el tiempo utilizando la excitación de átomos de calcio, los cuales vuelven a su estado base emitiendo dos fotones de manera aproximadamente simultánea. Sin embargo, hoy en día resulta más sencillo generar parejas enredadas de fotones, aprovechando las propiedades ópticas no-lineales de cristales no-centrosimétricos (es decir, cristales que presentan cierta asimetría en las celdas fundamentales de su red cristalina). Los fenómenos ópticos no-lineales se presentan cuando la respuesta del material –dada por el momento dipolar por unidad de volumen, también conocido como la polarización del material– a un haz de luz incidente deja de ser directamente proporcional a la amplitud del campo eléctrico que compone el haz. Notemos que fenómenos ópticos típicos como reflexión, refracción y difracción están asociados a la óptica lineal, mientras que aquéllos en donde se observa la conversión entre distintos colores (frecuencias ópticas) están asociados a la óptica no-lineal. Algunos ejemplos de procesos no-lineales son la generación de suma de frecuencias y la amplificación paramétrica.

En nuestro trabajo experimental se explota la *conversión paramétrica descendente*, que representa un proceso no-lineal que puede ocurrir en materiales no-lineales de segundo orden (aquéllos en donde la componente no-lineal de la polarización es proporcional al cuadrado del campo eléctrico de la luz incidente). En este proceso, un fotón de un haz de bombeo intenso ocasionalmente decae en una pareja de fotones, comúnmente llamados *señal* y *acompañante* (figura1). Este proceso cumple con la conservación de energía (la suma de las energías de los fotones generados es la energía de un fotón de bombeo) y con la conservación de momento, también conocida en este contexto como empatamiento de fases. En nuestro caso se utilizaron cristales de beta-borato de bario (BBO), bombeados por un haz ultravioleta con longitud de onda de 405nm (1nm=10^{-9}m), generando parejas de fotones centrados en 810nm. En común con la mayoría de los cristales no-lineales de segundo orden, el BBO es ópticamente anisotrópico, es decir que presenta una birrefringencia donde las polarizaciones horizontal y vertical experimentan respuestas ópticas distintas (caracterizadas, por ejemplo, por el índice de refracción). La dirección de propagación de una onda en el cristal, en la que las dos polarizaciones experimentan la misma respuesta, se llama *eje óptico*.

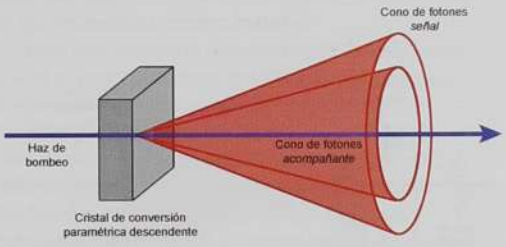

Figura 1. Conversión descendente del tipo I. Los fotones del rayo de bombeo son convertidos en fotones señal y acompañante que emergen del cristal a lo largo de diferentes direcciones. Los fotones emergentes tienen polarización idéntica opuesta a la de bombeo. Las posibles direcciones en que pueden emerger forman conos concéntricos.

En la mecánica cuántica, el estado en que se encuentra una partícula puede ser descrito por la llamada *función de onda* de la partícula, la cual

contiene la información de cuán probable es encontrarla en cada configuración experimental posible. En el caso donde tenemos un grupo de partículas (en nuestro caso, un par), el *estado conjunto* de las partículas también se puede expresar a través de una función de onda. Cuando existe más de un estado en el que el conjunto de partículas puede estar, su función de onda será una superposición de todos los estados o amplitudes cuánticas posibles. Si, además, esta superposición de las amplitudes cuánticas es tal que no se puede factorizar como contribuciones independientes para cada fotón, entonces decimos que el estado total no exhibe enredamiento cuántico. En este experimento, si el haz de bombeo tiene polarización horizontal, cada fotón generado tendrá polarización vertical. De modo similar, si el bombeo tiene polarización vertical y giramos el cristal por 90°, fotones generados tendrán polarización horizontal. Si colocamos un arreglo con un par de cristales dispuestos en serie, cuyos ejes ópticos son perpendiculares ente sí y el bombeo está polarizado a 45° [5], el estado total será la superposición de la contribución de cada uno de los cristales. Los caminos ópticos de las parejas de fotones generados forman conos, uno para cada cristal, centrados sobre el eje del haz de bombeo (figura 2). Si los cristales son suficientemente delgados, los conos se traslapan espacialmente y, al colectar los fotones utilizando un par de aperturas dispuestas en sitios diametralmente opuestos sobre los conos, seleccionamos parejas de fotones con estado de polarización enredado. Para eliminar la diferencia de fases entre los dos conos, producto de la propagación del haz de bombeo de un cristal al otro, se puede utilizar un dispositivo llamado compensador de Babinet. El estado generado es uno de los llamados estados de Bell que, en este caso, muestra enredamiento de polarización y que puede usarse en experimentos de no-localidad y violación de desigualdades de Bell [4].

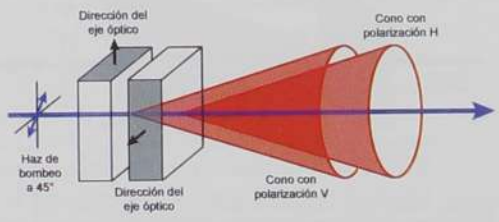

Figura 2. Arreglo geométrico de una fuente de fotones enredados por conversión descendente con dos cristales.

La longitud de onda de los fotones señal y acompañante generados en el experimento está en la región correspondiente al infrarrojo cercano (810nm), cerca del límite superior de la región visible del espectro electromagnético. La luz generada, compuesta por parejas de fotones, es muy tenue: en un caso típico, alrededor de uno de cada diez mil millones (10^{10}) de fotones de bombeo es aniquilado para producir una pareja de fotones. Para la detección de los fotones generados se utilizan *fotodiodos* de avalancha hechos de silicio, los cuales son capaces de detectar fotones individuales (en un intervalo espectral aproximado de 400nm a 900nm) con una eficiencia máxima cercana a 80%. La configuración de detección utilizada en este experimento es la de Dehlinger y Mitchell [5] y se muestra en la figura 3. En esta configuración se utiliza un par de rieles acoplados con un pivote colocado justo bajo los cristales no-lineales, describiendo una apertura angular entre los rieles, coincidente con la apertura de los conos de emisión de las parejas de fotones. Al otro extremo de cada riel se encuentra el sistema de detección y acoplamiento a fibras ópticas multi-modo (ver figura 4).

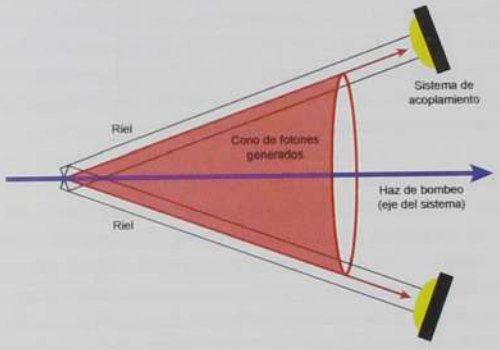

Figura 3. Colocación de los rieles.

Los fotones señal y acompañante de una pareja dada son acoplados a fibras ópticas enfocando los haces correspondientes al núcleo de la fibra mediante lentes que tienen un tratamiento anti-reflejante que las hace adecuadas para permitir máxima transmisión en la región del infrarrojo cercano; con esto se reducen perdidas ópticas de las parejas de fotones. Las fibras ópticas se encuentran conectadas a los puertos de entrada de los fotodiodos de avalancha mediante conectores tipo FC. Las señales electrónicas, producto de la detección de fotones individuales, son monitoreadas para determinar la tasa de coincidencias [6], es decir, el número de eventos de detección coincidente de los fotones señal y acompañante en un cierto intervalo de tiempo. Para ello, se compara el instante de arribo de las señales electrónicas provenientes de cada detector; si las dos señales se presentan dentro de una ventana de 25ns, las consideramos como coincidentes.

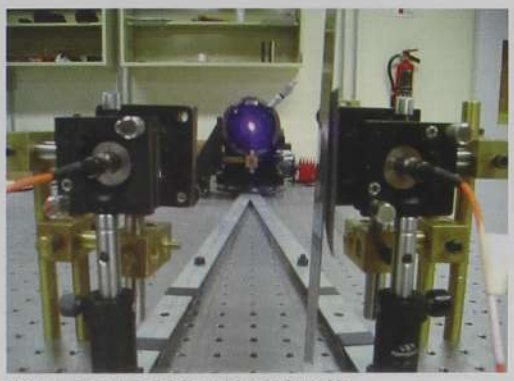

Figura 4. Fotografía del dispositivo de detección.

Al incluir un dispositivo capaz de modificar la polarización de los fotones señal y acompañante antes de ser detectados (una lámina de media onda), junto con un analizador o un polarizador (que permite el paso únicamente de fotones con una cierta polarización lineal), podemos estudiar correlaciones de polarización en cada pareja de fotones. En un experimento típico se fija la polarización del fotón acompañante a 45° y se hace rotar la polarización del fotón señal, obteniendo una tasa de detección que muestra una dependencia senoidal en función del ángulo de polarización del fotón señal. La aparición de una curva de interferencia senoidal con visibilidad óptima es compatible con un estado maximamente enredado. Una reducción de la visibilidad indica alguna imperfección experimental que reduce la calidad del enredamiento cuántico.

Supongamos que configuramos las láminas de media onda de modo tal que el ángulo de polarización del fotón señal es α y el ángulo de polarización del fotón acompañante es β. Si denotamos por $E(\alpha,\beta)$ a un parámetro de correlación en la pareja de fotones en las nuevas direcciones de polarización, podemos definir la siguiente cantidad:

$$S = E(\alpha,\beta) - E(\alpha,\beta') + E(\alpha',\beta) - E(\alpha',\beta'),$$

a la que llamaremos parámetro de Bell y en donde hemos usado tanto los ángulos α y β como sus versiones rotadas: $\alpha' = \alpha + 90°$ y $\beta' = \beta + 90°$. Cada una de las cantidades $E(\alpha,\beta)$ está a su vez dada por

$$E(\alpha,\beta) = P_{VV}(\alpha,\beta) + P_{HH}(\alpha,\beta) - P_{VH}(\alpha,\beta) - P_{HV}(\alpha,\beta),$$

donde cada término $P(\alpha,\beta)$ denota la probabilidad de detección simultánea del par de fotones dado su ángulo respectivo de polarización α y β; el subíndice *VV*, *HH*, *VH* o *HV* representa las distintas posibles combinaciones de estados de polarización original antes de ser modificados a los valores α y β. De este modo, para obtener experimentalmente un valor del parámetro de Bell *S*, debemos realizar 16 mediciones de probabilidades de detección conjunta de fotones o tasas de coincidencia. Se puede probar que la desigualdad de Bell en la forma CHSH es equivalente a $-2 \leq S \leq 2$. En este experimento se obtuvo $S = 2.664 \pm 0.052$, lo cual implica una clara violación a la desigualdad de Bell, en más de 12 desviaciones estándar.

Enredamiento en variables continuas

Hasta ahora hemos considerado el enredamiento cuántico en la polarización, la cual es una variable discreta debido a que puede tomar sólo dos valores distintos; para cada fotón emitido, podemos describir el estado de polarización con base en dos elementos; por ejemplo, polarización vertical y horizontal o polarización circular derecha e izquierda. No obstante, de manera más general, un fotón se encuentra determinado, además de por su polarización, por su color (frecuencia óptica) y por su dirección de propagación. Estas son variables continuas, en el sentido de que requerimos de un continuo de valores para poder describirlas. Podemos, entonces, esperar que el estado de dos fotones que se produce por conversión paramétrica descendente pueda contener una componente de variable continua, además de la componente de variable discreta asociada con la polarización. De hecho, los principios de conservación de energía y de momento, que, por supuesto, el proceso de conversión paramétrica descendente satisface, se traducen en una estructura complicada de enredamiento cuántico de variable continua.

Como hemos visto, para producir parejas de fotones con enredamiento en polarización, debemos implementar diseños experimentales muy específicos. Sin embargo, el enredamiento de variable continua aparece de manera natural en la mayoría de las geometrías experimentales.

Para una categoría importante de aplicaciones, que es el procesamiento de información cuántica, la aparición de enredamiento cuántico en variables continuas es un fenómeno indeseable, pues representa una limitante. Por ejemplo, se ha demostrado que la detección de uno de los dos fotones emitidos de una pareja de fotones enredada, proyecta a su acompañante a un estado cuánticamente impuro, lo cual significa, en términos prácticos, que no es posible hacerlo interferir con otros fotones individuales [7], y he aquí un problema: este tipo de interferencia de dos fotones individuales, que provienen de fuentes distintas, representa el corazón de la propuesta de Knill, LaFlamme y Milburn para llevar a cabo operaciones de computación cuántica usando fotones. Una discusión detallada de este tópico puede encontrarse en [8].

Es posible filtrar la emisión de la luz compuesta por las parejas de fotones, de manera que nos aproximemos a la emisión de una sola frecuencia y una sola dirección de propagación para cada fotón, y con esto lograr la supresión de enredamiento cuántico de variable continua. Sin embargo, como ya hemos mencionado, la conversión descendente paramétrica en el régimen espontáneo es un proceso ineficiente, en el que típicamente sólo un fotón de cada 10^{10} fotones del haz de bombeo es transformado por el cristal. Así, mientras que la filtración permite la supresión de enredamiento, el costo es una reducción prohibitiva de la ya limitada tasa de emisión. Esta es la principal motivación para encontrar distintas formas de controlar el enredamiento de variable continua de una fuente de parejas de fotones, sin recurrir a la filtración. Esto podría resultar en fuentes brillantes (que emiten un número relativamente elevado de parejas de fotones por segundo), optimizadas para aplicaciones de procesamiento de información cuántica.

Por otro lado, existen propuestas de aplicaciones que requieren fuentes de parejas de fotones con características particulares de enredamiento cuántico continuo. Por ejemplo, en una propuesta reciente se explotan estados fotónicos que exhiben enredamiento de frecuencia para un protocolo de posicionamiento cuántico [9]. Este protocolo está diseñado para determinar la posición de un objeto con una alta precisión, mayor de la que podría alcanzarse utilizando partículas descritas por la mecánica clásica. En particular, mientras que usando la mecánica clásica el error en la determinación de la posición de un objeto decrece idealmente como $1/\sqrt{N}$, donde N es el número de partículas, en el caso de estados fotónicos este factor de escalamiento puede alcanzar el valor $1/N$. Por lo tanto es posible alcanzar una mayor precisión en el caso cuántico en comparación con el caso clásico, para el mismo número de partículas. En el estado cuántico requerido para este tipo de posicionamiento se emiten N fotones, de modo que mientras que cada uno puede tener un rango amplio de posibles frecuencias ópticas, si se llega a determinar la frecuencia de uno solo de ellos, automáticamente y de manera no-local se determina la frecuencia de todos los demás fotones, pues ésta es idéntica a la del fotón medido [9].

Tanto para lograr la emisión de parejas de fotones útiles para la computación cuántica como en la producción de parejas de fotones útiles para esquemas tales como el posicionamiento cuántico (en el caso más sencillo con $N = 2$) necesitamos técnicas que permitan diseñar el estado de dos fotones.

En un trabajo previo hemos mostrado que las posibilidades de diseño de generación de parejas de fotones pueden incrementarse drásticamente si utilizamos un haz de bombeo en la forma de un tren de pulsos ultra cortos (en donde cada pulso puede tener una duración del orden de 10 femtoseg $=10\times10^{-15}$ seg), en lugar de un haz no-pulsado o de onda continua. Además, hemos probado que dentro del cristal no-lineal, las velocidades relativas de propagación de los pulsos de bombeo y de los fotones generados señal y acompañante determinan a un primer nivel de aproximación las propiedades de enredamiento de variable continua. Así, por ejemplo, en [10] demostramos que si se cumple la relación $2/v_p = 1/v_s + 1/v_i$, donde v_p, v_s, v_i son las velocidades de propagación del pulso de bombeo, del fotón señal y del fotón acompañante respectivamente, entonces es posible sintetizar estados de dos fotones libres de enredamiento en frecuencia sin recurrir a filtración. Los estados de dos fotones con estas características, como ya hemos mencionado, son de utilidad para aplicaciones de procesamiento de información cuántica. Usando la misma condición $2/v_p = 1/v_s + 1/v_i$ entre las velocidades, pero con una elección diferente de longitud de cristal y duración temporal de los pulsos de bombeo, se pueden generar parejas de fotones con correlación positiva, del tipo que se requiere para esquemas de metrología cuántica, como el de posicionamiento cuántico.

En la figura 5(a) se presenta una gráfica de la distribución de probabilidad conjunta para un caso típico de conversión paramétrica descendente, correspondiente a la emisión de una pareja de fotones, caracterizada por valores determinados de las frecuencias de emisión. En términos físicos, podemos interpretar las zonas rojas como aquéllas que contienen las parejas de valores de frecuencias de emisión más probables. En particular, es importante notar que el estado descrito por esta distribución de probabilidad exhibe marcadas correlaciones no-locales entre el fotón señal y el fotón acompañante. Esto significa que, por ejemplo, al llevar a cabo una medición de la frecuencia de uno de los dos fotones, la frecuencia de su contraparte se encuentra bien determinada, dentro de un intervalo de tolerancia (donde el inverso de esta tolerancia representa una medida del enredamiento cuántico presente), aun sin llevar a cabo una medición sobre el segundo fotón. En la figura 5(b) se muestra una gráfica de la distribución de probabilidad espectral asociada con un estado libre de enredamiento espectral, útil para aplicaciones de procesamiento de información cuántica. En ese caso, la medición de un fotón no arroja información alguna sobre su contraparte. Finalmente, en la figura 5(c) se presenta una gráfica de la distribución de probabilidad espectral asociada con un estado con correlación positiva, útil para el posicionamiento cuántico. Notemos que, en este último caso, mientras que cada fotón contiene un intervalo amplio de frecuencias, al hacer una medición simultánea sobre ambos fotones, ésta arrojaría frecuencias esencialmente

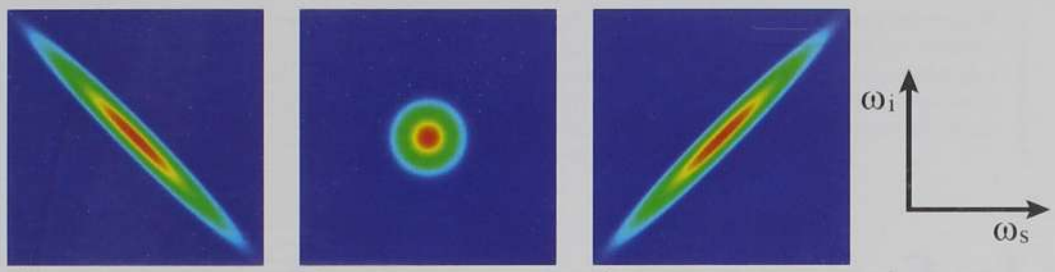

Figura 5. Gráfica de la distribución de probabilidad espectral conjunta para el fotón señal de frecuencia ωs y el fotón acompañante de frecuencia ωi, producidos por conversión paramétrica descendente. a) caso típico, b) estado sin enredamiento espectral, y c) estado con correlación positiva.

coincidentes, dentro de una cierta tolerancia, donde nuevamente el inverso de esta tolerancia representa una medida de enredamiento cuántico.

Finalmente algunas conclusiones. En el transcurso del último siglo, la validez de la mecánica cuántica ha sido objeto de escrutinio y cuestionamiento. Una de las pruebas más tenaces a las que esta teoría ha sido sometida es el planteamiento de Einstein, Podolsky y Rosen, quienes, tomando como base la suposición que los principios de realismo y localidad son válidos, argumentaron que la mecánica cuántica es una teoría incompleta. Ellos afirmaron que los fenómenos de acción a distancia asociados con el enredamiento cuántico debían ser explicados por variables ocultas compatibles con la localidad y el realismo –las cuales aún no se encuentran determinadas– y que formarán parte de una teoría más fundamental que la mecánica cuántica. El cuestionamiento de estos científicos llevó, eventualmente, al llamado teorema de Bell, el cual presenta una desigualdad que debe satisfacer cualquier sistema físico que se rige por los principios de realismo y de localidad. La demostración experimental de que sistemas con enredamiento cuántico pueden violar la desigualdad de Bell es de enorme importancia en la historia reciente de la ciencia, ya que puede considerarse como una refutación de las teorías de variables ocultas, sostenedoras de los principios de realismo y de localidad. Aunque en sentido estricto aún quedan lagunas –*loop-holes*– que podrían poner en duda tal refutación (por ejemplo, el supuesto de muestreo fiel), la interpretación estándar actual concluye que la evidencia experimental indica de manera abrumadora la validez de la mecánica cuántica como descripción correcta de la naturaleza a muy pequeña escala. En retrospectiva, resulta curiosa la argumentación de Einstein, Podolosky y Rosen, pues podríamos considerar que trataron de forzar la entrada de ciertos principios de operación sobre la naturaleza.

En este trabajo hemos presentado una descripción tanto del argumento de EPR como de las desigualdades de Bell. Hemos presentado resultados experimentales utilizando parejas de fotones emitidas por el proceso de conversión paramétrica descendente, donde demostramos claramente la violación de una desigualdad de Bell. Dado que los fotones cuentan con grados de libertad continuos (*e. g.* frecuencia óptica), además de los discretos (*e. g.* polarización), el enredamiento puede presentarse en ambos tipos de variables. Aunque las variables continuas son, en términos generales, menos accesibles a manipulación experimental, presentan nuevos retos y oportunidades en el estudio de la no-localidad. En esa dirección, este trabajo presenta, además, un panorama introductorio al enredamiento fotónico de variable continua, buscando ofrecer una perspectiva más amplia de las maravillas y misterios que encierra el universo cuántico que nos conforma. ●

[Referencias]

[1] A. Einstein, B. Podolsky y N. Rosen, Can Quantum-Mechanicald Description of Physical Reality Be Considered Complete? Phys. Rev. 47, 777-780 (1935).
[2] J.S. Bell, On the paradox Einstein-Podolky-Rosen, Physics 1 (Long Island City, N.Y), pp. 195-200, 1964; Speakable and Unspeakable in Quantum Mechanics: Collected Papers in Quantum Philosophy, Cambridge, UP. Cambridge (1993).
[3] A. Aspect y P. Grangier, Experiment on Einstein-Podolsky-Rosen correlations with pairs of visible photons. Editado por R. Penros and C.J. Isham, Quantum Concept in Space and Time, Oxford UP, 1986, pp 1-44.
[4] J.F. Clauser, M.A. Horne, A. Shimony y R.A. Holt, Proposed experiment to test local hidden-variable theories, Phys Rev. Lett. 23 (15), 880-884 (1969).
[5] P.G. Kwiat, E. Waks, A.G. White, I. Applebaum y P.H. Everhard, Ultrabright source of polarization entangled photons, Phys. Rev. A 60 (2), R773-R776 (1999).
[6] D. Dehlinger y M.W. Mitchell, Entangled Photons, nonlocality, Bell Inequalities in the undergraduated laboratory, Am. J. Phys. 79 (9), 903-910 (2002).
[7] A.B. U'Ren, Ch. Silberhorn, R. Erdmann, K. Banaszek, W.P. Grice, I.A. Walmsley y M.G. Raymer, Generation of pure single photon wavepackets by conditional preparation based on spontaneous parametric downconversion, Laser Physics 15, 146 (2005).
[8] P. Kok, W.J. Munro, K. Nemoto, T.C. Ralph, J.P. Dowling y G.J. Milburn, Linear optical quantum computing with photonic qubits, Rev. Mod. Phys. 79, 135 (2007).
[9] V. Giovannetti, S. Lloyd y L. Maccone, Quantum-enhanced positioning and clock synchronization, Nature 412, 417-419 (2001).
[10] W.P. Grice, A.B. U'Ren and I.A. Walmsley, Eliminating frequency and space-time correlations in multiphoton states, Phys. Rev. A 64, 063815 (2001).
[11] D. Bohm, A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables (I y II), Phys. Rev. 85, 166-179 (1952).

Información cuántica: ideas y perspectivas

LA INFORMACIÓN CUÁNTICA ES UNA NUEVA CIENCIA QUE SURGIÓ EN AÑOS RECIENTES DE LA REVISIÓN DE LOS CONCEPTOS ESENCIALES DE LA FÍSICA CUÁNTICA. AHORA, EL OBJETIVO ES ENTENDER CÓMO SE PUEDEN USAR LAS LEYES FUNDAMENTALES DE LA FÍSICA CUÁNTICA PARA MEJORAR LA TRANSMISIÓN Y EL PROCESAMIENTO DE INFORMACIÓN, LO CUAL PROMETE UN GRAN NÚMERO DE NUEVAS Y FASCINANTES TECNOLOGÍAS EN EL FUTURO.

Andrei B. Klimov

Gracias a los importantes avances de la física cuántica en los últimos 70 años se ha logrado describir la estructura del micromundo con una gran precisión. Sin embargo, aparte del sofisticado aparato matemático que nos permite determinar los estados energéticos de las micropartículas y su evolución temporal, existe una parte conceptual trascendental, que por muchos años no se había discutido en los amplios círculos de los físicos, ocupados de realizar cálculos "prácticos". A pesar de que los conceptos esenciales de la mecánica cuántica fueron discutidos con gran profundidad en un artículo de E. Schrödinger en el año 1935, estimulado por la famosa discusión entre N. Bohr, por un lado, y A. Einstein, B. Podolsky y N. Rosen, por el otro, la atención de la comunidad física comenzó a enfocarse en los aspectos fundamentales (o como los llaman a veces, "la parte filosófica") apenas en los últimos 15 años, cuando de la reconsideración de los mismos surgió una nueva ciencia: información cuántica.

En su destacado artículo, E. Schrödinger analizó el punto más esencial de la física cuántica: el proceso de medición y sus implicaciones en la relación entre los micro y macromundos, además fue en este trabajo donde por primera vez surgió el concepto de los estados enredados o entrelazados (*entangled states*), que es el punto medular de toda la información cuántica.

Para poder desenvolvernos libremente en este artículo enlistaremos brevemente los conceptos más importantes de la mecánica cuántica. Comencemos con la propiedad fundamental de todo sistema cuántico: su carácter probabilístico. Podemos describir un sistema cuántico sólo en forma estadística y esta propiedad no tiene nada que ver con el desconocimiento de alguna propiedad del sistema (como en la física estadística clásica), sino que, *de primeros principios*, no se puede disponer de la información completa.

Para describir sistemas cuánticos se utiliza el concepto de estado cuántico (que en la práctica se expresa en términos de una función de onda o de la llamada matriz de densidad en el caso de sistemas cuánticos mezclados), que contiene toda

ANDREI B. KLIMOV Profesor del Departamento de Física en la Universidad de Guadalajara. Miembro del Sistema Nacional de Investigadores (nivel III). Sus áreas de interés son la óptica cuántica y los sistemas cuánticos discretos. klimov@cencar.udg.mx

> Una propiedad esencial de los sistemas cuánticos consiste en que, como resultado de una medición, el estado inicial del sistema cuántico se destruye y el sistema colapsa a un nuevo estado, que se determina según el resultado de tal medición. Esto implica la imposibilidad de predecir con certeza el comportamiento de un sistema cuántico ante alguna operación arbitraria.

la información sobre resultados de las posibles mediciones efectuadas sobre el sistema. El concepto de estado para sistemas cuánticos es esencialmente distinto que el mismo para sistemas clásicos: determinar el *estado* de un sistema clásico consiste en especificar el conjunto de parámetros a partir de los cuales todas las propiedades del sistema puedan reconstruirse (momento, posición, etcétera); en tanto que la determinación del *estado* de un sistema cuántico implica el conocimiento de los posibles resultados de las mediciones de los observables asociados al sistema y las probabilidades de obtener tales valores, es decir, se requiere de una lista de operaciones que el observador puede hacer sobre el sistema y los resultados que puede obtener con las probabilidades correspondientes.

Una propiedad esencial de los sistemas cuánticos consiste en que, como resultado de una medición, el estado inicial del sistema cuántico se destruye y el sistema colapsa a un nuevo estado, que se determina según el resultado de tal medición. Esto también implica la imposibilidad de predecir con certeza el comportamiento de un sistema cuántico ante alguna operación arbitraria. Debido a que cualquier tipo de interacción entre un sistema clásico y uno cuántico se puede considerar como una medición (observación), es relevante mencionar que las propiedades cuánticas de los objetos del micromundo son extremadamente frágiles.

Otra propiedad fundamental de los sistemas cuánticos es su linealidad: es decir, si dos funciones de onda representan cada una un estado cuántico, la superposición lineal de éstas también describe un posible estado del mismo sistema. Esto implica, en particular, que un sistema cuántico se puede encontrar no sólo en los estados definidos por ciertos valores particulares de algún observable (por ejemplo, los estados de un electrón con espín "arriba" ($\uparrow$) y espín "abajo" ($\downarrow$), sino en una superposición de tales estados ($\psi = a\uparrow + b\downarrow$), donde a y b son números complejos tales que $|a|^2 + |b|^2 = 1$. Notemos que el número de estados posibles, por lo tanto, ¡es infinito! Recordemos que una medición de espín, por ejemplo "arriba", implicaría una reducción instantánea $\psi \Rightarrow \uparrow$. Sin embargo, en cada experimento particular no existe ninguna posibilidad de predecir cuál será el resultado de la medición cuando $a, b \neq 0$. Aunque por supuesto, si, $\psi = \uparrow$, el único resultado que se obtendría sería espín "arriba".

Es aquí donde aparece la famosa paradoja del gato de Schrödinger: en una caja, donde está encerrado un gato, hay un frasquito con veneno que se rompe por un mecanismo que se activa con el decaimiento de un átomo radiactivo. Debido a que el átomo se encuentra en una superposición de estados decaído y no decaído, el gato está en una superposición de gato vivo y gato muerto.

Los estados correspondientes $\uparrow$ y $\downarrow$ son ortogonales en el sentido de álgebra lineal, propiedad que es equivalente a la perpendicularidad geométrica, y forman lo que se llama una base en el espacio de todos los posibles estados de espín, es decir, cualquier estado es una superposición lineal de esos estados. Es notable que se puedan distinguir (se entiende que con seguridad) solamente los estados ortogonales entre sí. Es decir, todo el continuo de estados entre $\uparrow$ y $\downarrow$ (que son combinaciones lineales de dos estados ortogonales) son indistinguibles.

La linealidad de la mecánica cuántica también se refleja en el tipo de transformaciones que se pueden realizar sobre los estados cuánticos: sea U una transformación admisible (la que preserva la probabilidad total) y ψ_1, ψ_2 dos estados de un sistema cuántico, entonces $U(\psi_1 + \psi_2) = U\psi_1 + U\psi_2$.

Una consecuencia de la linealidad consiste en la imposibilidad de "clonar" un objeto cuántico aislado. Bajo la palabra "clonar" se entiende la obtención de una copia exacta de un objeto *desconocido* sin destruir su estado original. Este enunciado se conoce como el Teorema de no clonación (Wootters, Zurek, 1982) y juega un papel importante en la teoría de la información cuántica.

El papel crucial de las superposiciones de estados cuánticos se resalta en el caso de los llamados estados entrelazados.

Para guardar cada bit de información se utilizan objetos macroscópicos: granitos magnéticos de los discos duros de las computadoras. Un granito tiene aproximadamente cien mil millones de átomos y el reto consiste en utilizar cada vez un número menor de átomos para estos propósitos, así que en el límite podríamos llegar a usar objetos microscópicos como células elementales para almacenar la información.

Estados entrelazados

Comencemos con un ejemplo sencillo: consideremos dos sistemas cuánticos elementales, que pueden ser dos partículas idénticas con espín, como las consideradas en la sección anterior. Notemos que para este tipo de partículas los únicos resultados posibles de alguna medición, en un sistema de referencia fijo, consisten sólo en la detección de partículas con espín arriba o espín abajo.

Ahora, los estados posibles del sistema compuesto son $\uparrow\uparrow, \downarrow\downarrow, \uparrow\downarrow, \downarrow\uparrow$, donde la flecha de la izquierda representa el estado de la primera partícula y la de la derecha, el de la segunda. Podemos ver que los estados de tipo $\psi = a\uparrow\uparrow + b\downarrow\downarrow$ poseen una propiedad muy especial: si una medición sobre la primera partícula arroja, por ejemplo, el resultado espín arriba, la función de onda del sistema completo se reduce a $\psi \Rightarrow \uparrow\uparrow$, lo que implica que el resultado de una medición, ahora sobre la segunda partícula, será con certeza espín arriba, sin importar qué tan separadas espacialmente estén las partículas. Justamente esta cualidad singular fue discutida por Einstein, Podolsky y Rosen como un argumento en contra de la interpretación de la mecánica cuántica por la escuela de Copenhague, y luego retomada en el famoso trabajo de J. Bell (1964).

En general, dos sistemas se encuentran en un estado entrelazado puro (también existen estados mezclados, que no consideraremos en este artículo) si la función de onda de todo el sistema no se puede escribir como producto de las funciones de onda, correspondientes a cada uno de los sistemas: $\psi_{12} \neq \psi_1 \psi_2$.

Además, los estados entrelazados muestran otra propiedad meramente cuántica: el conocimiento completo del estado total del sistema no implica el mismo conocimiento sobre cada una de sus partes, es decir, es imposible considerar (y describir matemáticamente) la condición de cada partícula en forma independiente de la otra. Es posible probar que cualquier intento de "aislar" uno de los subsistemas disminuye drásticamente la información sobre éste y, en casos extremos, la reduce a cero.

Tales estados entrelazados se generan con relativa facilidad en los llamados fotones gemelos: cuando un fotón inicial de frecuencia 2ω se desdobla en dos fotones de frecuencias ω en un proceso no lineal, debido a la conservación del momento lineal estos fotones están entrelazados en sus estados de polarización.

En realidad, el entrelazamiento es un recurso físico que puede ser cuantificado, medido y transformado (al igual que la energía, por ejemplo), asociado a una peculiar correlación, que no existe clásicamente, entre dos sistemas separados. El entrelazamiento entre dos subsistemas genera un canal cuántico que se puede usar para transmitir información de una forma que es imposible con sistemas clásicos. Un ejemplo importante de la transmisión cuántica de información es la llamada teleportación cuántica.

Teleportación cuántica

La idea de la teleportación cuántica fue propuesta teóricamente en 1993 por C. Bennett *et al*. Básicamente consiste en la transmisión de información entre dos objetos a distancia: la información (que está codificada en un sistema cuántico) se destruye en el punto A (Alice) y aparece (se reconstruye el estado original) en el punto B (Bob). Clásicamente entendida, la teleportación implica un estudio exhaustivo del objeto y luego la transmisión de sus características a otro punto con la consiguiente reconstrucción del objeto inicial. Sin embargo, como ya lo habíamos visto, cualquier estudio de un objeto cuántico destruye su estado, por lo que tal procedimiento es inútil si queremos saber cuál es el estado del sistema y después enviar el resultado a otro punto. Así, el problema consiste en la transmisión de información de un estado *desconocido*.

La idea de la teleportación consiste en lo siguiente: Alice tiene una partícula, por ejemplo, un fotón, en un estado de polarización desconocido ψ. Además, Alice y Bob comparten un estado entrelazado Ψ_{12}, por ejemplo, fotones en estados de polarización enredados, de tal forma que uno de los fotones entrelazados lo tiene Alice y el otro lo tiene

Bob. Alice puede realizar mediciones sobre el sistema de dos fotones que ella posee (uno enredado con Bob y otro en un estado desconocido) y dependiendo de los resultados obtenidos (¡desconocidos *a priori*!), el fotón que tiene Bob se proyectará a un estado ϕ, que Bob tampoco conoce. Sin embargo, habiendo obtenido los resultados de la medición, Alice comunica a Bob por un canal clásico (le llama por teléfono) qué transformación tiene que hacer sobre su fotón para reconstruir el estado desconocido ψ que originalmente tenía Alice. Es importante aclarar que Alice se da cuenta del suceso de teleportación ya en el momento de medición, mientras que Bob no lo sabe hasta recibir la llamada de Alice, aunque ninguno de los dos conoce el estado.

En este procedimiento extraordinario, Alice y Bob logran usar un estado entrelazado como un canal de comunicación cuántico destruyendo el estado ψ del fotón que tenía Alice para recrear el mismo estado ψ (de otro fotón) y que ahora tiene Bob. Notemos que el procedimiento de teleportación no viola el Teorema de no clonación, ya que el estado ψ que tenía Alice se destruye, ni las leyes de la relatividad. Obviamente, el estado enredado es una pieza clave en este protocolo, que, además, permite la transferencia de información a distancias arbitrarias.

Por primera vez el efecto de teleportación fue probado experimentalmente por el equipo de A. Zeilinger en 1997, cuando utilizaron fotones gemelos entrelazados en polarización. Es interesante notar que el canal cuántico permite transferir de manera sencilla una cantidad en principio *infinita* de información clásica, debido a que el estado ψ podría ser una superposición de estados con coeficientes transcendentes (que para ser definidos en sistema binario requieren una secuencia infinita de ceros y unos), lo que nos lleva directamente al concepto de información cuántica y su relación con la información clásica.

Información cuántica

¿Cómo entendemos la *información*? La información para nosotros implica en realidad la distinguibilidad, es decir, qué tanto podemos separar el objeto que nos interesa, sea físico o matemático, de su medio ambiente.

En su forma rigurosa, el concepto de información fue definido por C. Shannon en 1949 y se representa en términos de la cantidad que desde entonces se llama *entropía de Shannon*. Supongamos que nos interesa una variable aleatoria binaria (sólo puede tomar dos valores: 0 y 1), que está definida por una distribución de probabilidad. Si ambos valores aparecen con la misma probabilidad, la entropía alcanza su valor máximo y, por lo tanto, representa la incertidumbre máxima. En este caso, la información codificada en el sistema es nula. La información máxima corresponde a la incertidumbre mínima sobre las alternativas: cuando alguna de las probabilidades es 1, la entropía de Shannon es cero.

Por otro lado, en la teoría de la información no nos interesa realmente entender el contenido de un mensaje, sino solamente cuantificar la cantidad de información contenida en él. Esto significa, en particular, que el medio físico utilizado para la transmisión no es importante. La pregunta relevante es: ¿hasta qué grado se puede comprimir el mensaje sin pérdida de información, de tal forma que la parte receptora pueda reconstruir el mensaje original unívocamente? En otras palabras, ¿se puede caracterizar la información por la cantidad de comunicación necesaria para transferirla? Resulta que el número mínimo de "letras" para transmitir la información se caracteriza justamente por la entropía de Shannon. Estas "letras" comúnmente se llaman *bits*.

La información clásica posee ciertas características fundamentales: no puede viajar más rápido que la luz, puede ser borrada y copiada.

El procesamiento de información es, básicamente, la forma de revelar "verdades implícitas" y se reduce al uso de operaciones de tipo "NOT" y "CNOT". La operación (compuerta lógica) NOT es local, es decir, se aplica a un solo *bit* y es un aparato que actúa de la siguiente forma: si la entrada (*input*) es 0, la salida (*output*) es 1 y viceversa. En otras palabras, la compuerta "NOT" voltea el *bit* que entra. La compuerta

CNOT (también llamada XOR) es no local, es decir, se aplica a dos bits simultáneamente, un *bit* de control y otro *bit* de blanco, de tal forma que el *bit* de blanco sólo se voltea si el *bit* de control es 1.

Actualmente, para guardar cada *bit* de información se utilizan objetos macroscópicos: granitos magnéticos de los discos duros de las computadoras. Cada granito tiene aproximadamente cien mil millones de átomos. El reto es utilizar cada vez un menor número de átomos para estos propósitos, así que en el límite podríamos llegar a usar objetos microscópicos como células elementales para guardar la información. Al llegar a estos límites utilizaremos los estados cuánticos de algunos sistemas físicos para codificar ceros y unos. Sin embargo, ya sabemos que los sistemas cuánticos se portan de forma drásticamente distinta de los sistemas clásicos, y la información guardada y transmitida mediante estos objetos microscópicos se rige por las leyes de la mecánica cuántica. La unidad de información cuántica, es decir, la cantidad de información cuántica que se puede resguardar en el estado del sistema cuántico más pequeño (que sólo tiene dos niveles de energía), por ejemplo, una partícula de espín ½, o los estados de polarización de un fotón, se llama *qubit*. La diferencia entre *bits* y *qubits* es abismal: como ya lo habíamos visto, un sistema cuántico de dos niveles de energía puede encontrarse en un estado de superposición $\psi = a\uparrow + b\downarrow$, donde los coeficientes a y b se codifican como una secuencia infinita de ceros y unos; de esta forma un *qubit* podría llevar una cantidad arbitraria de información clásica. Manipulando los estados cuánticos podemos transformar, procesar y transmitir la información cuántica. Sin embargo, debido a la peculiaridad de la medición de un *qubit* ¡podemos acceder a solamente un *bit* de información!

El procesamiento de la información cuántica también se reduce a operaciones con uno y dos *qubits*. Es más, las mismas puertas NOT y CNOT siguen siendo las básicas para estos fines. Sin embargo, la información cuántica no se puede copiar sin perturbarla (Teorema de no clonación) y, aunque ahora tenemos a nuestra disposición un recurso tan valioso como el enredamiento, seguimos sin poder de enviar mensajes más rápido que la luz.

Como ya sabemos, los estados cuánticos y, por consiguiente, la información almacenada en ellos, son extremadamente frágiles. Sin embargo, esta propiedad aparentemente negativa se puede usar de una forma revolucionaria para proteger los mensajes enviados de la posibilidad de ser interceptados y descifrados.

Criptografía cuántica

La necesidad de mantener en secreto información importante y comunicarla en forma confidencial ha sido una constante a lo largo de la historia de la humanidad. La disciplina que nos ayuda a transmitir información en forma segura es la criptografía. Ésta permite la elaboración de algoritmos para encriptar la información transmitida entre dos partes (Alice y Bob), de tal forma que un intento de monitorear esta transmisión fallaría. La idea de criptografía clásica es muy sencilla: Alice quiere enviar un mensaje secreto a Bob: {beca}. Para ello, a cada palabra de este mensaje se le pone en correspondencia un número según una regla acordada anteriormente, por ejemplo: a=1, b=2, c=3, etc... obteniendo: {2531}. Este procedimiento no es seguro y se puede descifrar fácilmente. Ahora vamos a encriptar este mensaje. Esto se hace de la siguiente forma: Alice y Bob (¡y sólo ellos!) tienen en su poder una secuencia de números aleatorios –el código secreto: {1364...}. A cada número del mensaje (no encriptado) le vamos a sumar un número del código (por ejemplo módulo 10), obteniendo {3895}. Bob, habiendo recibido el mensaje y conociendo el código fácilmente descifra el mensaje. Tal procedimiento es absolutamente secreto (Shannon, 1949) si el código es realmente aleatorio y se utiliza sólo una vez (de no ser así, cualquier código

En el establecimiento de un código secreto se pueden usar los dos canales de comunicación: clásico y cuántico. La ventaja que tiene el uso del canal cuántico es que, ante cualquier intento de una persona no autorizada por hacerse de la clave, se registra una marca (perturbación) en la misma, lo cual permite descubrir el intento no deseado. Se trata del Teorema de no clonación.

se rompe por medio de una búsqueda exhaustiva). La dificultad práctica consiste en la transmisión de un nuevo código entre Alice y Bob cada vez que se necesita enviar un nuevo mensaje. En las películas de espías para este fin se utilizan frases de algunos libros previamente acordados, que están en poder de Alice y Bob desde el principio.

La mecánica cuántica ofrece una posibilidad verdaderamente segura para transmitir los mensajes secretos haciendo uso de canales físicos. La idea detrás es el Teorema de no clonación: no se puede ganar información cuántica sin perturbar al sistema –el canal de comunicación cuántico. Entonces, para establecer el código secreto (¡el principal problema!) Alice y Bob pueden usar los dos canales de comunicación: clásico y cuántico. Pero el uso del canal cuántico garantiza que cualquier intento de una persona no autorizada por hacerse de la clave dejaría una marca (perturbación) en la misma, permitiendo descubrir el intento. Además, el Teorema de no clonación prohíbe hacer copias de la comunicación cuántica y luego procesarla fuera de línea. Así que, incluso con un poder de cálculo ilimitado, es posible garantizar la seguridad de estos protocolos.

La criptografía cuántica es una de las áreas más avanzadas en las aplicaciones prácticas (Gisin *et al.* 1996, 1997). Actualmente existen compañías en EUA y Suiza que comercializan los primeros aparatos donde se hace uso de los protocolos de encriptación cuántica.

Finalizamos con algunas conclusiones. En el creciente campo de la información cuántica se mezclan ideas bien desarrolladas de la información clásica con las de la mecánica cuántica. Su meta es entender cómo se pueden usar las leyes fundamentales de la física cuántica para mejorar la transmisión y el procesamiento de información, lo cual promete un gran número de nuevas y fascinantes tecnologías. La información cuántica es un ejemplo tangible de la teoría cuántica: cómo funciona, qué significa, cómo se debe interpretar y cómo el mundo clásico emerge del mundo cuántico.

Los progresos en las técnicas de manipulación de sistemas cuánticos, como el enfriamiento de iones y átomos, la producción de fotones gemelos y el hecho de que se sumen nuevos laboratorios y científicos al estudio de estos fenómenos, permiten profetizar que pronto la información cuántica será otra herramienta común en nuestras vidas. Estos prometedores avances convierten a los estudios en óptica e información cuántica en temas de tanta importancia para la sociedad, que en los años 1997, 2001 y 2005 el Premio Nobel de Física ha recaído en investigadores abocados a estas áreas.

Una línea que no hemos tocado en este artículo y que está íntimamente relacionada con el campo de la información cuántica es la llamada computación cuántica, cuya idea principal es hacer uso de las propiedades singulares de los estados cuánticos para procesar la información en una forma mucho mas eficiente que la que se tiene actualmente, así como reducir el tamaño actual de los equipos de cómputo, es decir, elaborar dispositivos cada vez más pequeños y con mayor capacidad. Debido a las recientes propuestas de varios algoritmos de computación cuántica, tales como la búsqueda rápida (Deutch, 1985 y Grover 1997) y la factorización eficiente de un número grande como un producto de números primos (Shor, 1994), se han aplicado grandes esfuerzos para encontrar los medios físicos que permitirían realización experimental de computadoras cuánticas, tales como: iones fríos atrapados, condensados de Bose-Einstein, moléculas en medios amorfos, espines nucleares y puntos cuánticos. Sin embargo, todavía existen severos problemas relacionados en su mayoría con la decoherencia (que es un proceso rápido de "clasicalización" de sistemas cuánticos debido a la interacción con el medio ambiente) y, por lo tanto, de destrucción de superposiciones cuánticas, necesarias para realizar los algoritmos propuestos . ●

[Bibliografía]

Bell J.S., *Physics* **1** 195-200 (1964).
Bennett H., *Phys. Rev. Lett.* **68** 3121 (1992).
Bennett H. *et al.*, *Phys. Rev. Lett.* **70** 1895 (1993).
Bohr N. (1935) *Phys. Rev.* **38** 696-702.
Bouwmeester D., Pan J-W. Mattle K., Eibl M., Weinfurtner H., Zeilinger A., *Nature* (Londres) **390** 575 (1997).
Deutsch D., Proc. Royal Soc. (Londres) A **400** 97-117 (1985).
Einstein A, Podolsky B. Rosen N, *Phys. Rev.* **45** 777 (1935).
Grover L.K., *Phys. Rev. Lett.* **79** 4709 (1997).
Hughes R.J *et al.*, *Contemp. Phys.* **38** 149 (1995).
Muller A., Zbinden H., Gisin N., *Europhys. Lett.* **33** 335 (1996); **33** 586 (1997).
Schrodinger E., *Naturwissenschaften* **23** 807, 823, 844 (1935).
Shannon C.E., *Bell Syst. Tech. J.* **28** 657 (1949).
Shor P.W., *Phys. Rev.* A **52** R2493 (1995). Shor P.W., in Proc. of the 35th Ann. Symp. of Found. Comp. Sci. (Los Alamitos, CA: IEEE Computer Society, 1994) p. 124.
Wootters W.K., Zurek W.H., *Nature* **299** 802-803 (1982).

Alicia y Beto se comunican. Introducción a la comunicación cuántica

EL ESTILO DE VIDA ACTUAL DEPENDE DE UN INTERCAMBIO CONTINUO DE INFORMACIÓN POR LO QUE ES NECESARIO GARANTIZAR TRANSMISIONES EFICIENTES Y SEGURAS. SIN ESTE PAR DE GARANTÍAS, LAS TRANSACCIONES FINANCIERAS SE VOLVERÍAN CAÓTICAS PONIENDO EN PELIGRO LA ECONOMÍA MUNDIAL. EN LA BÚSQUEDA DE SOLUCIONES AL PROBLEMA DE LA PRIVACIDAD EN LAS COMUNICACIONES, LA CIENCIA ACTUAL ESTÁ FORMULANDO MODELOS CUÁNTICOS DE CIFRADO. CON ELLO SE ESTÁ PREPARANDO TERRENO PARA INAUGURAR LA ERA DE LA COMUNICACIÓN CUÁNTICA.

Blas Manuel Rodríguez Lara

En este artículo se tratará el problema de Alicia y Roberto –Beto para los amigos– habitantes de un mundo ideal. Alicia desea compartir información cuántica generada en su laboratorio, por ejemplo un bit cuántico o qubit, con Beto, cuyo laboratorio se encuentra en una locación diferente. Ella quiere que la información sea transmitida de manera eficaz y eficiente. En caso de existir errores en la transmisión, necesita que él esté consciente de la existencia de esos errores y sea capaz de resarcirlos. Para lograr esta tarea, Alicia y Beto cuentan con un canal clásico de comunicación y un proveedor de qubits entrelazados. Utilizando estos recursos se establecerá un canal cuántico de transmisión de información entre ellos y se analizará una forma de codificar y corregir los posibles errores inducidos por ruido –ideal como su mundo– en dicho canal.

¿Por qué comunicaciones cuánticas?

El problema de las transmisiones eficientes y seguras es de vital importancia en nuestra sociedad. El estilo de vida moderno depende de un intercambio continuo de información con fidelidad y privacidad garantizadas. Sin este par de garantías en sus transacciones, el mundo financiero, por ejemplo, sería un caos y con él, las economías mundiales.

Más de alguno podría preguntarse: ¿por qué, si la información que manejamos cotidianamente

BLAS MANUEL RODRÍGUEZ LARA (D.C. INAOE 05, SNI-Candidato) Investigador becario postdoctoral, Departamento de Física Teórica, Instituto de Física, Universidad Nacional Autónoma de México. Entre sus intereses se encuentran la docencia de la óptica e informática cuántica y la investigación de la interacción radiación-materia y sus posibles aplicaciones para el cómputo cuántico. Ha trabajado en caracterización de correlaciones cuánticas, reversión de dinámica y caracterización de objetos mesoscópicos en modelos de interacción radiación-materia.
bmlara@fisica.unam.mx

es clásica, nos metemos en problemas trabajando con información cuántica? ¿Por qué utilizar comunicaciones cuánticas? Tres razones, suficientes para contestar la primera pregunta, son expuestas por Kamil Bradler en su contribución a este volumen, relacionada con la búsqueda de soluciones al problema de la privacidad en las comunicaciones. Un ejemplo muy particular de esas razones es el siguiente:

La criptografía clásica, utilizada actualmente para proteger la información transmitida por los canales de comunicación existentes, se basa en la especulación acerca de la imposibilidad de descomponer eficientemente números enteros grandes en sus factores primos utilizando un algoritmo clásico. En 1994, Peter Shor (Massachusetts Institute of Technology, EUA) demostró que encontrar los factores primos de un número entero puede realizarse de manera eficiente con un algoritmo cuántico. El día en que sea posible implementar el algoritmo de factorización en primos de Shor, las comunicaciones clásicas, con los modelos de cifrado que conocemos, dejarán de ser seguras. Si ese día llegare, será necesario tener una criptografía cuántica lista, que permita recuperar la privacidad en los procesos de transferencia de información.

La segunda pregunta, que funge como título de esta sección, puede justificarse en función de la respuesta anterior. Si es necesario utilizar modelos de criptografía cuántica para garantizar la privacidad de las comunicaciones, entonces será de vital importancia contar con canales de comunicación que permitan transmitir información cuántica.

Canal cuántico

Al medio capaz de transferir uno o más qubits se le llama canal cuántico. Establecer un canal de este tipo entre Alicia y Beto soluciona su primer problema: ¿cómo transmitir un qubit entre ellos?

Alicia y Beto cuentan con un proveedor de pares de qubits entrelazados, *deus ex machina*. Este proveedor les asegura que cada uno recibirá un qubit perteneciente a un par entrelazado, que es la superposición coherente con igual amplitud de los dos qubits en el estado cero y los dos qubits en el estado uno. Esto significa que si Alicia y Beto realizan la misma medición proyectiva en su respectivo qubit, encontrarán que los dos bit clásicos, resultado de sus mediciones, tendrán el mismo valor. Además, Alicia cuenta con un qubit adicional en un estado cualquiera que desea transferir a Beto; a este qubit se le llamará qubit mensaje.

Para realizar la transferencia, Alicia debe entrelazar el qubit mensaje con su qubit, perteneciente al par distribuido por el proveedor, y asegurarse que la información que contiene se transfiera al qubit de Beto. Esto lo puede lograr mediante dos pasos: una compuerta de negación controlada (CNOT) seguida de una compuerta Hadamard. Una vez realizadas este par de operaciones locales en el laboratorio de Alicia, existe una posibilidad de uno en cuatro que el qubit localizado en el laboratorio de Beto sea igual al qubit mensaje.

Alicia puede realizar una medición proyectiva en su qubit; dicha medición puede resultar en una de cuatro opciones de dos bits clásicos con igual probabilidad de ocurrencia: 00, 01, 10, 11. A cada uno

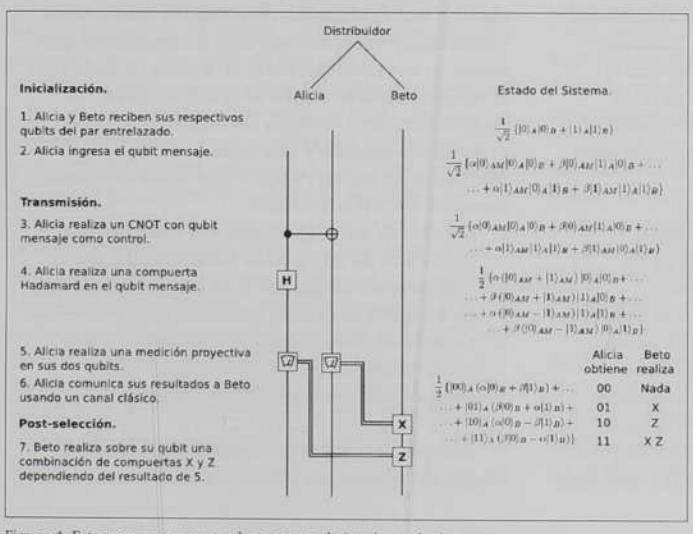

Figura 1. Este esquema muestra los pasos y el circuito cuántico para establecer el protocolo de teletransportación cuántica.

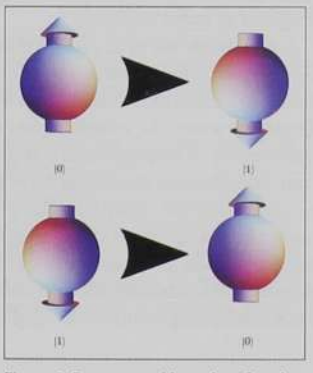

Figura 2. Representación en la esfera de Bloch de un error de tipo cambio de qubit.

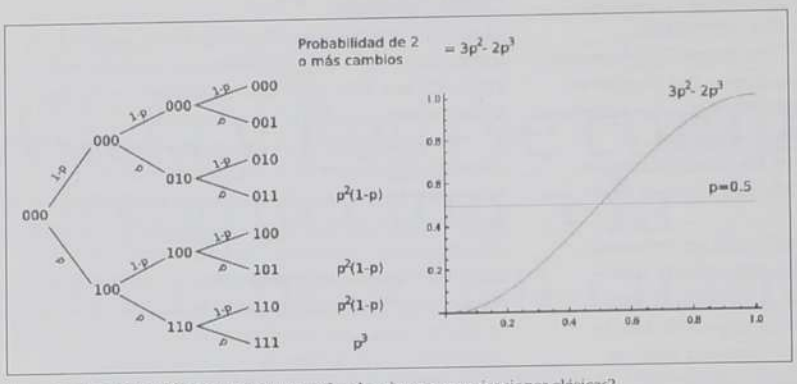

Figura 3. ¿Por qué funciona el cifrado por redundancia en comunicaciones clásicas?

de estos resultados corresponde un estado particular en el qubit de Beto. Por ejemplo, el qubit de Beto es idéntico al qubit mensaje si y sólo si Alicia obtiene como resultado de su medición los bits clásicos 00. Entonces, cuando Alicia obtiene este resultado, puede anunciarle a Beto que tiene el bit correcto utilizando el canal clásico. Esto es efectivo, pero no eficiente.

Para solucionar este problema de optimización, es posible asociar tres conjuntos de operaciones específicas a realizar en el laboratorio de Beto a fin de llevar el estado de su qubit al estado original del qubit mensaje de Alicia. Cada uno de estos conjuntos de operaciones estará relacionado con cada uno de los otros tres resultados restantes, que Alicia puede obtener en su medición proyectiva. De esta forma se asegura que la transmisión del estado del qubit mensaje del laboratorio de Alicia al qubit del laboratorio de Beto se realiza siempre, contando con que Alicia comparta cada vez, utilizando el canal clásico, los dos bits clásicos resultado de las mediciones proyectivas sobre sus dos qubits, y Beto realice las operaciones correspondientes para recuperar el qubit mensaje.

A este protocolo se le conoce como teletransportación cuántica, pues en ningún momento se transfiere un sistema físico de un laboratorio a otro. La información cuántica simplemente es transportada a la distancia utilizando el entrelazamiento que existe en el par de qubits, que originalmente comparten las partes. Cabe resaltar que la información en el qubit mensaje se pierde mientras se transfiere al qubit receptor. El protocolo de teletransportación constituye un canal de comunicación cuántico. Es importante mencionar que el canal cuántico se destruye en el momento en que Alicia realiza sus mediciones proyectivas. Para transmitir un segundo qubit de información es necesario que el proveedor distribuya a Alicia y a Beto un nuevo par de qubits entrelazados, lo cual permite ver al proveedor como un canal cuántico *per se*.

Canal cuántico con ruido

El problema de Alicia y Beto se ha resuelto en teoría. Los primeros contratiempos aparecen con las pruebas del sistema. Ellos deciden probar su canal de comunicación y realizan las mismas mediciones proyectivas en cada uno de sus laboratorios utilizando qubits mensaje bien caracterizados y el canal de comunicación clásico para compartir sus resultados. Alicia y Beto se dan cuenta que los bits clásicos que obtienen como resultado de su prueba, algunas veces no son los correctos. Es más, se dan cuenta que p veces de cada cien los resultados que obtienen son opuestos entre sí; q veces de cada cien el resultado que obtienen es el mismo pero con signo contrario; y pq veces de cada cien obtienen el resultado opuesto y con signo contrario. Estos resultados les hacen concluir que su canal cuántico presenta dos tipos de ruido:

1. Cambio de qubit (*qubit flip*). Los componentes del estado de un qubit se intercambian por el componente ortogonal de la base: el estado cero de un qubit pasa a ser un estado uno y viceversa.
2. Cambio de fase (*phase flip*). Este tipo de ruido corresponde a un cambio de signo en el componente en el estado uno del qubit.

Este par de errores discretos son los modelos ideales de errores que pueden ocurrir en un canal

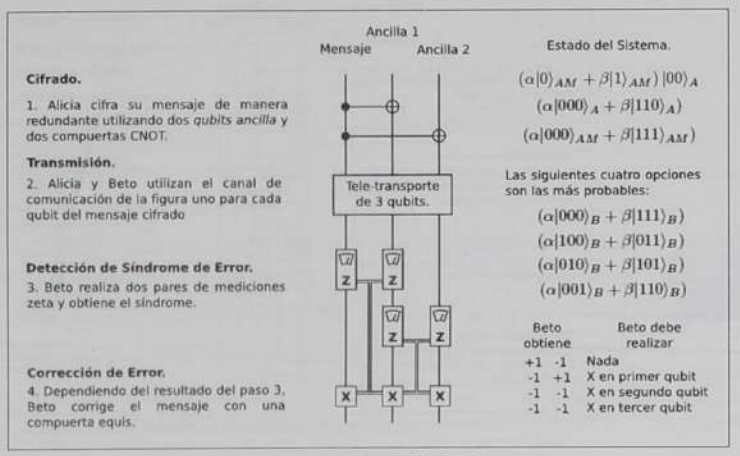

Figura 4. Circuito cuántico para corregir errores de cambio de qubit.

cuántico. Un error real es continuo y corresponde a una rotación aleatoria de un qubit, la cual puede ser tan pequeña que la diferencia entre el qubit original y el qubit con error sea casi imperceptible. Es posible demostrar, aunque queda fuera de los objetivos de este documento, que los métodos de corrección de errores que se presentarán a continuación protegen la información cuántica de rotaciones aleatorias.

Corrección de errores: cambio de qubit

Del par de errores encontrados por Alicia y Beto, el correspondiente a cambio de qubit existe en comunicaciones clásicas. De hecho, recibe un nombre análogo. La forma de corregirlo clásicamente es por redundancia, es decir, cifrar el mensaje original utilizando repetición del bit. Esto es, un bit cero se cifra en un bit lógico que contiene un número impar, al menos tres, de bits cero y un bit uno se cifra en un bit lógico compuesto por el mismo número impar que antes de bits uno.

Tal vez alguno se pregunte ¿por qué se repite el valor de un número impar mayor o igual que tres veces? o ¿qué tan seguro es cifrar por redundancia? El cifrado debe ser una repetición impar para dar lugar a un voto de mayoría. En el caso de redundancia triple, si dos bits del bit lógico son iguales y uno diferente, entonces por mayoría se decide que el bit correcto es el que aparece dos veces y se cambia el valor del bit diferente. Esto sólo se puede hacer cuando el número total de repeticiones es impar, con números pares existe la oportunidad de empate. Si la probabilidad de que ocurra uno y sólo un cambio de bit es menor de 50%, esta forma de cifrado tiene una probabilidad mayor a 50% de un voto de mayoría correcto.

Esta estrategia de corrección de errores puede extenderse al caso de información cuántica. Si la probabilidad de que ocurra un cambio de más de un qubit a la vez es muy pequeña, es posible utilizar un cifrado por repetición, donde Alicia cifre el qubit cero de su mensaje en un qubit lógico 000 y el qubit uno en un qubit lógico 111. Beto debe conocer en qué qubit suceden las cosas para intentar corregir el error, así que es importante conocer las variantes, o síndromes, de error ante el cifrado propuesto. A continuación se enumeran:

0. No pasa nada, no hay error.
1. Hay un cambio de qubit en el primer qubit.
2. Hay un cambio de qubit en el segundo qubit.
3. Hay un cambio de qubit en el tercer qubit.

Beto puede construir cuatro medidas proyectivas que diagnostiquen cada uno de estos síndromes. Cada una de las medidas entregaría un triplete de bits clásicos cero o uno dependiendo si el qubit tiene o no el tipo de error. En caso de que el triplete clásico resultado sea cero, el qubit lógico con el mensaje es destruido; en caso de que el triplete clásico resultado sea uno, el qubit lógico con el mensaje se mantiene igual y es posible corregirlo realizando un cambio de qubit en el qubit correspondiente. Nuevamente, Beto tiene en sus manos una primera estrategia efectiva, más no eficiente.

Es posible construir un par de operaciones de medición que no afecten el qubit lógico mensaje. Esto implica utilizar un medidor cuyos estados propios sean el qubit lógico cero y uno, por ejemplo, una compuerta zeta actuando en uno de los qubits. La compuerta zeta da como resultado un signo positivo, +1, si el estado del qubit es cero, y un signo negativo,

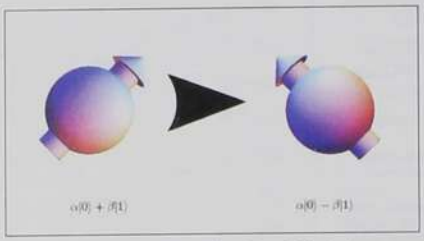

Figura 5. Representación en la esfera de Bloch de un error de tipo cambio de fase.

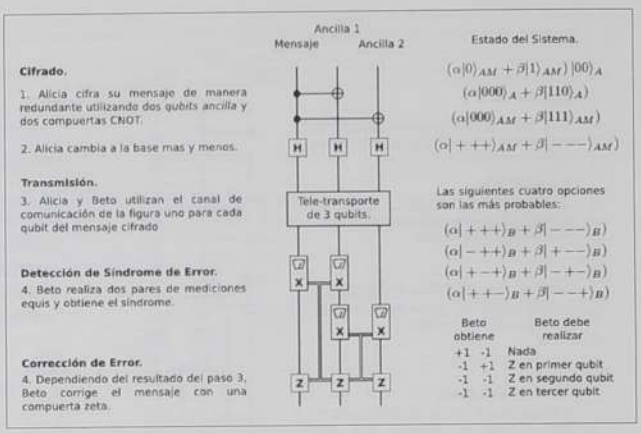

Figura 6. Circuito cuántico para corregir errores de cambio de fase.

-1, si el estado del qubit es uno dejando el qubit en el estado original. Si Beto mide con una compuerta zeta en el primer y segundo qubit del qubit lógico haciendo nada en el tercero, entonces obtendrá un signo positivo, si los dos qubits son iguales, y un signo negativo, si los dos qubits son diferentes. Si después Beto mide con una compuerta zeta en el segundo y tercer qubit del qubit lógico, entonces el resultado de las dos mediciones puede dar cuatro combinaciones:

0. Dos signos positivos. Es muy probable que los tres qubits son iguales, no tiene que corregir nada.
1. Primer signo negativo y segundo positivo. Es muy probable que el primer qubit es el diferente; para corregir, tiene que aplicar una compuerta equis, que realiza un cambio en el primer qubit.
2. Dos signos negativos. Es muy probable que el segundo qubit es el diferente; para corregir, tiene que aplicar una compuerta equis en el segundo qubit.
3. Primer signo positivo y segundo negativo. Es muy probable que el tercer qubit es el diferente y entonces se aplica una compuerta equis en el tercer qubit para corregir.

Ahora Beto tiene una estrategia de corrección del error de cambio de qubit de dos partes: la primer parte le permite diagnosticar, con una alta probabilidad de certeza, el síndrome de error presente en su qubit después de ser transmitido por el canal; en la segunda, según el diagnóstico, Beto puede no hacer nada o aplicar una compuerta equis en uno de los qubits para corregir el probable error.

Corrección de errores: cambio de fase

Por su parte, el cambio de fase no tiene un equivalente clásico. Esto puede hacer pensar que encontrar una estrategia de corrección para este error puede ser más difícil, pero no es así. El cambio de fase es de naturaleza cuántica y, precisamente, es la naturaleza cuántica lo que permite convertirlo en un error de cambio de qubit que ya se conoce y para el cual se tiene una estrategia de corrección.

Alicia puede realizar el cifrado utilizando el qubit lógico más, signo positivo, la superposición del qubit cero y el qubit uno y el qubit lógico menos, signo negativo, la superposición de qubit cero y el qubit uno con signo negativo. Utilizando este código, el error de cambio de fase cambia al qubit lógico más en el qubit

La criptografía clásica, utilizada actualmente para proteger la información transmitida por los canales de comunicación existentes, se basa en la especulación acerca de la imposibilidad de descomponer eficientemente números enteros grandes en sus factores primos utilizando un algoritmo clásico.

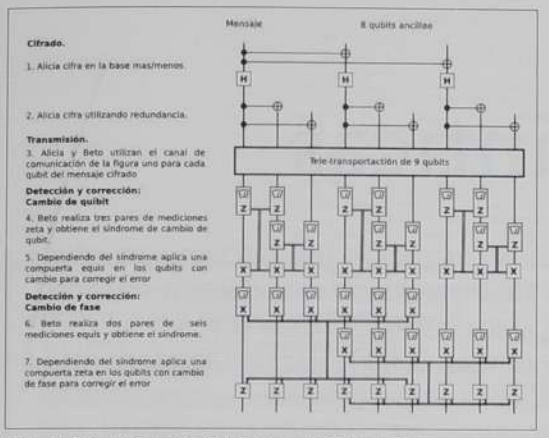

Figura 7. Circuito cuántico para realizar el cifrado de Shor.

lógico menos, y viceversa. Es decir, Alicia convierte un error de cambio de fase en un error de cambio de qubit. Alicia y Beto ya han desarrollado una estrategia para detectar y corregir este error utilizando redundancia. La diferencia con la estrategia previa se encuentra en la forma de diagnosticar el síndrome de error y corregirlo. En este caso, el diagnóstico se realiza utilizando la compuerta equis en el primero y el segundo qubit, y la compuerta equis en el segundo y tercer qubit. El síndrome resultado corresponde con las combinaciones de signo obtenidas anteriormente. La corrección se da aplicando la compuerta zeta en el qubit correspondiente.

Corrección de errores: cifrado de Shor

Es posible utilizar un cifrado combinado para combatir ambos tipos de errores. Primero, es necesario que Alicia cifre su qubit mensaje en la superposición definida para combatir el cambio de fase utilizando tres qubits y realizar un qubit lógico redundante en estados más y menos; después, ella debe cifrar el qubit lógico resultado utilizando el código para cambio de bit replicando el qubit lógico anterior tres veces. Este cifrado entrega un qubit lógico final compuesto por nueve qubits. A este código de cifrado se le conoce como *cifrado de Shor*. Es posible demostrar que dicho cifrado protege contra los efectos de un error arbitrario, pero eso rebasa los fines de este documento.

Así, pues, es altamente probable escapar de los efectos de un error arbitrario en el canal cuántico de comunicación utilizando nueve qubits para cifrar un qubit en un qubit lógico con el cifrado de Shor y realizando un total de seis operaciones zeta en pares –para analizar triadas de qubits y detectar los síndromes de cambios de qubit– y doce operaciones equis, en dos conjuntos de seis –para detectar el síndrome de cambio de fase ocurrido y entregar información a Beto sobre las operaciones que debe realizar para corregir el error introducido por el paso a través del canal.

Como conclusión resaltamos que se ha presentado un modelo de juguete de comunicación cuántica entre dos puntos con un protocolo específico de corrección de errores, el cifrado de Shor. Este protocolo permite ejemplificar de manera sencilla las ideas que subyacen en un código de corrección de errores cuántico: cifrado, detección de síndrome y recuperación del mensaje original.

Esto es sólo la punta del iceberg de un campo de investigación que utiliza el análisis funcional y la geometría diferencial como herramientas básicas.[1]

[Notas]

[1] Para personas interesadas en una presentación formal del tema con todas sus implicaciones, es recomendable revisar las siguientes fuentes disponibles de manera gratuita en Internet:

Notas del curso en computación cuántica de John Preskill (CalTech, EUA) en http://www.theory.caltech.edu/people/preskill/ph229/

Tesis doctoral en códigos estabilizadores y corrección de errores cuánticos de Daniel Gottesman bajo la supervisión de John Preskill en http://www.arxiv.org/abs/quant-ph/9705052

Para ampliar la información sobre cifrado cuántico y corrección cuántica de errores, el lector puede consultar, además, las siguientes publicaciones:

Quantum computation and quantum information de Michael Nielsen e Isaac Chuang.

The physics of quantum information, editada por Dirk Bowmeester, Artur Ekert y Anton Zeilinger. En esta última se hacen conexiones con sistemas físicos y sus implementaciones en laboratorio.

Finalmente, está disponible un par de bitácoras digitales, escritas por investigadores que desde hace varios años tratan el tema de la informática cuántica:

The Quantum Pontiff, bitácora de Dave Bacon (U.Washington, EUA):http://scienceblogs.com/pontiff/

Shtetl Optimized, bitácora de Scott Aaronson (MIT, EUA): http://scottaaronson.com/blog/

Aquí se pueden encontrar comentarios sobre los últimos acontecimientos en las áreas de computación, informática y mecánica cuántica, además de vínculos a las bitácoras digitales de otros investigadores como David Deutsch, Michael Nielsen, Isaac Chuang, entre otros.

Distribución de claves cuánticas

LA TEORÍA DE INFORMACIÓN CUÁNTICA ES UNA DISCIPLINA RELATIVAMENTE NUEVA PERO HA ENSANCHADO LOS CONOCIMIENTOS BÁSICOS EN EL CAMPO DE LA MECÁNICA CUÁNTICA. DESDE EL PUNTO DE VISTA DE LAS APLICACIONES PRÁCTICAS, LA PARTE MÁS DESARROLLADA ES LA COMUNICACIÓN CUÁNTICA Y LA DISTRIBUCIÓN DE CLAVES CUÁNTICAS COMO SU PRINCIPAL EXPONENTE. ESTE ELEMENTO CRIPTOGRÁFICO HA AUMENTADO SUSTANCIALMENTE EL NIVEL DE SEGURIDAD DE ALGUNAS CLASES DE COMUNICACIÓN PRIVADA, DEBIDO A LAS LEYES DE MECÁNICA CUÁNTICA QUE LO RIGEN.

Kamil Bradler

Una de las metas principales de la criptografía clásica es proveer de confidencialidad a los mensajes que son transportados y/o almacenados. Este procedimiento se conoce como encriptación de datos, y básicamente se refiere a la transformación matemática reversible de un texto en claro (mensaje) a un texto cifrado. La operación inversa se conoce como desciframiento. Para encriptar el texto en claro, los participantes autorizados están equipados con una clave compartida. Uno de los requerimientos básicos en la confidencialidad es que la información sobre el mensaje que una tercera persona pueda obtener (un adversario sin el conocimiento de la clave), pueda hacerse arbitrariamente pequeña con la condición de que no existan premisas sobre la sofisticación tecnológica o poder computacional del adversario (seguridad incondicional). En la comunidad criptográfica al emisario se le llama Alice, al destinatario Bob, y al adversario Eve (nomenclatura tradicional para los participantes, que proviene de la criptografía clásica). En lo subsecuente seguiremos esta nomenclatura. Es importante mencionar que la criptografía cuántica es un amplio conjunto de protocolos de comunicación cuántica. En este artículo, se hablará solamente del protocolo más importante (desde el punto de vista práctico): la distribución de claves cuánticas (*Quantum Key Distribution*, QKD).

La criptografía clásica moderna tiene un uso muy amplio, por lo que cabe preguntarse ¿por qué sustituirla y considerar algo como QKD? Existen al menos tres razones para hacerlo:

1. La seguridad de la mayoría de los esquemas criptográficos cuánticos con usos prácticos (procesos bancarios y comunicación por Internet) yace en alguna hipótesis matemática proveniente de la teoría de números, que está relacionada con las llamadas funciones de un solo sentido. Dichas funciones son fáciles de calcular en una dirección pero difíciles de invertir. Desafortunadamente, el grado de dificultad de las transformaciones inversas de las funciones de un solo sentido utilizadas en la práctica no ha sido probada, únicamente existen conjeturas al respecto.

KAMIL BRADLER School of Computer Science, McGill University, Montreal, Quebec, Canadá e Instituto de Física, UNAM, México D. F. Obtuvo su doctorado en la Charles University de la República Checa siendo precisamente su área de especialidad la información cuántica. Ha hecho contribuciones relevantes en la descripción y propuesta de protocolos de comunicación cuántica. Actualmente trabaja en las consecuencias de la relatividad en procesos de interés en esta subdisciplina. kbradler@cs.mcgill.ca

2. Aun si su validez fuera probada, tendríamos que adivinar el poder computacional teórico de un intruso para asegurar que el texto cifrado no pueda ser descifrado por un ataque de fuerza bruta, que se defina como una búsqueda exhaustiva a lo largo de todo el espacio de la clave. Por tanto, vemos que la mayoría de los algoritmos clásicos utilizados en la práctica yacen en la llamada "seguridad computacional", *i. e.*, seguridad basada en adivinar qué tan rápida puede ser la computadora del intruso. Aparentemente, las estimaciones hechas el día de hoy no serán válidas el día de mañana.
3. Más aún, muchos protocolos que se cree son difíciles de ser atacados por las computadoras clásicas son vulnerables a los ataques cuánticos por las llamadas computadoras cuánticas. Por lo tanto, cuando las computadoras cuánticas estén disponibles, mucha de la criptografía clásica será desesperadamente obsoleta.

Por el contrario, la seguridad de la QKD se basa en las leyes de la naturaleza, en este caso, en la mecánica cuántica. Como consecuencia, este protocolo no sufre ninguna de las desventajas enunciadas previamente. El propósito de la QKD es establecer una secuencia aleatoria de bits (la clave) compartida por Alicia y Bob, en donde cada uno de ellos puede estar altamente seguro de que la espía llamada Eva no sabe casi nada sobre la clave. En el caso ideal, donde existen los componentes tecnológicos perfectos, ella realmente no obtendría información alguna o, de hacerlo, nosotros sabríamos que alguien ha escuchado la conversación y la transmisión se cancelaría. Sin embargo, en la realidad la situación es más complicada. Afortunadamente, se ha comprobado que aún bajo las condiciones tecnológicas reales podemos de manera arbitraria limitar la información por encima y alcanzar el nivel de seguridad incondicional.

Detalles de la QKD

Describamos, entonces, el esquema típico para la QKD, así como algunos de los componentes básicos y algoritmos utilizados para ello. Alicia y Bob están interconectados a través de un canal clásico y un canal cuántico. Eva puede hacer todo lo que las leyes de la física le permitan con el canal cuántico; en cambio, el canal clásico puede ser espiado, pero no alterado. En otras palabras, Alicia y Bob están autentificados, lo que es un requerimiento natural. Veremos pronto cómo es que la autentificación puede realizarse de una manera segura incondicionalmente.

En este punto, es deseable recordar que la QKD está compuesta por tres procedimientos criptográficos diferentes.

A) Autentificación de un canal clásico. Existen algoritmos clásicos provenientes de la familia de los esquemas de autentificación Wegman-Carter (WC), que son incondicionalmente seguros. El esquema WC requiere de alguna información secreta previamente compartida (Alicia y Bob necesitan al menos reunirse una vez), lo que se utiliza para su autentificación. Para la siguiente sesión, una pequeña parte de la clave generada a partir de la QKD es utilizada, de manera que no necesitan encontrarse nuevamente. Sin la etapa de autentificación, Eva puede pretender ser Alicia cuando habla con Bob y pretender ser Bob cuando habla con Alicia, lo que se conoce como ataque de ìhombre intermedioî. Otra forma de autentificación es el uso de las llamadas funciones *hash* ñhuellas digitales de los archivosñ como el algoritmo MD5 o la familia SHA-x, utilizadas actualmente en la comunicación por Internet. Debe enfatizarse que se supone que éstas son computacionalmente seguras; sin embargo, su seguridad no ha sido probada y a lo largo de su existencia, ésta ha sido comprometida en repetidas ocasiones.

B) QKD en sí. Aunque profundizaremos posteriormente, debe mencionarse que su seguridad está probada aún en la presencia de componentes tecnológicos imperfectos (QKD realista) y de la (casi) todopoderosa Eva, mencionada previamente.

C) Uso de la clave (en la criptografía convencional). La clave puede ser utilizada por Alicia y Bob para la encriptación de un mensaje. *One-time-pad* (también conocido como cifrado Vernam) es un cifrado clásico que pertenece al concepto de cifrados que son perfectos desde el punto de vista de seguridad pero completamente inservibles desde el punto de vista práctico. La razón es que si se quiere utilizar un cifrado Vernam, se requiere una clave aleatoria de, al menos, la misma longitud que el mensaje. La clave (en la forma de una serie de bits) es añadida, módulo dos (operación XOR), al mensaje

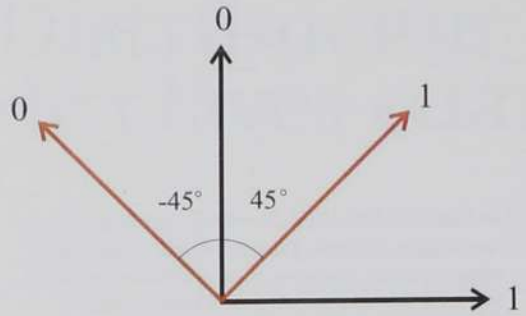

Figura 1. Ilustración del protocolo BB84 mediante el cual se construye una clave secreta compartida, que puede ser utilizada como llave para cifrar o descifrar mensajes. Este protocolo fue el primero en su tipo en el que se aprovecharon las características de bases cuánticas no ortogonales con fines criptográficos.

(una serie de bits, también), y se obtiene un texto cifrado. El desciframiento se realiza de la misma manera. Otro requerimiento de la seguridad del cifrado es que Alicia y Bob necesitan compartir una clave nueva y aleatoria para cada sesión. Es entonces cuando se dice que el cifrado Vernam es *perfectamente seguro*, lo cual es un subgrupo de cifrados seguros incondicionalmente. En otras palabras, el mensaje y el texto cifrado son estadísticamente independientes, y Eva no tiene ninguna información sobre el texto en claro. Sin embargo, ahora es evidente cuál es el problema respecto a la utilidad del cifrado: debido a que tienen que encontrarse para intercambiar la clave, la encriptación no es necesaria. La otra posibilidad es la creación y distribución de un libro de códigos; libros de una serie aleatoria de bits, utilizados como la clave para la encriptación y el desciframiento. Podemos imaginar fácilmente qué peligroso sería si uno de tales libros fuera descubierto por Eva. Como veremos, sólo la QKD, basada en la física cuántica, es la que da a este cifrado un poder inmenso: la seguridad requerida y aplicabilidad deseada. Desafortunadamente, el uso actual de la QKD no es factible para este propósito y las series generadas sirven como claves para los cifrados simétricos clásicos, como AES (*Advanced Encryption Standard*). Su seguridad no ha sido probada, y es la parte más débil de la QKD. La generación de la clave dentro de la QKD no es lo suficientemente rápida para encriptar en tiempo real grandes cantidades de datos con un cifrado Vernam.

QKD realista

La promesa de la criptografía cuántica fue anunciada por primera vez a principios de los años setenta, en trabajos de S. Wiesner. En 1984, Ch. Bennett y G. Brassard propusieron el primer esquema QKD, conocido como el protocolo "BB84". Con este esquema es posible ilustrar cómo trabaja la QKD (figura 1). En BB84, Alicia escoge aleatoriamente uno de los dos (cero lógico y uno) posibles estados de un *qubit* (quantum bit es la unidad elemental de la información cuántica que generaliza bits de la información clásica) y los envía a Bob. Éste escoge aleatoria e independientemente la base y mide la señal. Debido a la no-ortogonalidad de ambas bases y a la elección independiente de las medidas de base, Bob obtiene valores determinísticos aproximadamente en la mitad de los casos (cuando las bases coinciden). De hecho, esta es la única parte cuántica de todo el protocolo. Para excluir el uso de diferentes bases, Alicia se comunica con Bob por teléfono (o por otro canal clásico), y descarta los casos en los que las bases no coinciden. ¡Ellos NO se dicen los valores de los bits medidos! La serie de bits que queda se conoce como clave tamizada.

Antes de continuar, es importante mencionar otras alternativas de la QKD. En 1991, A. Ekert desarrolló un enfoque diferente a la QKD, que finalmente probó ser fructífero. Ekert propuso un protocolo de distribución de claves en el que pares entrelazados de qubits (estado de dos partículas correlacionadas cuánticamente, cuyas propiedades no son posibles de describir únicamente mediante correlaciones clásicas) son distribuidos a Alicia y Bob, quienes posteriormente extraen los bits de la clave tamizada mediante la medición en sus qubits. Muchas otras variantes de la QKD fueron propuestas posteriormente, tales como: el "protocolo de seis estados", en el que Alicia envía cada qubit en uno de seis posibles estados definidos; el protocolo B92, de Ch. Bennett, en el que Alicia envía uno de dos estados no-ortogonales. Sin embargo, desde el punto de vista práctico –y parcialmente desde el punto de vista de la seguridad– los protocolos más importantes siguen siendo el protocolo BB84 y el protocolo de Ekert con pares entrelazados. Continuaremos ilustrando la QKD en el primero de ellos.

La promesa de la criptografía cuántica fue anunciada por primera vez a principios de los años setenta en trabajos de S. Wiesner. Entre las contribuciones a esta disciplina destaca la creación del primer esquema de la distribución de claves cuánticas (QKD) por Ch. Bennett y G. Brassard (1984), conocido como protocolo "BB84", así como la invención del protocolo basado en pares entrelazados, contribución de A. Ekert en 1991.

Cuando se obtiene la clave tamizada, es necesario probarla en presencia de Eva. Algunos de los bits de la clave tamizada son sacrificados, es decir, su valor es revelado y comparado en un canal clásico. Si existe algún error, sabemos que alguien ha escuchado. En la práctica la situación no es tan simple. Todo lo anteriormente dicho podría funcionar adecuadamente si contáramos con los componentes físicos perfectos, como fuentes de fotones, canales y detectores ideales. Sin embargo, nada puede estar más lejos de la realidad. Para enunciar solamente algunos problemas, las fuentes de fotón, que producen estados de fotón únicos a demanda, no existen aún; los canales cuánticos son ruidosos y erróneos; y la eficacia de la detección de los detectores cuánticos es muy baja. Todo ello pudiera sobreponerse; sin embargo, el problema es cómo distinguir estos errores de los errores introducidos por la actividad de Eva. Estas dificultades técnicas son exactamente de las que Eva se aprovecha para ocultar su intromisión. El proceso para descubrirla es el siguiente: durante el estado de sacrificio de bits mencionado previamente, los participantes legales calculan la llamada "tasa cuántica de errores" (*Quantum Bit Error Rate*, QBER), es decir, una porción de los bits erróneos en la secuencia sacrificada. Esta función no es igual a uno porque Eva no es tan inocente como para espiar de manera continua, sino de vez en vez. Si QBER es lo suficientemente baja, podríamos ejecutar dos algoritmos clásicos. El primero de ellos es la *corrección clásica de error*, donde los bits erróneos de la clave tamizada son corregidos, lo que es seguido de una *amplificación clásica de la privacidad*. Al emplear este procedimiento, podemos lograr que la información en la clave accesible a Eve sea arbitrariamente pequeña. El precio a pagar es que la serie de la clave es acortada, por lo que la clave resultante es muy pequeña (kbits/sec). Si, por otro lado, la QBER es muy alta, detenemos la transmisión. A continuación se describen las versiones más simples y no-óptimas de ambos algoritmos.

Corrección clásica del error

Alicia y Bob mezclan la clave tamizada para *aleatorizar* la ocurrencia de errores. Posteriormente, dividen la secuencia en bloques, cuya longitud es una función de la QBER. Existe una alta posibilidad de sólo un error en el bloque, lo que puede indicarse mediante el cálculo de la paridad (la suma de todos los ceros y unos por módulo dos). La paridad se anuncia y si coincide para ambos participantes, el bloque se preserva temporalmente. En el caso opuesto, el bloque se divide en sub-bloques, y todo el procedimiento se repite hasta que se encuentra el bit equivocado. Existe aún una pequeña probabilidad de que un número par errores ocurran; para minimizar esta posibilidad, el procedimiento se repite en diversas ocasiones, con diferentes aleatorizaciones. Después de cada anuncio de paridad, el bit más importante de cada bloque se descarta para prevenir que Eva pueda conocer demasiado acerca de la serie de bits.

Amplificación clásica de la privacidad

Cuando ambos participantes están casi seguros de que comparten la misma secuencia, es tiempo de limitar la información de Eva por debajo de un nivel dado. Una vez más, Alicia y Bob dividen sus series en sub-secuencias, para las cuales calculan nuevamente la paridad. Sin embargo, la paridad ahora no es anunciada, puesto que constituye los bits de la clave final. Aparentemente, mientras más amplias las secuencias que escojan, más corta será la clave final. Este es el precio que los participantes legales pagan. Por otro lado, la información fugada puede ser hecha arbitrariamente pequeña (para una clave tamizada suficientemente larga).

Regresemos a las actividades maliciosas de Eva. ¿Cómo, exactamente, la mecánica cuántica puede

La QKD está compuesta por tres procedimientos criptográficos diferentes: autentificación de un canal clásico, la QKD en sí, y uso de la clave (en la cripotografía convencional).

prevenir que Eva obtenga información considerable sobre la clave? En otras palabras, ¿Por qué Eva necesariamente introduce errores durante un intento de espionaje? Existen dos razones principales desde el punto de vista de la mecánica cuántica: la imposibilidad de distinguir los estados no-ortogonales y el principio de no clonación.

Imposibilidad de distinguir los estados no-ortogonales

Hemos visto que Alicia envía un total de cuatro qubits en un espacio bidimensional de Hilbert, por lo que son no-ortogonales. Los postulados de la mecánica cuántica nos dicen que no podemos discriminar entre los estados no-ortogonales sin introducir errores. Aun cuando consideremos a Eva sobrenatural, creemos que tiene que obedecer las leyes de la mecánica cuántica. Lo que a Eva se le permite hacer es construir una serie de proyectores (operadores de medición), que minimicen el error de un resultado incorrecto. El conjunto es, por supuesto, conocido, de tal manera que sabemos, en principio, cuánta información puede obtener Eva.

Principio de no-clonación

Otra posibilidad que podría funcionar perfectamente en el mundo clásico es simplemente copiar los qubits que provienen de Bob y esperar el anuncio de las bases para ser capaz de medirlas. Por medio de esta estrategia, Eva podría obtener la máxima información sobre la clave. Afortunadamente, esto no es posible en el mundo cuántico. La linealidad de la mecánica cuántica prohíbe la clonación perfecta, lo que es completamente opuesto a lo que ocurre en el mundo clásico. La única cosa que Eva puede hacer es una clonación aproximada, lo que le da alguna información, pero introduce errores nuevamente. Una vez más, la estrategia óptima es el conocimiento, de tal manera que Eva no pueda sorprendernos nuevamente.

En general, al interactuar con un sistema cuántico y extraer alguna información, Eva siempre causa perturbaciones, que pueden ser detectadas y/o corregidas por los participantes legales. La raíz de esta propiedad peculiar puede ser trasladada a las relaciones de incertidumbre de Heisenberg entre dos observables incompatibles (como la posición y el momento). Si la perturbación es tan alta que ninguna clave puede ser establecida, la transmisión se termina y así ninguna información secreta es revelada.

¿Cómo codificar qubits?

Ya sabemos lo que Alicia y Bob tienen que hacer con sus qubits para extraer la clave final, pero no sabemos cómo hacerlo. En otras palabras, no sabemos cómo se codifica o se construye físicamente un qubit. A continuación se describen dos posibilidades, que usualmente se llevan a cabo en la práctica.

Codificación de polarización. Esta codificación fue utilizada en la primera demostración experimental de la QKD en 1992, y es muy útil para la descripción de los principios de la QKD. Los valores lógicos de los bits están representados por los grados de libertad de la polarización de los fotones. Primero, de acuerdo con la descripción de la QKD, la base diagonal u horizontal es escogida aleatoriamente, seguida de la elección aleatoria de las direcciones de polarización que representan los valores lógicos 0 y 1. El qubit es enviado a Bob, como se ve esquemáticamente

La linealidad de la mecánica cuántica prohíbe la clonación perfecta, lo que es completamente opuesto a lo que ocurre en el mundo clásico. Un intruso sólo puede hacer una clonación aproximada, lo que le da alguna información, pero siempre causa perturbaciones, que pueden ser detectadas y corregidas por los participantes legales.

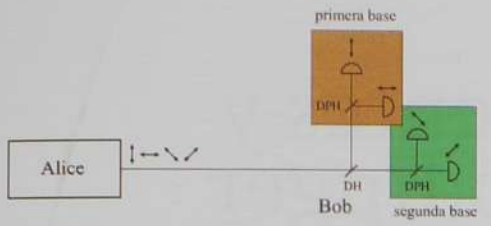

Figura 2. La QKD basada en la codificación de polarización. Bob está equipado con el ajuste pasivo, donde no necesita activamente cambiar las bases de medición. Alice aleatoriamente envía uno de los cuatro estados de polarización que primero alcanza un divisor balanceado de haz (DH), que decide cuál de las bases se usará. En cada rama del DH espera un divisor polarizador balanceado de haz (DPH) que, si las bases coinciden, envía el fotón que se dirige al detector correspondiente con el valor lógico del bit enviado.

en figura 2, donde, para analizar el qubit, Bob usa un ajuste pasivo. En el caso del ajuste pasivo, los qubits se encuentran primero con un divisor de haz balanceado, que aleatoriamente decide cuáles de las bases de Bob se usarán para la medición. Después, un divisor polarizador de haz para la base particular (horizontal o diagonal) manda el fotón a uno de los detectores. Podemos ver, por ejemplo, cuando Alicia envía un bit lógico 1 en la base diagonal y Bob mide en la misma base, Bob obtiene el valor 1 con probabilidad 100%. Si las bases difieren, la probabilidad del éxito es solo 50% y el bit se descarta posteriormente con fundamento en el anuncio público de las bases.

Codificación de fase. La codificación de fase se puede demostrar con dos interferómetros no balanceados de tipo Mach-Zehnder (ver figura 3). La razón para este tipo del intereferómetro es evitar la interferencia del primer grado, así que la diferencia entre las ramas del interferómetro debe ser superior a la longitud de coherencia del fotón. Los valores lógicos de los bits son representados como los cambios de fase en una rama del interferómetro de Alicia. Cuando el fotón llega al interferómetro de Bob, éste aleatoriamente escoge su base particular de medición, mediante el cambio de fase. Analizando el comportamiento de los fotones en los interferómetros, se puede mostrar que cuando las bases son las mismas, Bob obtiene el bit mandado por Alicia con certeza. Actualmente, todos los productos comerciales de la QKD usan este tipo de codificación. Notemos que la codificación de polarización se usa para la comunicación del espacio libre, mientras que codificación de fase es adecuada para las fibras ópticas.

El autor expresa su agradecimiento a Abigail Ortiz Domínguez por su ayuda con la traducción del idioma inglés al español .

bit	fase	base
0	0	1
1	π	1
0	π/2	2
1	3π/2	2

fase	base
0	1
π/2	2

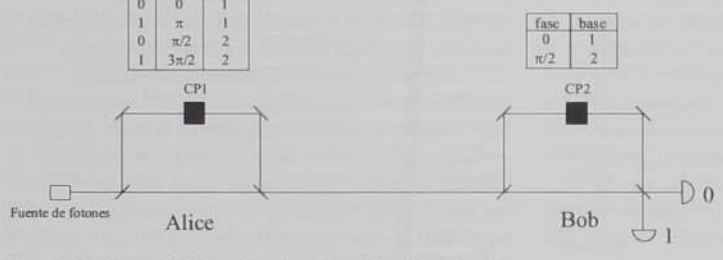

Figura 3. Un sistema QKD típico basado en la codificación de fase. Un fotón generado por Alice pasa por el interferómetro de tipo Mach-Zehnder, donde en una da las ramas encuentra el cambio de fase (CF). En las tablas podemos ver la codificación particular de Alice y Bob. Bob tiene el mismo aparato y aleatoriamente escoge la fase para determinar la base de medición. En el caso de las bases coincidentes, los fotones en las diferentes bases lógicas (0 y 1) siempre aparecen en las salidas distintas del interferómetro de Bob.

[Referencias]

G. S. Vernam (1926), *AIEE*, **45**, 109.
Ch. H. Bennett y G. Brassard, *Proc. IEEE InternationalConference on Computers, Systems, and Signal Processing* (Bangalore, India, 1984) (New York: IEEE), p. 175.
S. Wiesner (1983), *SIGACT News*, **15**, 78.
A. K. Ekert (1991), *Phys. Rev. Lett.*, **67**, 661.
W. K. Wootters y W. H. Zurek (1982), *Nature* **299**, 802.
M. A. Nielsen e I. L. Chuang (2000), *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge.

Estados coherentes y gatos de Schrödinger

LAS PROPIEDADES DE LA LUZ DESCUBIERTAS POR GLAUBER EN 1963 HAN SIDO DE VITAL IMPORTANCIA PARA EL DESARROLLO DE LA ÓPTICA CUÁNTICA Y LAS APLICACIONES TECNOLÓGICAS QUE USAMOS EN NUESTRA VIDA DIARIA. TAMBIÉN SON IMPORTANTES PARA ESTUDIAR LA CARA OCULTA DE LOS SISTEMAS CUÁNTICOS Y ENTENDER QUÉ ES LO QUE SEPARA EL COMPORTAMIENTO DE LOS OBJETOS MACROSCÓPICOS DEL COMPORTAMIENTO DE OBJETOS TAN DIMINUTOS COMO LOS ELECTRONES.

Sara Cruz y Cruz
Oscar Rosas-Ortiz

La interferencia de la luz es uno de los fenómenos más importantes e interesantes que se estudian en física. En un modelo sencillo, para producir interferencia se requiere de una fuente monocromática de luz y dos pantallas. La primera de las pantallas tiene dos rendijas paralelas, suficientemente angostas y cercanas entre sí (la apertura de las rendijas y la distancia entre ellas dependerá del color de la luz). La otra pantalla se coloca a una distancia perpendicular de la primera que es superior a la separación entre las rendijas. Cuando se hace pasar la luz monocromática por las rendijas y los haces emergentes se proyectan en la segunda pantalla, lo que se observa es una serie de franjas brillantes intercaladas con franjas oscuras (patrón de interferencia, ver figura 1). La explicación más sencilla de este fenómeno se obtiene al considerar a la luz como compuesta por ondas. Así, ambas rendijas se interpretan como una única fuente de ondas en fase que se superponen unas a otras: la coincidencia de crestas se manifiesta como franjas brillantes y la coincidencia de valles corresponde a las franjas oscuras (consultar la referencia [1] para más detalles). Decimos que la luz es más coherente mientras mejor definidas estén las franjas. Por ejemplo, como el patrón de interferencia de la luz emitida por una vela está menos definido que el de la luz emitida por un láser resulta que la primera es menos coherente que la segunda.

A partir de la teoría electromagnética propuesta por James Clerk Maxwell en el siglo XIX, la luz se ha interpretado como una combinación de campos eléctricos y magnéticos que se propaga en forma ondulatoria a través del espacio (*radiación electromagnética*). Esta bella formulación parecía establecer una clara distinción entre la radiación y los componentes fundamentales de la materia. Sin embargo, a principios del siglo XX se encontró que además de la luz, y bajo condiciones muy específicas del arreglo experimental, cualquier haz de partículas produce patrones de interferencia. Antes de este descubrimiento las partículas siempre se concibieron como pequeñas pelotitas desplazándose e interactuando entre ellas como si fuesen canicas. Con este punto de vista parecía inconcebible que dichas canicas se comportasen como ondas.

SARA CRUZ Y CRUZ es Profesora titular de la UPIITA-IPN. Obtuvo el Premio Arturo Rosenblueth 2006 a la mejor tesis doctoral del Cinvestav en el área de ciencias exactas. Investigadora visitante en estancia posdoctoral en el Departamento de Física del Cinvestav. Miembro del Sistema Nacional de Investigadores. sara@fis.cinvestav.mx

OSCAR ROSAS-ORTIZ es investigador titular en el Departamento de Física del Cinvestav. Obtuvo el Premio Arturo Rosenblueth 1998 a la mejor tesis doctoral del Cinvestav en el área de ciencias exactas. Miembro del Sistema Nacional de Investigadores y de la Academia Mexicana de Ciencias. orosas@fis.cinvestav.mx

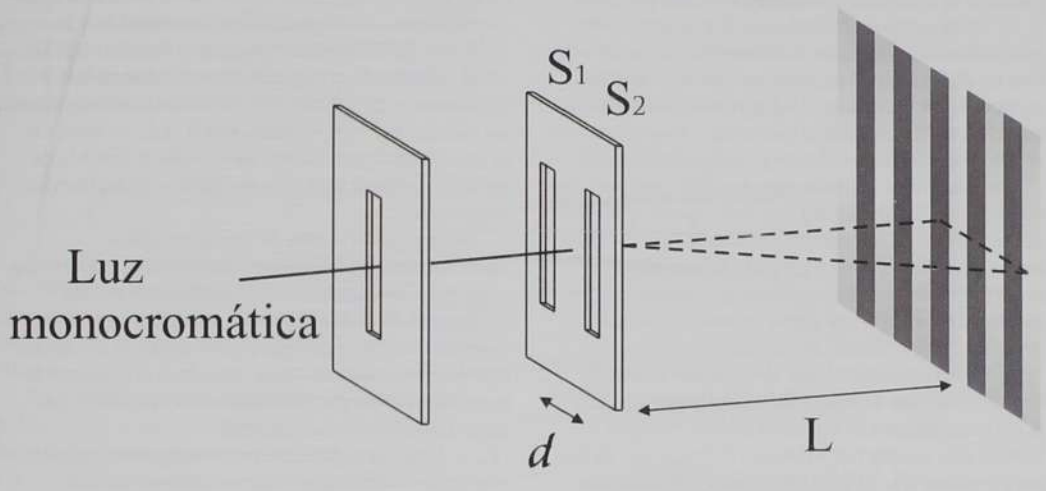

Figura 1. Interferencia de la luz producida por dos rendijas. Las rendijas S_1 y S_2 funcionan como una única fuente de ondas en fase. La distancia *d* entre ellas es inferior a la distancia *L*.

La intriga aumentó al descubrir, también a principios del siglo anterior, que la luz se dispersa al hacerla pasar por una nube de partículas. En la explicación más sencilla de este nuevo fenómeno se considera que la radiación electromagnética está compuesta por pequeños paquetes de energía que son indivisibles (*fotones*). Así, alguna de las partículas colisiona con un fotón y ambos rebotan como si fuesen canicas. En otras ocasiones, el fotón es absorbido por la partícula y re-emitido por ésta misma un poco más tarde. El juego es todo o nada: o bien el fotón es completamente absorbido por la partícula, o bien éste se comporta como otra partícula durante la colisión. El concepto más primitivo de fotón fue introducido por Max Planck en 1900. Un poco más tarde, en 1905, Albert Einstein perfeccionó el modelo de Planck para explicar porqué se produce una corriente eléctrica al bañar algunos materiales con luz de un determinado color (*efecto fotoeléctrico*).

La locura se hizo doble: las partículas y la radiación estudiadas por la Física de Newton y la de Maxwell intercambiaron papeles. Esta "contradicción" se volvió la huella digital de las investigaciones científicas del incipiente siglo XX y, alrededor de 1927, se logró estructurar un marco teórico que hoy en día es conocido como *Mecánica Cuántica*. Actualmente decimos que la luz tiene un *comportamiento clásico* si el fenómeno en cuestión puede explicarse satisfactoriamente con la formulación Maxwelliana de la radiación electromagnética. Por otro lado, cuando es indispensable introducir el concepto de fotón hablamos del *comportamiento cuántico* de la luz. En forma equivalente, las partículas presentan un comportamiento cuántico cuando no es suficiente con interpretarlas como pequeñas pelotitas y para su estudio se requiere del concepto de onda.

¿Dónde termina el comportamiento clásico y dónde empieza el cuántico? Aunque muchos de los fundadores de la teoría cuántica se plantearon esta pregunta fue a partir de 1926, gracias a un trabajo de Erwin Schrödinger [2], que los físicos abordaron el problema en forma sistemática. Schrödinger investigó el comportamiento cuántico del sistema físico más sencillo, el oscilador armónico lineal, y encontró que la teoría cuántica permite hacer predicciones "clásicas" bajo condiciones muy singulares.

Por otro lado, en 1927, Paul Adrien Maurice Dirac combinó la formulación Maxwelliana de la luz con el concepto de un oscilador cuántico y obtuvo una descripción cuántica de la radiación electromagnética [3]. En general, las predicciones de la formulación de Dirac no empatan del todo con los resultados de Maxwell ya que corresponden a dos descripciones diferentes de un mismo sistema, aplicables cada una de ellas en extremos opuestos del comportamiento de la luz.

En 1963 John R Glauber propone un modelo cuántico de la luz que permite hacer predicciones muy similares a las de Maxwell al tiempo que preserva la estructura teórica establecida por Dirac [4, 5]. De acuerdo con Glauber, la luz de Dirac debe producirse en estados de polarización coherentes si ésta ha de compararse con la luz Maxwelliana. Los *estados coherentes de Glauber* llamaron de inmediato la atención de la comunidad científica y fomentaron un sinfín de desarrollos teóricos y experimentales [6].

Tomando en cuenta lo anterior, cabe preguntarse hasta dónde es posible dar una descripción cuántica de los sistemas macroscópicos (sistemas como usted mismo, estimado lector). En 1935 Schrödinger reporta el diseño de un experimento donde se involucran un inocente gato y la desintegración de un átomo (decaimiento atómico). Para mostrar las "aparentes contradicciones" de la teoría cuántica con el "concepto de realidad" Schrödinger primero le adjudica un estado cuántico al gato, después mezcla éste último con el estado cuántico del átomo para concluir que el gato estará vivo y muerto a la vez en tanto no lo "observemos" [7]. Como veremos al final de este artículo, se pueden usar los estados coherentes de Glauber para representar al sistema cuántico del gato, incluso a nivel experimental [8].

Estados coherentes de la luz

"¿Te gustaría vivir en la casa del espejo minino?
Me pregunto si allí te darían leche."
Alicia hablando con su gatito frente al espejo.[1]

Clásicamente, un oscilador armónico corresponde a una masa unida al extremo de un resorte. Al aplicar una fuerza sobre la masa para que el resorte se comprima o se expanda notaremos que después de eliminar dicha fuerza el resorte "buscará" regresar a su posición inicial. Esto producirá un vaivén armónico en el sistema que se mantendrá así en tanto no se aplique ninguna otra fuerza. La energía que suministramos al sistema masa-resorte para modificar su estado inicial es arbitraria, será poca o mucha dependiendo de qué tanto comprimamos o expandamos al resorte, y permanecerá constante hasta que apliquemos una fuerza adicional.

Desde el punto de vista cuántico, el oscilador armónico no admite cualquier cantidad de energía; sólo es posible administrarle múltiplos semi-enteros de la cantidad $\hbar\omega$ (para una revisión de la evolución de conceptos, resultados e ideas asociados con la Mecánica Cuántica el lector puede consultar [9]). En otras palabras, la energía de un oscilador cuántico está cuantizada (admite sólo valores discretos) y toma los valores $E_n = \left(n+\frac{1}{2}\right)\hbar\omega$, $n = 0, 1, 2, \ldots$ donde $\hbar$ es una constante universal que recibe el nombre de *constante de Planck* y ω es la frecuencia de oscilación del resorte.

Dirac explotó la idea de que la radiación electromagnética puede modelarse matemáticamente como un conjunto infinito de osciladores donde cada modo de oscilación de los campos magnético y eléctrico corresponde a un resorte ideal. Al pensar en osciladores cuánticos, Dirac introdujo el concepto de *cuantización del campo electromagnético* y encontró que para el punto cero de la energía ($E_0 = \frac{1}{2}\hbar\omega$), la radiación electromagnética presenta fenómenos físicos muy interesantes que no están previstos en los resultados de la teoría Maxwelliana. A continuación mostramos algunos de los pasos teóricos involucrados, los lectores con poco o ningún entrenamiento matemático pueden ignorar cada una de las ecuaciones y prestar sólo atención a lo que se dice de ellas.

La formulación clásica de los campos electromagnéticos se hace a través del análisis de las ecuaciones de Maxwell. Para campos en el vacío, éstas llevan a las siguientes ecuaciones de onda:

$$\nabla^2 \vec{E} - \frac{1}{c^2}\frac{\partial^2}{\partial t^2}\vec{E} = 0 \ , \qquad \nabla^2 \vec{H} - \frac{1}{c^2}\frac{\partial^2}{\partial t^2}\vec{H} = 0 \ , \quad (1)$$

donde $\vec{E}$ es el campo eléctrico, $\vec{H}$ es el campo magnético y c es la rapidez de la luz. Para simplificar nuestro análisis consideraremos que los campos están dentro de una cavidad de volumen L^3 y que el campo eléctrico está polarizado en la dirección x mientras que el campo magnético tiene polarización y. Para un solo modo normal de amplitud q podemos escribir (ver [10]):

A partir de la teoría electromagnética, propuesta por James Clerk Maxwell en el siglo XIX, la luz se ha interpretado como una combinación de campos eléctricos y magnéticos que se propaga en forma ondulatoria a través del espacio. Por otro lado, a principios del siglo XX, gracias a las ideas de Max Planck y Albert Einstein, se entendió que la luz está compuesta de diminutos e indivisibles paquetes (o corpúsculos) de energía, que actualmente son llamados fotones.

$$E_x(z,t)=\left(\frac{2\omega^2 m}{\varepsilon_0 L^3}\right)^{1/2} q(t)\sin(kz),\quad H_y(z,t)=\left(\frac{2\omega^2 m}{\varepsilon_0 L^3}\right)^{1/2}\left(\frac{\dot{q}(t)\varepsilon_0}{k}\right)\cos(kz) \quad (2)$$

donde ε_0 es la *permitividad eléctrica* en el vacío. El número de onda k y la frecuencia ω satisfacen $k=\frac{\omega}{c}$. La energía correspondiente está dada por la función de Hamilton H:

$$H=\frac{1}{2}\int_{L^3}\left(\varepsilon_0 E_x^2+\mu_0 H_y^2\right)dv=\frac{1}{2}\left(m\omega^2 q^2+\frac{p^2}{m}\right) \quad (3)$$

con dv un elemento diferencial de volumen, $p=m\dot{q}$ el momento canónico de q y μ_0 la *permeabilidad* magnética. La expresión de la derecha corresponde a la energía de un oscilador armónico clásico.

En mecánica clásica el producto qp es igual al producto pq, se dice entonces que q y p conmutan. En el tratamiento cuántico usamos otros objetos matemáticos para representar a la amplitud y a su momento canónico, tenemos la correspondencia $q\to Q$, $p\to P$. Estos nuevos símbolos son tales que su producto no conmuta, simbólicamente escribimos:

$$[Q,P]=QP-PQ=i\hbar\ ,\quad [Q,Q]=[P,P]=0 \quad (4)$$

y decimos que Q y P son *operadores*. Conviene introducir un nuevo par de operadores a y a^+, definidos en términos de P y Q como sigue:

$$a=\frac{1}{\sqrt{2m\hbar\omega}}\left(m\omega Q+iP\right),\quad a^+=\frac{1}{\sqrt{2m\hbar\omega}}\left(m\omega Q-iP\right). \quad (5)$$

Estos nuevos operadores satisfacen las reglas de conmutación:

$$\left[a,a^+\right]=1\ ,\quad [a,a]=\left[a^+,a^+\right]=0\ . \quad (6)$$

La cuantización de los campos electromagnéticos empieza por escribir las soluciones (2) en términos de estos nuevos operadores:

$$E_x(z,t)=\varepsilon\left(a+a^+\right)\sin(kz),\quad H_y(z,t)=-i\varepsilon_0 c\varepsilon\left(a-a^+\right)\cos(kz), \quad (7)$$

donde la cantidad ε se expresa en unidades de campo eléctrico[2]. De esta forma, los objetos matemáticos usados en (7) para representar la polarización de los campos eléctrico y magnético son también operadores, al igual que la energía:

$$H=\hbar\omega\left(a^+a+\tfrac{1}{2}\right). \quad (8)$$

La expresión (8) es el *Hamiltoniano* de un oscilador cuántico, así que la energía de la correspondiente radiación electromagnética toma sólo valores discretos. Ahora investigamos los estados cuánticos correspondientes; a cada valor E_n de la energía le asociamos un vector $|n\rangle$ y pedimos que éste sea solución de la ecuación de *eigenvalores* $H|n\rangle=E_n|n\rangle$. La primera solución $|0\rangle$ corresponde al estado con energía más baja (estado base) $E_0=\frac{1}{2}\hbar\omega$ y se obtiene fácilmente notando que $|0\rangle$ también satisface la ecuación $a|0\rangle=0$. En otras palabras, el operador a "aniquila" al estado base. Por procedimientos algebraicos se muestra que $a^+|0\rangle=|1\rangle$ y, en general,

$$a|n\rangle=\sqrt{n}|n-1\rangle\ ,\quad a^+|n\rangle=\sqrt{n+1}|n+1\rangle\ . \quad (9)$$

Podemos entonces expresar un vector arbitrario $|n\rangle$ en términos de la acción iterada (n-veces) de a^+ sobre el estado base:

$$|n\rangle=\frac{1}{\sqrt{n!}}\left(a^+\right)^n|0\rangle,\quad n!=n(n-1)(n-2)\cdots 2\cdot 1 \quad (10)$$

La notación que estamos usando fue acuñada por Dirac mientras que la construcción de los estados $|n\rangle$ fue estudiada por Vladimir A. Fock. En este esquema el vector $|n\rangle$ indica que hay n fotones con energía E_n y la acción de a (a^+) sobre el estado $|n\rangle$ representa la pérdida (ganancia) de un fotón por parte del campo electromagnético. Por esta razón es que a y a^+ son conocidos respectivamente como operadores de aniquilación y creación. Obsérvese que $|0\rangle$ significa la

Los aspectos ondulatorios y corpusculares de la luz fueron inteligentemente combinados por Paul Adrien Maurice Dirac mediante su propuesta de la cuantización del campo electromagnético. La formulación de Dirac y la de Maxwell describen fenómenos que están en extremos opuestos del comportamiento de la luz.

ausencia de fotones con energía E_0, de tal suerte que esta energía debe corresponder al vacío.

Cabe notar que el fotón perdido o ganado por el campo es, a su vez, emitido o absorbido por la "materia" circundante y, en particular, por nuestros aparatos de medición. Así, los vectores de Fock son útiles para dar una descripción de la interacción de la luz con la materia. Otro aspecto importante de esta representación se hace patente al analizar las ecuaciones (7). Cada uno de los operadores del campo está escrito como una suma de los operadores de creación y aniquilación, es decir, cada uno incluye la información de las aniquilaciones tanto como la de las creaciones de fotones. Además, estos operadores no conmutan, así que ahora es importante la forma y el orden en que se multipliquen las polarizaciones E_x y H_y de los campos. En la formulación cuántica esto significa que ya no podemos medir simultáneamente a E_x y a H_y con precisión arbitraria. ¿Cómo podemos entonces, con la ayuda de estos operadores, recuperar la descripción Maxwelliana de la radiación electromagnética donde sí es posible medir E_x y H_y simultáneamente?

Regresemos a la ecuación (4). Si ΔQ y ΔP representan el error asociado a la medición de la amplitud y el momento canónico del oscilador cuántico, entonces el conmutador $[Q,P]=i\hbar$ nos lleva a la relación $\Delta Q\Delta P \geq \hbar/2$. Notamos que al hacer infinitamente pequeño el error ΔQ se tiene, por necesidad, un valor infinitamente grande de ΔP y viceversa (una expresión similar vale para ΔE_x y ΔH_y). En particular, para los vectores de Fock $|n\rangle$, los estados de la energía del oscilador cuántico satisfacen[3]:

$$\Delta_n Q \Delta_n P \geq \left(n+\frac{1}{2}\right)\hbar, \quad n=0,1,2,\ldots \qquad (11)$$

Para reducir al máximo la *relación de incertidumbre* (11) explotamos la habilidad que tienen los vectores n para superponerse y buscamos la combinación lineal:

$$|z\rangle_c = \sum_{n=0}^{\infty}\alpha_n|n\rangle = \alpha_0|0\rangle+\alpha_1|1\rangle+\ldots, \quad \alpha_k \in C, \quad k=1,2\ldots \qquad (12)$$

donde cada uno de los vectores de la suma (12) es un estado de la energía, así que el vector $|z\rangle_c$ también es un estado de la energía. Ahora exigimos que para este vector se cumpla

$$\Delta_c Q \Delta_c P = \frac{\hbar}{2} \qquad (13)$$

con $\Delta_c Q$ y $\Delta_c P$ los errores asociados con medir Q y P. En general, la ecuación (13) corresponde al mínimo valor posible de la incertidumbre (11). A los estados que satisfacen (13) se les llama *estados comprimidos*. En particular, si la ecuación (13) es tal que $\Delta_c Q = \Delta_c P = \sqrt{\hbar/2}$, decimos que los vectores $|z\rangle_c$ corresponden a *estados coherentes*.

Es sencillo mostrar que el estado fundamental $|0\rangle$ del oscilador cuántico es un estado coherente que puede representarse por la función:

$$\varphi_0(x)=\left(\frac{m\omega}{\pi\hbar}\right)^{1/4}\exp\left(-\frac{m\omega}{2\hbar}x^2\right) \qquad (14)$$

El módulo al cuadrado $|\varphi_0(x)|^2$ representa la probabilidad de encontrar al oscilador con la energía E_0 en el punto x. Esta probabilidad corresponde a una función Gaussiana centrada en el origen. Por otro lado, un estado coherente arbitrario se construye identificando los coeficientes α_k de la suma (12) que sean apropiados para que $\Delta_c Q = \Delta_c P = \sqrt{\hbar/2}$ se cumpla. Esto se logra exigiendo que $|z\rangle_c$ satisfaga la ecuación de eigenvalores $a|z\rangle_c = z|z\rangle_c$, con z un eigenvalor complejo. El resultado final se lee:

$$|z\rangle_c = \exp\left(-\frac{|z|^2}{2}\right)\sum_{n=0}^{\infty}\frac{z^n}{\sqrt{n!}}|n\rangle = \exp\left(-\frac{|z|^2}{2}\right)\left\{|0\rangle+z|1\rangle+\frac{z^2}{\sqrt{2}}|2\rangle+\cdots\right\}. \qquad (15)$$

La justificación de este último paso es como sigue: los operadores E_x y H_y son los objetos matemáticos que representan a las correspondientes polarizaciones de la radiación electromagnética. Por su naturaleza, estos operadores no pueden "leerse" como una función o un número, se requiere de sus eigenvectores para hacer predicciones dentro

Los estados coherentes de John R. Glauber entrelazan los resultados de Maxwell y los de Dirac y permiten dar una descripción cuántica del comportamiento clásico de la luz.

de la formulación cuántica. Por la ecuación (7) sabemos que E_x y H_y son, a su vez, expresados en términos de a y a^+. Así que los eigenvectores de la polarización son eigenvectores de estos últimos operadores. Según la teoría de Maxwell lo que se mide en el laboratorio es $|E_x(z)|^2$, que corresponde a la intensidad del campo eléctrico en el punto z. Para calcular la correspondiente expresión cuántica $\langle E_x^2 \rangle$ basta con obtener los eigenvectores de la parte de E_x que contiene al operador de aniquilación (los detalles se pueden consultar en referencias [5], [10] y [11]).

¿Qué es lo que hace coherente a los estados $|z\rangle_c$? A fin de contestar esta pregunta analicemos al más sencillo de ellos, representado por la función (14). Supongamos que al tiempo $t=0$ el oscilador cuántico no está en el origen sino en el punto $x=x_0$. La función $\varphi_0(x,0)$ que representa a este nuevo estado del sistema es idéntica a (14) pero cambiando $x \rightarrow x-x_0$ en el argumento de la exponencial. La teoría predice que la evolución temporal de este oscilador cuántico implica la siguiente densidad de probabilidad:

$$|\varphi_0(x,t)|^2 = \left(\frac{m\omega}{\pi\hbar}\right)^{1/2} \exp\left[-\frac{m\omega}{\hbar}\left(x - x_0\cos\omega t\right)^2\right]. \quad (16)$$

La curva descrita por (16) oscilará armónicamente hacia atrás y hacia delante 'como un todo', sin cambiar de forma. En otras palabras, esta función representa un *paquete de ondas* que no se deforma mientras se desplaza; las crestas de las ondas se mantienen unas sobre otras a lo largo del recorrido en forma coherente. Además, el centro del paquete de ondas se comporta como una partícula clásica sometida a la acción de un potencial de oscilador armónico. Lo mismo ocurre con todas y cada una de las funciones de onda asociadas con los vectores $|z\rangle_c$.

En resumen, los estados energéticos de la radiación electromagnética pueden estudiarse en términos de osciladores. Para compaginar las predicciones de la teoría cuántica con las predicciones de la formulación Maxwelliana lo mejor que podemos hacer es usar los estados coherentes $|z\rangle_c$ del oscilador cuántico. En este sentido, la radiación electromagnética que pueda describirse en términos de los vectores $|z\rangle_c$ no sólo es altamente coherente sino que también es la que más se asemeja, en su comportamiento, al concepto Maxwelliano de la luz. Entonces, la combinación de las formulaciones de Maxwell, Dirac y Glauber permite dar una descripción completamente satisfactoria de los comportamientos clásico (interferencia) y cuántico (efecto fotoeléctrico) de la luz así como de la transición entre ellos (estados coherentes).

Es notable que los estados coherentes hayan escapado muy pronto de las manos de Glauber y del ramo de la Óptica Cuántica para extenderse al campo de la Física-Matemática (ver por ejemplo [12]). Hoy en día hay *estados coherentes generalizados* que se definen con base en una estructura grupo-algebraica 'a la Perelomov' [13] (véase también [14] y referencias allí citadas), estados coherentes asociados con pares de hamiltonianos, que son socios supersimétricos [15], y estados coherentes definidos con base en la evolución temporal del sistema bajo estudio (ver por ejemplo [16] y referencias allí citadas). También se les encuentra en Física Nuclear [17] y en el estudio del efecto Hall cuántico [18]. Aún más importante es el hecho de que los estados coherentes proporcionan una posibilidad real de llevar acabo experimentos muy interesantes donde se requiere que la naturaleza cuántica de la luz se manifieste en forma clásica, tal y como ocurre con los llamados estados tipo "gato de Schrödinger", como veremos enseguida.

El gato de Schrödinger

> *"Bueno, estoy acostumbrada a ver gatos sin sonrisa," pensó Alicia; "¡pero una sonrisa sin gato es la cosa más curiosa que yo haya visto en mi vida!"*
> Alicia charlando con el gato Chesire.[4]

En su trabajo de 1935, Schrödinger escribe un párrafo que resulta por demás provocador:

> Uno puede aún diseñar situaciones un tanto ridículas. Un gato se coloca en una cámara de acero, junto con el siguiente dispositivo diabólico (que debe protegerse contra la interferencia directa del gato). En un contador

La combinación de las formulaciones de Maxwell, Dirac y Glauber representan un esquema completamente satisfactorio de los comportamientos clásico (interferencia) y cuántico (efecto fotoeléctrico) de la luz, así como la transición entre ellos (estados coherentes).

> dioactiva, tan pequeña que en el transcurso de una hora es probable que uno de los átomos decaiga pero también, con igual probabilidad, ninguno; si ocurre [lo primero entonces] el contador activa un martillo que rompe un recipiente con cianuro. Al abandonar el sistema [gato-átomo] por una hora uno podría decir que el gato todavía vive en tanto el átomo no haya decaído. El primer decaimiento atómico habría envenenado al gato. La función Ψ del sistema completo incluiría [el estado de] un gato vivo y un gato muerto (perdonen la expresión) mezclándolos o revolviéndolos en partes iguales.[5]

Asumiendo que el sistema gato-átomo puede describirse en términos de un determinado vector $|\psi\rangle$, éste tendría que construirse con los vectores que representan a los estados de "gato vivo" y "gato muerto", digamos $|\text{☺}\rangle$ y $|\text{☹}\rangle$, y los estados internos del átomo radioactivo cuando no ha decaído $|+\rangle$ y cuando ha decaído $|-\rangle$. Además, dicho vector tendría que representar la dependencia del estado del gato con el estado del átomo. Matemáticamente escribimos:

$$|\psi\rangle = \frac{|\text{☺}\rangle|+\rangle + |\text{☹}\rangle|-\rangle}{\sqrt{2}}. \qquad (17)$$

El término $|\text{☺}\rangle|+\rangle$ significa que si abrimos la cámara y encontramos al gato vivo sabremos inmediatamente, sin hacer medición alguna, que el átomo no ha decaído. El término $|\text{☹}\rangle|-\rangle$ significa que al encontrar al gato muerto entonces, necesariamente, el átomo ha decaído. Por otro lado, supongamos que de alguna forma, al abrir la cámara no podemos ver al gato pero sí podemos conocer el estado del átomo. Entonces la ecuación (17) nos indicará cuál es la condición del gato: si el átomo no ha decaído ($|+\rangle$) el gato estará vivo ($|\text{☺}\rangle$) mientras que el gato estará muerto ($|\text{☹}\rangle$) si el átomo está en el estado $|-\rangle$. Por esta razón decimos que los sistemas gato y átomo están *entrelazados* o *correlacionados*: lo que le ocurra al segundo influye fuertemente en la suerte del primero y viceversa, sin que medie información alguna entre ellos. La combinación de estas descripciones dada por el vector (17) significa que, en tanto no midamos (observemos) nada de lo que ocurre dentro de la cámara, el sistema completo se encuentra en una superposición de estados gato-vivo-no-decaimiento y gato-muerto-decaimiento. Antes de la medición, lo único que podemos asegurar es que hay igual probabilidad (50%) de encontrar al sistema completo en uno u otro estado. Esta situación desafía nuestro sentido de realidad porque, en nuestra experiencia cotidiana, esperamos que el gato esté ya sea vivo o muerto, independientemente de que lo miremos o no.

Sin embargo, la teoría cuántica es de carácter probabilístico así que, para confirmarla o rechazarla, debemos hacer un análisis estadístico. Esto significa repetir el experimento tantas veces como sea posible (mientras más veces mejor) y registrar cada uno de los resultados. Al final, lo que encontraríamos sería que la mitad de las veces tenemos un gato muerto y la mitad de las veces tendríamos un gato vivo. Así no hay misterio bajo la alfombra. Los problemas de interpretación de la teoría surgen al exigir que ésta sea aplicable incluso en eventos individuales, involucrando un solo gato y un solo átomo radiactivo en un solo experimento. Aunque la discusión está abierta desde prácticamente el surgimiento de la teoría cuántica (sugerimos al lector consultar las referencias [9,19,20]), de momento nos es suficiente con la primera de las interpretaciones mencionadas y saber que hay una forma de construir vectores del tipo (17) en el laboratorio sin involucrar a ningún inocente gatito.

Dado que en el mundo macroscópico no hay superposición de estados, si queremos construir un *estado tipo gato de Schrödinger* debemos buscar sistemas cuánticos con estados parecidos a $|\text{☺}\rangle$ y $|\text{☹}\rangle$. Es decir, necesitamos sistemas cuánticos que sean distinguibles macroscópicamente, tales como los estados de polarización de la luz descritos por Glauber. Escribimos:

$$|\psi\rangle = \frac{|z\rangle_c|+\rangle + |-z\rangle_c|-\rangle}{\sqrt{2}} \qquad (18)$$

donde $|z\rangle_c$ y $|-z\rangle_c$ son dos estados coherentes separados espacialmente (los paquetes de onda correspondientes tienen sus centros localizados en diferentes puntos de tal forma que la distancia entre ellos es mayor que el ancho de cada paquete). En general, las combinaciones lineales de estados coherentes

$$|\phi_+\rangle = N_+(z)\left[|z\rangle_c + |-z_c\rangle\right], \quad |\phi_-\rangle = N_-(z)\left[|z\rangle_c - |-z_c\rangle\right] \quad (19)$$

donde $N_\pm(z)$ es una constante de normalización, reciben el nombre de gatos de Schrödinger *positivo* y *negativo*, respectivamente.

La construcción de estados con paquetes de onda clásicos no es exclusiva de la radiación electromagnética. Estos también pueden obtenerse con superposiciones de los estados de vibración en moléculas o cristales [21], con corrientes eléctricas en un anillo superconductor [22] y en átomos dentro de trampas electromagnéticas (ver [23] y referencias allí citadas) o bien encerrados en una "botella láser" [8].

Como hemos visto, la interferencia de estados cuánticos es de vital importancia para las investigaciones y aplicaciones de los fenómenos del micromundo. Desafortunadamente, también es una limitante para hacer ingeniería cuántica [24] ya que no es posible aislar indefinidamente a los sistemas cuánticos y éstos, necesariamente, interactúan con su entorno. Es decir, tanto los estados coherentes de la luz como los gatos de Schrödinger intercambian fotones con los recipientes que los contienen. A esta interacción incontrolable de los sistemas con su entorno se le llama *decoherencia* y literalmente significa que los sistemas bajo estudio pierden la coherencia cuántica que los caracteriza. Esta es una de las principales limitantes para la realización de computadoras cuánticas o la teleportación cuántica, donde los estados coherentes tanto como los gatos de Schrödinger juegan un papel importante.

Los autores agradecen el apoyo secretarial de Miriam Lomelí. Este trabajo se realizó con financiamiento del Conacyt, proyecto 50766 .

[Referencias]

[1] E Hecht y A Zajac, *Optics* (Addison-Wesley, Menlo Park, California 1974).
[2] E Schrödinger, *Naturwissenschaften*, **14** (1926) 664.
[3] PAM Dirac, *Proc Roy Soc A* **114** (1927) 243.
[4] RJ Glauber, *Phys Rev Lett* **10** (1963) 84; *Phys Rev* **130** (1963) 2529; *ibid* 2766.
[5] RJ Glauber, en *Quantum Optics and Electronics*, Les Houches, eds. C DeWitt, A Blandin y C Cohen-Tannoudji (Gordon and Breach, New York 1965).
[6] O Rosas-Ortiz, "El premio Nobel de Física 2005", *Conversus* diciembre 2005-enero 2006, 75 pp; O Rosas-Ortiz, "Detrás de la magnetorresistencia gigante", *Conversus* diciembre 2007-enero 2008, 8 pp.
[7] E Schrödinger, *Naturwissenschaften* **23** (1935) 807. Traducción al inglés en referencia [20], 152 pp.
[8] C Monroe, DM Meekhof, BE King y DJ Wineland, *Science* **272** (1996) 1131.
[9] B Mielnik y O Rosas-Ortiz, "Quantum Mechanical Laws" en *Fundamentals of Physics*, editado por JL Morán-López, Encyclopedia Of Life Support Systems (EOLSS). Developed under the auspices of the UNESCO. Eolss Publishers, Oxford, U.K. [http://www.eolss.net].
[10] MO Scully y MS Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge 1997).
[11] C Cohen-Tannoudji, B Diu y F Laloë, *Quantum Mechanics*, vols. I y II (John Wiley & Sons, New York 1977); LE Ballentine, *Quantum Mechanics, A Modern Development* (World Scientific, Singapore 1998).
[12] JR Klauder y BS Skagerstan, *Coherent States. Aplications in Physics and Mathematical Physics* (World Scientific, Singapore 1985).
[13] A Perelomov, *Generalized coherent states and their applications* (Springer-Verlag, Berlin 1986).
[14] S Cruz y Cruz, S Kuru y J Negro, *Phys Lett A* **372** (2008), 1351.
[15] DJ Fernández C, V Hussin y LM Nieto, *J Phys A: Math Gen* **27** (1994) 3547; DJ Fernández C, LM Nieto y O Rosas-Ortiz, *J Phys A: Math Gen* **28** (1995) 2693; O Rosas-Ortiz *J Phys A: Math Gen* **29** (1996) 3821; DJ Fernández C y V. Hussin, *J Phys A: Math Gen* **32** (1999) 3603.
[16] DJ Fernández C, V Hussin y O Rosas-Ortiz, *J Phys A: Math Theor* **40** (2007) 3491.
[17] J Recamier, O Castaños, R Jáuregui y A Frank, *Phys Rev A* **61** (2000) 06308.
[18] G Loyola, M Moshinsky y A Szczepaniak, *Am J Phys* **57** (1989) 811.
[19] JA Wheeler y W Zurek (Editores), *Quantum Theory and Measurement* (Princeton University Press, Princeton, NJ 1983).
[20] A Whitaker, *Einstein, Bohr and the Quantum Dilema; From Quantum Theory to Quantum Information* (Cambridge University Press, Cambridge 2006).
[21] J Jansky, AV Vinogradov, T Kobayashi y Z Kis, *Phys Rev A* **50** (1994) 1777.
[22] A Leggett y A Garg, *Phys Rev Lett* **54** (1985) 857.
[23] O Castaños, R Jáuregui, R López-Peña, J Recamier y VI Manko, *Phys Rev A* **55** (1977) 1208.
[24] O Rosas-Ortiz, "Manipulando el mundo atómico: Ingeniería Cuántica", *Avance y Perspectiva* **23**, oct-dic de 2004, 19 pp; O Rosas-Ortiz "¿Computación Cuántica?", en M Santillán *et al.* (Editores), *Tendencias actuales de la Física en México*, Publicaciones del IPN (en imprenta).

[Notas]

1 Frase tomada del libro de Lewis Carroll, *Alice's adventures in wonderland & Through the looking-glass*, Signet Classic (U.S.A. 1960), p. 131 (traducción del inglés por los autores).
2 Se dice que ε representa el aporte de un fotón al campo eléctrico.
3 Los detalles de la definición matemática de $\Delta_\lambda Q$ y $\Delta_\lambda P$ en términos de vectores del tipo $|\lambda\rangle$, con λ alguna variable o parámetro tal como $\lambda = n$, no son necesarios para los intereses de este artículo. El lector interesado puede revisar la referencia [11] o cualquier otro texto contemporáneo de Mecánica Cuántica.
4 Lewis Carrol, *ibid*, p. 66.
5 Tomado de E. Schrödinger, referencia [7]; traducción del inglés por los autores.

Procesadores cuánticos atómicos

LA TEORÍA QUE DESCRIBE EL COMPORTAMIENTO DE ÁTOMOS AISLADOS, LA MECÁNICA CUÁNTICA, AHORA PROPORCIONA UN NUEVO PARADIGMA PARA LA COMPUTACIÓN. ACTUALMENTE, SU IMPLEMENTACIÓN EN ÁTOMOS ES UNA DE LAS ÁREAS MÁS PERSEGUIDAS EN FISICA ATÓMICA.

Eduardo Gómez García

Muchas veces se ha oído decir que las dos grandes revoluciones de la física del siglo pasado son la mecánica cuántica y la relatividad. Sin embargo, pareciera que estas revoluciones no han tenido gran impacto en nuestra vida cotidiana. En general es cierto que la mecánica cuántica aparece sólo de manera indirecta permitiéndonos construir mejores modelos de algún sistema. Una excepción notable es el láser. Las propiedades del láser, que lo hacen tan llamativo, como lo es el hecho de que viaje en línea recta casi sin deformarse, son evidencia directa de fenómenos cuánticos. Los efectos cuánticos tienden a desaparecer una vez que promediamos sobre un número grande de partículas. La observación de efectos cuánticos requiere, entonces, de sistemas puros y muy bien aislados.

Existen dos áreas de aplicación donde los principios de la mecánica cuántica pueden tener un impacto mucho más visible y directo; estas son las áreas de computación y comunicaciones. Algunas compañías de comunicaciones ofrecen sus servicios de transmisión segura de información utilizando tecnologías cuánticas. Dichas tecnologías son intrínsecamente más seguras ya que es imposible, en principio, extraer información de una de estas líneas de comunicación sin ser detectado o sin destruir la información. Asimismo, la computación cuántica ofrece algunas ventajas sobre su contraparte tradicional, aunque la tecnología aún permanece en la etapa de desarrollo y no ha alcanzado un nivel comercial.

En estos últimos años hemos presenciado una continua miniaturización de aparatos electrónicos. Fue reconocido por Feynman y otros que dicha miniaturización alcanzaría un punto en donde entraría en el dominio de la mecánica cuántica. En este dominio las reglas del juego son muy diferentes a lo que estamos acostumbrados en nuestra vida cotidiana y, por lo tanto, la electrónica digital, tal y como la conocemos hoy en día, dejaría de ser válida. Sin embargo, se observó que podemos utilizar estas nuevas reglas a nuestro favor, en cuanto que existen ciertos problemas que pueden resolverse de manera más eficiente utilizando a la mecánica cuántica. El

EDUARDO GÓMEZ GARCÍA Doctor en Física por la Universidad de Stony Brook en Nueva York (2005) con beca Fulbright-Conacyt. Realizó un postdoctorado en el Instituto Nacional de Estándares y Tecnología en Maryland. Profesor-investigador V del Instituto de Física de la Universidad Autónoma de San Luís Potosí. Pertenece al Sistema Nacional de Investigadores. Entre sus intereses de investigación se encuentran las mediciones de precisión en sistemas atómicos, en particular de la interacción entre átomos y superficies utilizando trampas de átomos ultra-fríos, y la medición de la fuerza nuclear débil mediante estudios de violación de paridad. Fue acreedor de la medalla Gabino Barreda durante su licenciatura, del President's Award por su trabajo doctoral y del premio Fanie and Nathaniel Sorroff 2004.
egomez@ifisica.uaslp.mx

ejemplo clásico es el problema de la factorización. Una computadora tradicional tardaría la edad del universo en factorizar un numero de mil dígitos, mientras que una computadora cuántica podría lograrlo en segundos. Debido a que los sistemas de encriptación más usados se basan en la dificultad de factorizar un número, la existencia de una computadora cuántica significaría el final de dicho método de encriptación.

Existen muchas posibilidades para la implementación de un procesador cuántico. Los distintos sistemas que se utilizan para ello, como lo son átomos, iones, fotones, squids, etcétera, comparativamente gozan de ventajas y desventajas pero, como aún no se ha declarado un ganador, la investigación ocurre de manera paralela en todos ellos. En este artículo se describe una implementación particular utilizando átomos para mostrar los detalles experimentales involucrados en este tipo de sistemas. En los átomos se observan efectos cuánticos de manera natural. De hecho, fue en átomos que se verificó de manera contundente la mecánica cuántica y de ahí su utilidad como procesadores.

Cualquier procesador disipa calor, por esto es que su computadora requiere de alguna manera de refrigeración (el ventilador en este caso). El caso de un procesador cuántico no es la excepción. La refrigeración de átomos es la mejor que existe, y es tan buena que se alcanzan temperaturas de tan sólo una millonésima de grado sobre el cero absoluto (ver recuadro 1). Cuando enfriamos un gas atómico a estas temperaturas algo mágico sucede: el sistema realiza un cambio de fase (similar al que se opera cuando el agua se solidifica en hielo) y un gran número de los átomos se condensa al nivel más bajo de energía formando un condensado de Bose-Einstein. En este estado todos los átomos del gas se comportan como si fueran un solo átomo grandote, de tal suerte que funcionan como un amplificador para efectos cuánticos.

Para evitar que los átomos se dispersen, es necesario mantenerlos atrapados. El problema es que, una vez que pongamos a los átomos en un recipiente, su temperatura se equilibrará con la del recipiente y, por tanto, la temperatura final estaría determinada por el recipiente. Las trampas de luz ofrecen una solución a este problema. La luz de un láser, con las características adecuadas, forma un contenedor de luz en donde se confinan a los átomos sin perturbarlos demasiado. La "temperatura" del contenedor de luz puede ser extremadamente baja si se minimizan las variaciones de intensidad y frecuencia del láser y, en este caso, no será el factor limitante de la temperatura mínima alcanzada.

Una configuración un tanto más elegante consiste en utilizar dos haces láser que se propagan en direcciones opuestas. Estos haces forman una onda estacionaria similar a la vibración de una cuerda en la guitarra. Los átomos "ven" a esta onda estacionaria como un potencial periódico sinusoidal, esto es, con mínimos (o valles) separados entre sí por una distancia igual a la mitad de la longitud de onda ($\lambda/2 \sim 0.5\ \mu m$) de la luz utilizada (el potencial es proporcional al campo eléctrico de la luz al cuadrado). Los mínimos funcionan como contenedores donde los átomos se acumulan. Para confinar en los tres ejes cartesianos, creamos potenciales similares también en la dirección "*y*" y "*z*". Una manera de visualizar el potencial generado es imaginar los átomos atrapados en los huecos de un cartón de huevo, colocados varios de éstos uno sobre otro. La figura 1 muestra el caso de uno de estos cartones de huevo, en donde intercambiamos cada huevo por un átomo.

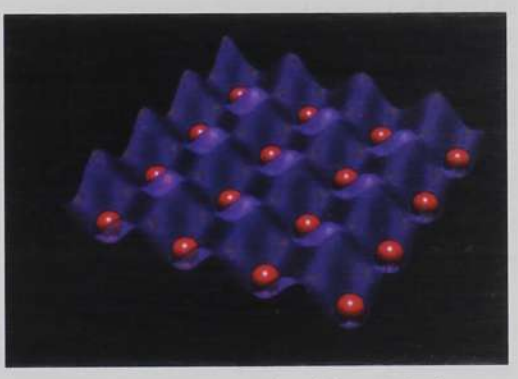

Figura 1. Potencial periódico generado por la intersección de pares de láseres retro-reflejados propagándose en direcciones perpendiculares. Cortesía de James Porto (NIST).

La figura 1 parece estar en violación de la termodinámica, ya que el estado presentado es un estado altamente ordenado. Generalmente, uno esperaría una distribución donde en algunos contenedores tengamos un átomo, en otros dos o más o ninguno. Esto es el caso cuando dejamos caer varias canicas sobre el cartón de huevo. Sin embargo la mecánica cuántica viene nuevamente a nuestro rescate, haciendo uso de una transición cuántica a un aislante de Mott. Imagine que empezamos con un cartón de huevo completamente aplastado y lo llenamos de agua. En este caso, el nivel del agua será el mismo en todas partes. Después procedemos a levantar las paredes del cartón de huevo, hasta llegar a la situación donde el agua está repartida en todos los contenedores. Si hacemos esto de manera lenta y gradual, vemos que la cantidad de agua en todos los contenedores es la misma. Lo mismo ocurre con los átomos: si introducimos el potencial periódico lentamente, entonces terminamos con un átomo en cada contenedor. Esto, gracias a que a estas bajas temperaturas el condensado se comporta como un superfluido (un líquido sin fricción).

Cada uno de los átomos corresponde entonces a un bit, pero no es un bit cualquiera, es un qbit (q de quantum). El qbit se forma utilizando dos niveles de energía del átomo. Si el átomo esta en uno de ellos decimos que el estado es **0**, y si esta en otro el estado es **1** (correspondientes al **0** y **1** de la electrónica digital). Para el caso cuántico, el átomo puede estar en una superposición arbitraria de **0** y **1**, y este hecho puede ser explotado para realizar en paralelo una multitud de operaciones. Es aquí donde las computadoras cuánticas pueden ser superiores a las clásicas para cierto tipo de problemas. Para que el procesador cuántico funcione se requieren varias condiciones. Primero, debemos ser capaces de preparar cualquier superposición en los átomos. Segundo, debemos ser capaces de medir con gran precisión en qué nivel se encuentran los átomos. Finalmente, el tiempo que dura esta superposición (tiempo de coherencia) debe ser mucho mayor que el tiempo que nos toma realizar una operación (menos de una milésima de segundo para una suma). Los átomos cumplen bastante bien con estas tres condiciones: podemos preparar superposiciones arbitrarias iluminando los átomos con microondas, podemos saber en qué nivel se encuentran los átomos iluminándolos con un láser y contando el número de fotones dispersados y, finalmente, los átomos pueden alcanzar tiempos de coherencia de segundos.

Una vez teniendo los qbits, nos gustaría realizar operaciones entre ellos. Desafortunadamente, en nuestro cartón de huevo tenemos a todos los átomos aislados y, por lo tanto, no interactúan entre sí. Nos gustaría poder modificar el cartón a manera de acercar dos átomos adyacentes para que interactuaran. Una configuración muy ingeniosa para lograrlo se muestra en la figura 2. En este caso, sustituimos los haces independientes en el eje "*x*" y "*y*" por un único haz retro-reflejado. En el cruce tenemos haces propagándose en direcciones opuestas en el eje "*x*" y "*y*", como teníamos anteriormente con la diferencia de que ahora provienen todos de un único haz. Añadimos a este haz dos moduladores electro-ópticos (EOM), un retardador y un polarizador. El modulador nos sirve para modificar la fase del haz láser, mientras que el retardador y polarizador afectan la polarización. Modificando estos tres elementos es posible controlar la forma del potencial periódico.

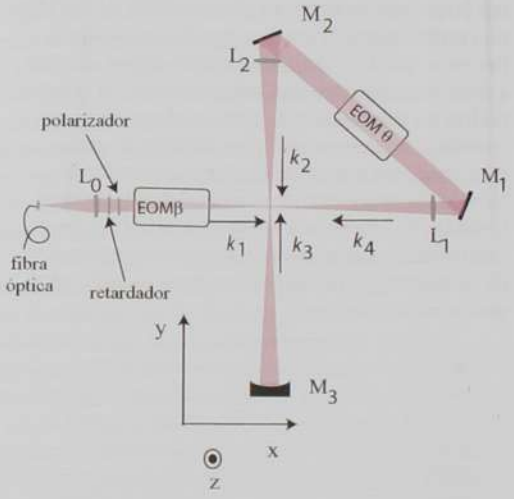

Figura 2. Configuración del láser en el plano "*xy*" capaz de cambiar continuamente entre un potencial con periodo λ/2 a un potencial con periodo λ. Cortesía de James Porto (NIST).

En estos últimos años hemos presenciado una continua miniaturización de aparatos electrónicos. R. P. Feynman predijo que esta miniaturización alcanzaría un punto en que entraría en el dominio de la mecánica cuántica y la electrónica digital, tal y como la conocemos hoy en día, dejaría de ser válida.

El potencial puede ser modificado continuamente de un potencial con separación entre contenedores igual a $\lambda/2$ a uno con separación igual a λ (figura 3). Dos de los átomos en el potencial tipo $\lambda/2$ van a dar a un solo contenedor en el potencial tipo λ. Así hacemos interactuar de manera controlada pares de átomos para realizar operaciones entre ellos. La energía de un átomo se ve modificada debido a la presencia del otro átomo. La magnitud del cambio depende del estado inicial de cada uno de los átomos, así como del tiempo que dure la interacción. Escogiendo de manera adecuada los estados iniciales y los tiempos de interacción se pueden implementar distintas operaciones entre los dos qbits. Una vez terminada la operación, transformamos el potencial de vuelta a uno del tipo $\lambda/2$ para poner los átomos en contenedores separados. Hecho esto, interrogamos de manera individual a cada uno de estos átomos sobre el nivel que ocupan o los hacemos interactuar con algún otro de sus vecinos.

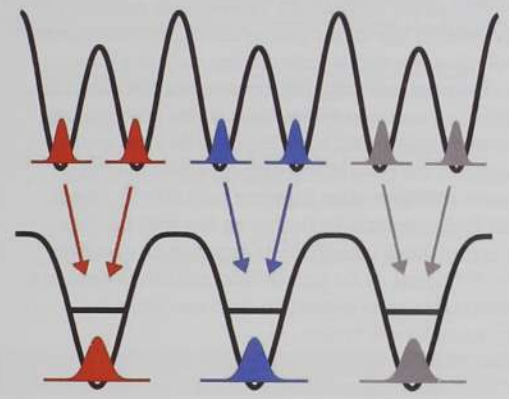

Figura 3. Transferencia de átomos de un potencial con periodo $\lambda/2$ a un potencial con periodo λ. Dos átomos del potencial original van a dar a un solo contenedor del nuevo potencial. Cortesía de James Porto (NIST).

La descripción presentada simplifica grandemente el proceso experimental real y esconde muchos de los detalles finos debajo del tapete. Cada uno de estos detalles requiere de trucos ingeniosos y una cuidadosa implementación. Poniéndolos todos juntos se ha logrado realizar la operación denominada $(\text{Intercambio})^{1/2}$ [1]. La operación Intercambio consiste en intercambiar el estado de los dos átomos, es decir, si el átomo **a** está en el estado **0** y el átomo **b** en el **1**, al final tendremos al átomo **a** (**b**) en el estado **1** (**0**) (ver recuadro 2). La operación $(\text{Intercambio})^{1/2}$ no tiene un equivalente clásico, pero corresponde a detener la operación Intercambio a medio camino [2]. En este caso, los átomos quedan en una superposición de las dos posibilidades para la asignación del estado de cada uno. El átomo **a** está en una superposición de **0** y **1** y el átomo **b** también, con ambas superposiciones relacionadas entre ellas (ver recuadro 2). Esta superposición es análoga a la descrita al principio excepto que ahora involucra a dos átomos. Estos dos átomos quedan enredados y ya no es posible considerarlos como dos entidades separadas. Cualquier medición hecha sobre uno de los átomos modifica el estado del otro átomo.

Se sabe que combinando una operación $(\text{Intercambio})^{1/2}$ con operaciones de un solo qbit (que son posibles en átomos) se puede realizar cualquier operación arbitraria, es decir, estas dos operaciones forman un conjunto de operaciones universales. ¿Quiere decir esto que ya tenemos una computadora cuántica? Sí, la tenemos en el sentido de que podemos realizar operaciones muy sencillas, pero este procesador aún esta muy lejos de ser capaz de resolver problemas de importancia práctica. Para llegar hasta ese punto se necesita, entre otros requerimientos, incrementar la eficiencia del procesador para evitar lo más posible los errores en el cálculo, aumentar su tamaño para que realice decenas de miles de operaciones diferentes y transportar información de un lado al otro del mismo. Cada uno de estos puntos exige aún varios años de investigación.

Un simulador cuántico, pariente cercano a la computadora cuántica, es capaz de determinar el estado en el que se encuentra una estrella de neutrones.

Una persona con experiencia en programación puede resolver las ecuaciones cuánticas de un sistema dado, por ejemplo, de un átomo. Este es un problema muy demandante desde el punto de vista computacional, en tanto que requerimos de gran poder de cómputo para resolverlo. El problema se vuelve aún más complicado cuando consideramos no uno sino varios átomos, de tal modo que el tiempo que tardaríamos en resolver el problema sería demasiado largo. En los comienzos de la computación cuántica se propuso que se podría utilizar un sistema cuántico para modelar otro sistema cuántico y de ese modo entender el comportamiento del sistema. Dicho aparato es un pariente cercano a la computadora cuántica y se le llama un simulador cuántico.

Entre los problemas que pueden ser resueltos por un simulador cuántico está la determinación del estado en el que se encuentra una estrella de neutrones. Los neutrones son partículas sin carga que forman parte de los núcleos. A los neutrones, como a cualquier otra partícula fermiónica, no les gusta compartir su estado con nadie más, de tal modo que no se puede encontrar a dos de ellos en el mismo estado ocupando el mismo lugar. Los neutrones en este tipo de estrellas se encuentran comprimidos a gran densidad debido a la atracción gravitacional, pero no continúan comprimiéndose puesto que no se enciman, como buenos fermiones. Resulta que este es un problema increíblemente complicado para resolverse por la vía computacional, no obstante, podemos simular el estado de dicha estrella utilizando átomos fríos. Al emplear átomos fermiónicos como ^{40}K en una trampa óptica podemos obtener información sobre el comportamiento de las estrellas. La densidad en la trampa es mucho menor que la de la estrella, sin embargo se puede compensar si incrementamos enormemente la fuerza de interacción en el caso de los átomos. Esto está dentro de los trucos con los que contamos en física atómica. No sólo podemos poner pares de átomos a interactuar de manera controlada, sino que también podemos modificar la fuerza de interacción con sólo cambiar el campo magnético. La fuerza va desde fuertemente atractiva hasta fuertemente repulsiva y todas las intensidades intermedias, incluyendo fuerza cero. Algunos de estos simuladores ya existen en la actualidad y comienzan a aportar información a otras áreas donde el cómputo teórico no existe.

Los beneficios que promete la obtención de una computadora cuántica explican el incremento de la investigación en esta área a nivel mundial. Existe una multitud de grupos e inclusive centros de investigación dedicados a resolver este problema. En México hay varios grupos trabajando en aspectos relacionados con la información cuántica y, como lo muestra este volumen, comienza a formarse un esfuerzo coordinado para atacar este problema de manera más sistemática. Algunos de estos grupos enfocan sus esfuerzos al estudio experimental de gases atómicos ultra fríos (ver recuadro 3). Aun si las computadoras cuánticas no llegaran nunca a tener utilidad comercial, la experiencia obtenida en el control de las propiedades cuánticas resultará invaluable en el desarrollo de lo que serán las tecnologías del futuro . ●

Una computadora tradicional tardaría la edad del Universo en factorizar un número de mil dígitos, mientras que una computadora cuántica podría lograrlo en segundos. Los beneficios que promete la obtención de este tipo de computadoras explica el incremento mundial de la investigación en esta área. En México ya hay varios grupos de científicos trabajando en ese reto.

Recuadro 1. Enfriado atómico

La mayoría de los experimentos en átomos ultra fríos utilizan dos técnicas para el enfriado de átomos: las trampas magneto-ópticas y la evaporación. Las trampas magneto-ópticas emplean una combinación de láseres y campos magnéticos para capturar y enfriar átomos. Los átomos son bombardeados constantemente por los fotones del láser, lo cual va disminuyendo su velocidad. Esto equivale a querer detener un coche aventándole piedras. Así como en el caso del coche se requieren muchas pedradas para detenerlo, en el caso del átomo se requieren muchos fotones, pero esto no es problema ya que contamos con láseres de potencia suficiente. El campo magnético ayuda a que todos los átomos se acumulen en el lugar donde el campo magnético es cero; de esta manera enfriamos y atrapamos los átomos. En la trampa, los átomos no quedan completamente inmóviles; después de todo, estamos apedreándolos continuamente. Para reducir la temperatura todavía más utilizamos el proceso de evaporación. Si dejamos escapar los átomos más calientes en la trampa, entonces los que quedan tendrán una temperatura más baja. Iterando este proceso varias veces se alcanzan temperaturas por debajo de una millonésima de grado sobre el cero absoluto.

Recuadro 2. Tabla de verdad de las operaciones Intercambio e (Intercambio)1/2

La siguiente tabla describe el estado final después de la aplicación de las operaciones Intercambio e (Intercambio)$^{1/2}$ dependiendo del estado inicial. Esta tabla es equivalente a las tablas de verdad utilizadas en electrónica, excepto que no existe análogo clásico para algunos de los estados finales.

Estado inicial	Estado final (Intercambio)	Estado final (Intercambio)$^{1/2}$
$\|0_a,0_b\rangle$	$e^{i\pi/4}\|0_a,0_b\rangle$	$\|0_a,0_b\rangle$
$\|0_a,1_b\rangle$	$(\|0_a,1_b\rangle - i\|1_a,0_b\rangle)/2^{1/2}$	$\|1_a,0_b\rangle$
$\|1_a,0_b\rangle$	$(-i\|0_a,1_b\rangle + \|1_a,0_b\rangle)/2^{1/2}$	$\|0_a,1_b\rangle$
$\|1_a,1_b\rangle$	$e^{i\pi/4}\|1_a,1_b\rangle$	$\|1_a,1_b\rangle$

Recuadro 3. Investigación experimental en gases atómicos ultra fríos en México

Las tecnologías de enfriado atómico láser son relativamente recientes. México apenas está empezando a desarrollarlas por lo que existen pocos centros donde se realiza este tipo de investigación. El Centro Nacional de Metrología (Cenam) cuenta con la única trampa magneto-óptica funcional actualmente. La trampa se usa para el desarrollo de patrones de tiempo y la definición del segundo [3]. Existen otras dos trampas magneto-ópticas en construcción: la primera, en el Instituto de Ciencias Nucleares de la UNAM, se dedicará al estudio de átomos de Rydberg, que son átomos en niveles altamente excitados [4]; la segunda, en el Instituto de Física de la UASLP, servirá para la medición de la fuerza de Casimir-Polder, que es una fuerza de origen cuántico que aparece entre un átomo y una superficie [5]. Esta última servirá también de paso intermedio para la construcción de un condensado de Bose-Einstein, que permitirá estudiar, entre otros casos, los procesos que limitan el tiempo que duran las superposiciones cuánticas (tiempo de coherencia).

[Referencias]

1. M. Anderlini, P.J. Lee, B.L. Brown, J. Sebby-Strabley, W.D. Phillips, J.V. Porto, 2007, Controlled exchange interaction between pairs of neutral atoms in an optical lattice, en *Nature*, vol. 448, núm. 7152, pp. 452-456.
2. Una animación de la operación antes descrita se encuentra en zhttp://www.nist.gov/public_affairs/releases/quantum_gate.html
3. http://www.cenam.mx
4. http://www.nuclecu.unam.mx/
5. http://www.ifisica.uaslp.mx/%7Egomez/indexsp.html

Autoensamblado de puntos cuánticos semiconductores

LA DENSIDAD DE ESTADOS DISCRETA DE LOS PUNTOS CUÁNTICOS SEMICONDUCTORES (PCS) ABRE LA POSIBILIDAD DE APLICACIONES NOVEDOSAS, QUE VAN DESDE LA FABRICACIÓN DE LÁSERES DE ALTO RENDIMIENTO PARA LA OPTOELECTRÓNICA HASTA LA PRODUCCIÓN DE QUBITS PARA LA COMPUTACIÓN CUÁNTICA. SIN EMBARGO, LA REALIZACIÓN EXITOSA DE COMPUTACIÓN CUÁNTICA EMPLEANDO PCS AÚN PLANTEA GRANDES RETOS A LA FÍSICA EXPERIMENTAL.

Máximo López-López
Víctor Hugo Méndez-García

La computación cuántica es un campo emergente y de intenso crecimiento que combina la ciencia computacional con la mecánica cuántica. La unidad fundamental de información en una computadora cuántica (QC) es el bit cuántico (qubit). Un qubit puede verse como un sistema de dos estados, por ejemplo, los estados electrónicos ½ de espín, o un par de niveles de un átomo. A diferencia de los bits clásicos, los cuales únicamente toman valores 0 ó 1, el qubit se basa en la habilidad adicional de los sistemas cuánticos de encontrarse en una superposición de los estados. Así, para la realización de cómputo cuántico debemos tener las siguientes condiciones básicas: 1) un sistema de dos niveles (**0** y **1**); 2) la habilidad de preparar al qubit en cualquiera de los estados; 3) la capacidad de medir cada qubit; 4) la capacidad de construir operaciones básicas de compuerta; 5) tiempos de coherencia suficientemente grandes, y 6) densidad suficiente de unidades de memoria o qubits. Precisamente, las tecnologías de estado sólido parecen ser las más prometedoras para satisfacer los requerimientos anteriores mediante el empleo de nanoestructuras semiconductoras con cero dimensiones o puntos cuánticos (PCs). El estado base y el primer estado excitado en un PC se pueden utilizar como los estados **0** y **1** del qubit. También se pueden aplicar pulsos electromagnéticos para manipular los estados en los PCs. Adicionalmente se pueden usar campos eléctricos estáticos cerca de un PC, que actúen como compuerta y/o modifiquen los tiempos de coherencia. De manera sencilla podemos entender

MÁXIMO LÓPEZ-LÓPEZ Doctor en Ciencias por la Universidad Tecnologica de Toyohashi, Japón (1992). Investigador **Cinvestav** 3D adscrito al Departamento de Física. Fue jefe de la Sección de Física del Estado Sólido (2000-2004). Pertenece al Sistema Nacional de Investigadores (nivel III). Entre sus intereses de investigación se encuentra el desarrollo de materiales semiconductores nanoestructurados, sistemas de baja dimensionalidad y el crecimiento por epitaxia de haces moleculares (MBE). Ha dirigido 4 tesis de licenciatura, 13 maestría y 7 de doctorado. Premio de investigación 2003 de la Academia Mexicana de Ciencias en el área de ingeniería y tecnología.
mlopez@fis.cinvestav.mx

VÍCTOR HUGO MÉNDEZ-GARCÍA Doctor en Ciencias por el Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional (1999). Profesor investigador nivel VI adscrito a la Facultad de Ingeniería, comisionado al Instituto de Investigación en Comunicación Óptica de la Universidad Autónoma de San Luis Potosí (SLP). Funge como responsable del Laboratorio de Nanoestructuras Luminiscentes. Pertenece al Sistema Nacional de Investigadores. Líneas de investigación: crecimiento y caracterización de nanoestructuras semiconductoras, heteroestructuras láser y dispositivos de efecto Hall cuántico. Es miembro activo de la Mesa Directiva de la Sociedad Mexicana de Ciencia y Tecnología de Superficies y Materiales. Ha dirigido tesis de licenciatura, maestría y doctorado en ciencias aplicadas.
vmendez@cactus.iico.uaslp.mx

El término *punto cuántico* se utiliza, generalmente, para describir un nanocristal (en nuestro caso de un material semiconductor) con confinamiento cuántico en las tres dimensiones espaciales. Las fronteras físicas de los PCs confinan a los portadores de carga dentro del material. Este confinamiento da lugar a propiedades inusuales que no se manifiestan en materiales en forma de bulto o tamaños macroscópicos.

por tiempo de coherencia como el tiempo durante el cual una QC puede permanecer realizando un cómputo. Pequeñas perturbaciones al sistema cuántico e interacciones con el medio ambiente pueden ocasionar que el tiempo de coherencia disminuya y el proceso de cómputo colapse.

Antes de que los PCs emerjan como una tecnología triunfante en la construcción de QCs deben superarse varios obstáculos. Algunos de ellos son la fabricación de PCs semiconductores de alta calidad cristalina, uniformemente espaciados y de dispersión mínima en su geometría. Si bien con el uso de técnicas de crecimiento modernas, como la epitaxia de haces moleculares y el modo de crecimiento de Stransky-Krastanov, se sintetizan rutinariamente PCs de InAs sobre GaAs, es además necesario optimizar los parámetros de crecimiento a fin de obtener la máxima calidad cristalina, el mejor nivel de confinamiento electrónico, así como la menor dispersión en el tamaño de los PCs, características deseables para su uso en QCs.

En este artículo exponemos un panorama general de la investigación en PCs y su aplicación a la QC. Presentamos nuestros estudios sobre la dependencia del tamaño y la fotoluminiscencia de los puntos cuánticos auto-ensamblados de InAs con las condiciones de crecimiento y proponemos tratamientos térmicos *in situ* que homogenicen la geometría de los PCs.

Puntos cuánticos autoensamblados

El término punto cuántico se utiliza generalmente para describir un nanocristal (en nuestro caso de un material semiconductor) con confinamiento cuántico en las tres dimensiones espaciales. Las fronteras físicas de los PCs confinan a los portadores de carga dentro del material. Este confinamiento da lugar a propiedades inusuales que no se manifiestan en materiales en forma de bulto (o tamaños macroscópicos). Por ejemplo, el silicio, que es generalmente un pobre emisor de luz en su forma de bulto porque su estructura de bandas de energía es indirecta, se vuelve un buen emisor de luz cuando se le confina en forma de PCs [1]. El confinamiento de los portadores de carga se puede ajustar variando el tamaño de los PCs, lo cual afecta algunas propiedades fundamentales del material.

Una medida del tamaño del nanocristal requerido para observar efectos cuánticos es la longitud de onda de Broglie de los portadores de carga dentro del material huésped, que es típicamente del orden de algunas decenas de nanómetros [2]. Si consideramos PCs esféricos con un diámetro (D), el nivel de confinamiento se puede caracterizar por su relación al radio de Bohr (a_B) del excitón (par electrón-hueco ligados electrostáticamente). El confinamiento fuerte ocurre cuando $D < 2a_B$, confinamiento intermedio cuando $D \sim 2a_B$, y el confinamiento se considera débil cuando $D > 2a_B$.

Los PCs se pueden preparar usando varias técnicas incluyendo las siguientes: litografía, epitaxia de haces moleculares y métodos coloidales. Todos estos métodos comparten la característica común de que el PC es delimitado con un material distinto como frontera. Hay otros métodos para crear los PCs donde bloqueos o trampas eléctricas se utilizan para añadir confinamiento a electrones de un gas bidimensional dentro de un pozo cuántico. En cualquiera de estos casos, los sistemas electrónicos contenidos dentro de los PCs se aíslan mejor del ambiente y tienen menores grados de libertad internos que otros sistemas con más dimensiones. Ambas características son útiles para aumentar los tiempos de coherencia de los estados del qubit codificados dentro del punto y, por lo tanto, se ha desarrollado gran interés en los usos potenciales que tienen los PCs para computación cuántica de estado sólido. El uso de puntos cuánticos autoensamblados es preferible ya que evita emplear técnicas costosas para delimitar estas nanoestructuras; adicionalmente, no hay daño a los PCs durante su

fabricación ya que todo el proceso se realiza durante el crecimiento de los materiales. Sin embargo, para lograr buenos resultados en la aplicación de PCs autoensamblados deben satisfacerse requerimientos estrictos en cuanto a la uniformidad en el tamaño, forma y densidad. Esto nos lleva al estudio de la cinética del crecimiento de los PCs autoensamblados. El mecanismo más avanzado para la construcción de estas estructuras a escala nanométrica es por epitaxia de haces moleculares (MBE, *molecular beam epitaxy*) en el modo de crecimiento de Stranski-Krastanov. A continuación presentaremos los fundamentos básicos de la técnica de MBE.

Epitaxia de haces moleculares

Una de las técnicas de crecimiento más poderosas para lograr la síntesis de PCs es la epitaxia por haces moleculares (MBE, *molecular beam epitaxy*). Esta técnica fue inicialmente desarrollada por J. R. Arthur y A. Y. Cho de los laboratorios Bell para el crecimiento de GaAs y heteroestructuras GaAs/AlGaAs. Ha sido subsecuentemente extendida a una gran variedad de materiales manteniendo ventajas sobre otras técnicas de crecimiento de películas epitaxiales. Estas ventajas incluyen la capacidad de controlar la reproducibilidad del crecimiento en dimensiones menores a monocapas atómicas y la posibilidad de monitorear el crecimiento *in situ* y a tiempo real. Debido al ambiente de ultra alto vacío que se usa en los sistemas MBE, es posible estudiar la dinámica de los propios procesos de crecimiento usando técnicas como reflexión de electrones difractados de alta energía (RHEED: *reflection high-energy electron diffraction*). Además, otras técnicas *in situ* tales como espectroscopía de reflectancia diferencial (RDS, *reflectance difference spectroscopy*) pueden emplearse para examinar la superficie de la muestra en crecimiento. En esencia, la técnica MBE es más que un método de evaporación basado en ultra alto vacío. En la práctica es una técnica de depósito capaz de obtener materiales con un nivel de impurezas por debajo de diez partes por billón de una manera reproducible, con un control sin precedente sobre la composición, el dopaje de las estructuras y sobre el espesor a escala nanométrica.

La figura 1 muestra el esquema de la cámara de crecimiento de un sistema MBE. En la técnica de MBE, los elementos constituyentes del material a crecer son propulsados en forma de haces moleculares hacia un substrato cristalino sobre el cual se formará la película epitaxial en crecimiento. Estos haces emergen al evaporar térmicamente fuentes sólidas elementales de muy alta pureza, contenidas en crisoles (contenedores) ubicados dentro de celdas situadas frente al substrato. En sistemas MBE de elementos III-V las celdas contienen materiales sólidos de alta pureza de Al, Ga, As, Be, In y Si. En algunos sistemas suelen utilizarse fuentes de gases, como el nitrógeno o hidrógeno. Las cámaras de crecimiento se mantienen en un ambiente de ultra alto vacío (UAV), a una presión del orden de 10^{-11} torr, que nos garantiza la pureza del material en las fuentes. Rodeando las celdas, sobre las paredes internas de la cámara, se localizan criopaneles; al mantenerlos a temperatura de nitrógeno líquido, éstos se convierten en medios efectivos para el atrapamiento de impurezas. Frente a las celdas, justamente en el centro de la cámara, se encuentra el substrato montado sobre un porta-substrato de molibdeno (*moliblock*), sujeto a su vez a un mecanismo manipulador que le permite rotar con respecto a la normal del substrato. Durante el crecimiento, este movimiento ayuda a homogeneizar el crecimiento de la película. En la parte posterior del *moliblock* se encuentra un medidor de ionización tipo Bayard-Alpert, con el cual se calibran los flujos y, por lo tanto, es un componente indispensable para el control del crecimiento. La manipulación del substrato dentro de la cámara de crecimiento nos permite utilizar técnicas de caracterización *in situ* tales como RHEED. En esta técnica, un haz de electrones de alta energía se dirige sobre la superficie de la muestra a un ángulo razante. A consecuencia de la interacción con la red cristalina del sustrato, en el otro extremo, en una pantalla fosforescente, se forma un patrón de difracción que nos brinda información acerca de la calidad cristalina del depósito y la cinética del crecimiento.

Las características anteriores del sistema de MBE y sus herramientas de análisis permiten la obtención de nanoestructuras semiconductoras de muy alta calidad cristalina. En particular, para la síntesis de puntos cuánticos semiconductores se toma ventaja del modo de crecimiento Stransky-Krastanov.

Antes de que los puntos cuánticos semiconductores (PCs) emerjan como una tecnología triunfante en la construcción de computadoras cuánticas, deben superarse varios obstáculos. Algunos de ellos son la fabricación de PCs semiconductores de alta calidad cristalina, uniformemente espaciados y de dispersión mínima en su geometría.

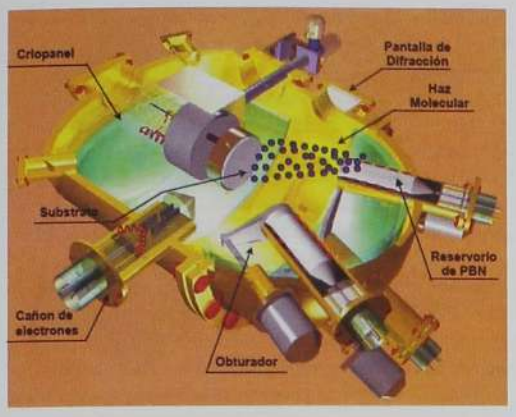

Figura 1. Diagrama esquemático de la cámara de crecimiento de un sistema MBE III-V.

Modo de crecimiento Stransky-Krastanov

La obtención de PCs autoensamblados mediante el modo de crecimiento de Stransky-Krastanov (S-K) se basa en la relajación de energía elástica producida por la diferencia en constantes de red del material a depositar y el substrato. Ilustraremos este modo de crecimiento tomando como ejemplo el crecimiento de InAs sobre GaAs. Estos cristales poseen diferente constante de red, 6.05Å del InAs y 5.65Å del GaAs, lo cual conduce a un desacople de redes de aproximadamente 7%. En las etapas iniciales del depósito de InAs, éste crece acoplado a la red cristalina del substrato GaAs, como se ilustra en la figura 2(a). A esta primera capa que cubre toda la superficie del substrato se le conoce como *capa de mojado*. Sin embargo, los esfuerzos debidos al desajuste de los parámetros de red provocan la deformación elástica del InAs acumulando energía elástica conforme avanza el crecimiento. A esta etapa del crecimiento se le denomina *régimen pseudomórfico*. Con el aumento del volumen de InAs depositado, la energía elástica se va acumulando. Esta situación persiste hasta alcanzar un determinado espesor, denominado espesor crítico, para el que la energía acumulada se libera mediante la formación espontánea (o autoensamble) de nanoislas tridimensionales coherentes (figura 2(b)), es decir, islas de InAs libres de defectos cristalinos. Este mecanismo de autoensamble de nanoestructuras 0-dimensionales permite la síntesis de miles de millones ($10^{10}/cm^2$) de PCs con diámetro entre 1 y 10 nanómetros con un alto grado de uniformidad en un único paso de crecimiento. Los puntos pueden ser inmediatamente cubiertos por una segunda capa del material sustrato, configurando de esta manera un nano-material con una alta calidad óptica, el cual puede ser utilizado en la generación de excitones con aplicaciones a QC, como se describe a continuación.

Figura 2. (a) Ilustración del régimen de crecimiento pseudomórfico y (b) la posterior formación de nano-islas durante el modo de crecimiento Stransky-Krastanov.

Aplicación a computación cuántica

Cuando se bombean fotones a un semiconductor, los electrones de la banda de valencia se excitan a la banda de conducción dejando huecos (portadores de carga positiva) en la banda de la valencia. La interacción coulombiana de los electrones con los huecos da lugar a pares enlazados electrón-hueco que, como mencionamos anteriormente, se conocen como excitones. Un sistema de QC puede llevarse a cabo usando los excitones localizados en PCs como excitaciones elementales que representen los binarios lógicos: lógica uno (cero) corresponde a la presencia (ausencia) de un excitón en un PC. Funciones de compuerta se pueden introducir mediante radiación electromagnética coherente (un pulso de láser, por ejemplo). Este análisis se basa en el sistema físico simple propuesto por H. Kamada [3], donde un arreglo lineal de PCs colocado entre dos electrodos de metal se excita mediante un láser, como se observa en la figura 3. Este arreglo lineal se puede obtener creciendo los PCs sobre sustratos con direcciones cristalinas específicas [4]. Las compuertas lógicas cuánticas se realizan excitando los PCs con láseres de diferentes longitudes de onda. Dado que en cualquier sistema real siempre habrá cierta dispersión en el tamaño de los PCs, esto hace posible excitar PCs individualmente, pues cada PC tendrá los niveles cuantizados a diferentes energías. Así pues, empleando un láser sintonizable se puede producir una resonancia sólo en un PC individual. La manipulación rápida de los qubits se hace posible induciendo una evolución temporal unitaria con pulsos de laseres de pico o femto segundos. La lectura en el PC puede lograrse posicionando los haces de los láseres de excitación y de prueba en un lugar específico, en donde un número de qubits con diversas frecuencias excitónicas puedan ser accesibles [3]. Las operaciones de compuerta condicionales de dos qubits se pueden dar vía la interacción dipolo-dipolo en dos PCs adyacentes. Aplicando un campo eléctrico entre los electrodos la interacción dipolo-dipolo se puede modular para modificar el acoplamiento entre dos qubits [5].

Cabe mencionar que, además del mecanismo anterior basado en excitones, el cual exige nanoestructuras de alta calidad óptica, se está realizando investigación en el uso, por ejemplo, de los

estados de espín confinados en PCs [6]. Nuestro estudio está dirigido a la optimización del crecimiento de los PCs, cualquiera que sea el método que se emplee posteriormente para implementarlos en una QC.

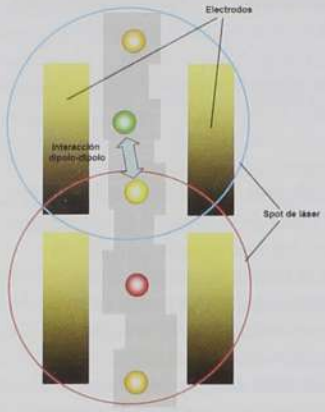

Figura 3. Arreglo lineal de PCs para el cómputo todo-óptico. PCs individuales son excitados y reconocidos mediante la focalización de láseres en posiciones específicas. La distribución estadística de las características de los PC permite identificar un excitón en un PC particular mediante discriminación de frecuencia [3].

Optimización del autoensamblado de PCs

A continuación se comentan los resultados de un experimento orientado a la optimización del crecimiento de PCs autoensamblados de InAs sobre sustratos de GaAs, empleando la técnica de MBE en el modo de crecimiento Stransky-Krastanov.

Como se mencionó anteriormente, una dificultad a resolver en este modo de crecimiento es la dispersión en tamaños de los PCs. Con el propósito de mejorar la distribución en tamaños de los PCs se ha propuesto una variedad de métodos. Nuestra aproximación es someter la superficie del GaAs previo al depósito de InAs a un proceso de recocido *in situ* a altas temperaturas durante un intervalo de tiempo corto, en el cual no exista flujo de la fuente de As sobre la superficie del GaAs. El propósito de este tratamiento es cambiar el estado químico y físico del GaAs previo al depósito del InAs [7].

La figura 4(a) muestra una imagen de microscopía de fuerza atómica (MFA) de PCs obtenidos mediante el depósito, de manera convencional, de 2.1 monocapas (MCs) de InAs (1 MC – 0.3 nm) sobre una superficie de GaAs (muestra A21 sin tratamiento). El tamaño del barrido en la imagen es de 500×500 nm^2 y la escala vertical es de 10 nm. Los PCs presentan una densidad de 15×10^{10} cm^{-2} y una gran dispersión de tamaños, lo cual es característico del modo de crecimiento S-K. Por el contrario, la figura 4(b) muestra una imagen de MFA para una muestra sometida al tratamiento térmico *in situ*, descrito anteriormente (muestra B21), y a la cual se le depositó posteriormente la misma cantidad de 2.1 MC de InAs. Sin embargo, como se puede apreciar en la imagen, la superficie es plana y no presenta la formación de PCs. Es claro que el proceso de recocido *in situ* cambió considerablemente el estado físico-químico de la superficie, dado que después del depósito de las 2.1 MCs de InAs el crecimiento permanece pseudomórfico sin el uso de surfactantes y bajo condiciones estables de As. En la figura 4(c) presentamos la imagen de MFA para una muestra (A34) que se preparó de manera convencional (sin recocido) con un mayor depósito equivalente a 3.4 MC de InAs. En esta muestra observamos la coalescencia de los PCs y la formación de islas de mucho mayor tamaño. Por otro lado, el depósito de 3.4 MC de InAs sobre una superficie de GaAs recocida *in situ* (muestra B34) sí presentó la formación de PCs, como se puede observar en la figura 4(d). Aunque los PCs parecen estar aún distribuidos aleatoriamente, hay una mayor uniformidad en sus tamaños así como mayores dimensiones que los PCs obtenidos convencionalmente. Los PC en la muestra B34 exhiben una densidad en torno a 5×10^{10} cm^2. Obviamente, esta nueva morfología de los PCs es resultado del proceso de recocido al cual se sometió la superficie de GaAs, puesto que, en general, la formación de los PCs está fuertemente influenciada por las etapas tempranas del crecimiento.

Un análisis cuantitativo de la topología superficial se encuentra en la figura 5, que presenta histogramas de altura de los PCs en las cuatro muestras de la figura 4. Estos resultados reflejan tanto la superficie plana obtenida para la muestra B21 como las nanoislas de mayor tamaño que se observan en la muestra A34. Notamos la fuerte dispersión en tamaños para esta muestra, que contrasta con la disminución en dispersión observada en la muestra B34. Estos cambios en la morfología de los PCs afectan sus propiedades ópticas. Una técnica muy usada para evaluar la calidad óptica de PCs es la espectroscopía de fotoluminiscencia (FL). Espectros de FL tomados a una temperatura de 14 K se presentan en la figura 6 para las muestras A21 y B34. En estos espectros los picos de FL se localizan a las energías de 1.03 y 0.93 eV para las muestras A21 y B34, respectivamente.

La obtención de PCs autoensamblados mediante el modo de crecimiento de Stransky-Krastanov se basa en la relajación de energía elástica producida por la diferencia en constantes de red del material a depositar y el substrato.

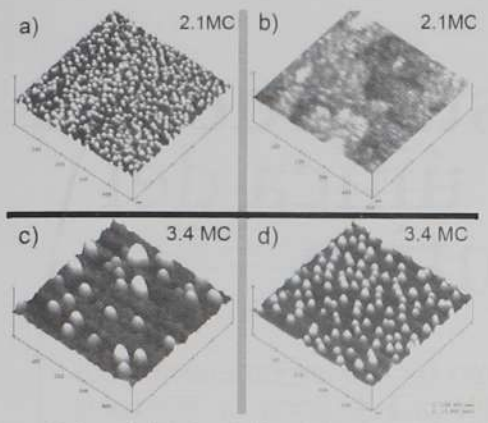

Figura 4. Imágenes de MFA después del crecimiento de InAs: a) y c) sobre superficies de GaAs sin tratamiento; b) y d) sobre superficies de GaAs recocidas *in situ*. El espesor equivalente de InAs para cada una de las muestras se indica en la figura.

No se obtuvo señal de FL en esta región espectral para las otras muestras; esto se debe a que en la muestra B21 no se observaron PCs y las islas de la muestra A34 son demasiado grandes. Por lo tanto, en la siguiente discusión nos centramos en las muestras A21 y B34. Realizando una estadística de los tamaños de los PCs en estas muestras obtuvimos los siguientes resultados: los PCs obtenidos del crecimiento de manera convencional tienen una altura promedio de 2.1 ± 1 nm y diámetro de 12 ± 3.1 nm, mientras que los PCs crecidos sobre GaAs recocido tienen una altura promedio de 5.9 ± 0.5 nm y diámetros de 25 ± 2.5 nm. Se observa que la fuerte dispersión en diámetro y altura de los PCs en la muestra A21 disminuyó a menos 10% para la muestra B34.

Las mejorías anteriores en la dispersión de tamaños de los PC se reflejan en su emisión de FL. En la figura 6 observamos una disminución en el ancho del espectro de emisión de la muestra B34 como consecuencia de la mayor uniformidad en los tamaños de los PCs. Respecto a la posición en energía de los espectros de FL notamos que el aumento en los tamaños de los PCs (menor confinamiento cuántico) concuerda con el corrimiento hacia el rojo observado para la muestra B34. Mas aún, en otros experimentos encontramos que la magnitud del corrimiento al rojo depende tanto del tiempo de recocido a alta temperatura como de la cantidad de InAs depositado.

Adicionalmente, la presión de arsénico y la temperatura de crecimiento de los PCs son parámetros que se pueden variar para controlar el pico de emisión de los PCs [8]. La posibilidad de manipulación de la emisión de los PCs tiene importantes ventajas para aplicaciones en QC y en una variedad de dispositivos optoelectrónicos novedosos.

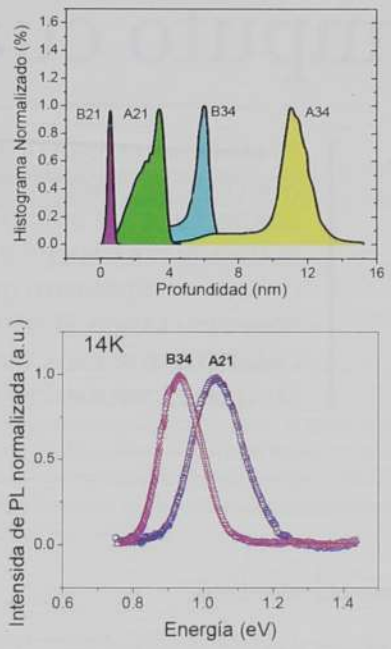

Figura 6. Espectros de fotoluminiscencia a 14 K de los PCs en las muestras A21 y B34.

Se puede concluir que las propiedades físicas intrínsecas a los puntos cuánticos hacen que estos sistemas sean fuertes candidatos para la realización de computación cuántica. La fabricación de estas nanoestructuras mediante un proceso de autoensamblado empleando la técnica de MBE tiene grandes ventajas sobre otros métodos, principalmente debido a que los puntos cuánticos se forman sin necesidad de procesamientos externos. Sin embargo, aún se requiere de investigación sobre los procesos de autoensamblado para lograr tener un control adecuado del tamaño, densidad y forma de los PCs. ●

[Referencias]

[1] Pavesa L., Dal Negro L., Mazzoleni C., Franzo G. y Priolo F. Optical gain in silicon nanocrystals. *Nature*, 408:440-444 (2000).
[2] Kouwenhoven L.P. *et al.* Mesocopic Electron Transport. NATO Science Series, vol. 345. Proceeding of the NATO Advanced Study Institute (1996).
[3] Kamada H. Quantum computating with QD excitons. *NTT Tech. Rev.*, 1:31-40 (2003).
[4] López-López M., Cruz-Hernández E., Martínez-Velis I., Rojas-Ramírez J., Ramírez-López M., Pulzara-Mora A. y Hernandez-Rosas J. Self-Assembly of Nanostructures on (631)-Oriented GaAs Substrates. Advanced Summer School in Physics 2007, AIP Conference Proceedings, vol. 960, pp. 210-215 (2007).
[5] Biolatti E., Iotti R.C., Zanardi P. y Rossi F. Quantum Information Processing with Semiconductor Macroatoms. *Phys. Rev. Lett.* 85: 5647-5650 (2000).
[6] Loss D. y DiVincenzo D.P. Quantum computation with quantum dots. *Phys. Rev.* B 59: 2070-2078 (1999).
[7] Méndez-García V.H. InAs quantum dots grown on GaAs(100) surfaces subjected to novel in-situ treatments. *Rev. Mex. Fis.* 51: 230-235 (2005).
[8] Pulzara A. Estudio de Películas Semiconductoras de Compuestos III-V Nitridadas Crecidas por Sputtering y Epitaxia de Haces Moleculares. Tesis de doctorado. Departamento de Física, Cinvestav, México (2006).

Codificación superdensa: característica única del cómputo cuántico

EL CÓMPUTO CUÁNTICO HA DADO LUGAR A PROCEDIMIENTOS QUE ACELERAN DE MANERA NOTORIA LA RESOLUCIÓN DE PROBLEMAS INTRÍNSECAMENTE DIFÍCILES EN EL PARADIGMA DE LA COMPUTACIÓN CLÁSICA. EL PARALELISMO INHERENTE AL CÓMPUTO CUÁNTICO PERMITE UN MAYOR RENDIMIENTO QUE EL FUNCIONAMIENTO SERIAL PROPIO DEL CÓMPUTO CLÁSICO: SI SE UTILIZA EL ENTRELAZAMIENTO DE ESTADOS CUÁNTICOS, POR CADA QUBIT DE INFORMACIÓN RECIBIDO SE PUEDE DUPLICAR LA INFORMACIÓN DE TIPO CLÁSICA.

Guillermo Morales-Luna

En la mecánica cuántica, un *estado cuántico* es la superposición de algunos otros estados. Cuando a un estado cuántico se le toma una medición, entonces cesa la superposición y el estado se restringe a ser alguno de los estados superpuestos. La composición de dos estados cuánticos produce uno, que resulta de adjuntar cada estado superpuesto del primero con cada uno de los estados superpuestos del segundo. Así, la composición no es la mera yuxtaposición de dos estados factores, sino una superposición de todas las posibilidades de los estados superpuestos. El libro de Nielsen y Chuang [5] presenta con detalle las nociones básicas de cómputo cuántico.

El célebre artículo de Einstein, Rosen y Podolsky [3] dio origen a la noción de entrelazamiento, la cual desde la década de los 90 se utilizó para presentar algoritmos eficientes de comunicación [1]. Un tratado muy completo de las posibildades reales y formales de este paradigma se puede encontrar en [4].

A lo largo de estas páginas pretendemos mostrar al lector las bases de tipo algebraico y simbólico en la codificación de bits clásicos utilizando qubits y compuertas cuánticas del tipo de operadores de Pauli. En un principio presentaremos el caso de codificación superdensa (o superdensidad), que comprende la utilización de qubits entrelazados, es decir, de estados cuánticos con sólo dos estados básicos superpuestos, para luego exponer el caso de estados entrelazados con más de dos niveles cuánticos. Hemos querido resumir aquí los procedimientos involucrados pero sin excluir referencias a trabajos, como el de William de la Cruz [2], que permiten al lector profundizar en el tema. Es pertinente aclarar que, en la terminología, utilizaremos las llamadas *qupalabras* y *quregistros* para denotar palabras y registros cuánticos, apegados a maneras convencionales más que a una corrección gramatical en nuestro idioma.

GUILLERMO MORALES-LUNA Es investigador titular en el Departamento de Computación del **Cinvestav**. Obtuvo el grado de licenciatura en Física y Matemáticas (ESFM-IPN), es maestro en Ciencias con especialidad en Matemáticas (**Cinvestav**) y doctor en Ciencias Matemáticas (Instituto de Matemáticas, Academia Polaca de Ciencias). Sus áreas de interés son los fundamentos matemáticos de computación, lógica y deducción automática, criptografía y teoría de la complejidad. Ha sido profesor en el Instituto Politécnico Nacional y en la B. Universidad Autónoma de Puebla. Ha realizado dos estancias sabáticas en el Instituto Mexicano del Petróleo. Es mexicano por nacimiento y en 2005 le fue concedida la ciudadanía polaca. gmorales@cs.cinvestav.mx

El entrelazamiento cuántico se ha utilizado desde la década de los 90 para presentar algoritmos eficientes de comunicación.

Superdensidad en dos dimensiones

Transformaciones de Pauli. El plano cartesiano real posee una estructura de espacio lineal, y las operaciones de suma de vectores y de multplicación por escalares tienen connotaciones geométricas bien definidas. Si dicho plano se identifica con el campo de los números complejos entonces, además de las dos operaciones mencionadas, se tiene la multiplicación compleja: si a un número complejo se le escribe en coordenadas polares, se está distinguiendo su valor absoluto (también llamado *longitud* o *módulo*) y el ángulo que forma con el eje real, llamado *argumento*. Multiplicar cualquier complejo (digamos, multiplicando) por un multiplicador significa rotar el multiplicando a un ángulo igual al argumento del multiplicador y luego elongarlo por una razón igual al módulo del multiplicador. Así pues, la *homotecia* que a cada complejo lo multiplica por un multiplicador fijo actúa como una rotación seguida de una elongación del plano *complejo*.

En el plano cartesiano real se puede identificar todo un grupo de isometrías. Por ejemplo, las matrices

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad (1)$$

definen transformaciones del plano real en sí mismo: la primera es la identidad y deja al plano sin cambio alguno, la segunda lo refleja a lo largo de la diagonal principal y la tercera lo refleja a lo largo del eje de las abscisas.

Al considerar al producto cartesiano del plano complejo consigo mismo se obtiene un espacio lineal complejo bidimensional H_1 (pero isomorfo a uno de dimensión 4 sobre los números reales). Las transformaciones enlistadas arriba actúan de manera similar sobre H_1. Pero ahora, la transformación con entradas complejas

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

hace una reflexión a lo largo de la diagonal principal, en la primera coordenada hace un giro de noventa grados, digamos que en sentido positivo, y en la segunda, otro en sentido negativo. Las matrices σ_x, σ_y, σ_z se dicen ser de Pauli y junto con la identidad σ_0 forman una base de las transformaciones lineales de H_1 sobre sí mismo: cada tal transformación es una combinación lineal única de esas 4 matrices.

Renombradas, las transformaciones de Pauli pueden ser escritas como

$$\sigma_{00} = \sigma_0\ ,\ \sigma_{01} = \sigma_x\ ,\ \sigma_{10} = \sigma_y\ ,\ \sigma_{11} = \sigma_z$$

Al multiplicarlas dos a dos se obtiene la tabla1.

Tabla 1. Multiplicación de las matrices de Pauli

	σ_{00}	σ_{01}	σ_{10}	σ_{11}
σ_{00}	σ_{00}	σ_{01}	σ_{10}	σ_{11}
σ_{01}	σ_{01}	σ_{00}	$-i\,\sigma_{11}$	$i\,\sigma_{10}$
σ_{10}	σ_{10}	$i\,\sigma_{11}$	σ_{00}	$-i\,\sigma_{01}$
σ_{11}	σ_{11}	$-i\,\sigma_{10}$	$i\,\sigma_{01}$	σ_{00}

Toda isometría lineal en el espacio de qubits se expresa en términos de las matrices de Pauli.

Qubits y quregistros. Los vectores en la base canónica $e_0 = (1,0)$, $e_1 = (0,1)$, los que se escriben también como $|0\rangle$ y $|1\rangle$, respectivamente, se identifican con los valores deterministas *falso* y *verdadero*, ó 0 y 1 (obsérvese que este último 0 es el cero lógico, no es el cero del espacio vectorial). Cualquier vector en la esfera unitaria de H_1 es una combinación lineal de los vectores básicos, en la que la suma de los cuadrados de los coeficientes da el valor 1 y se ve como una superposición de los valores 0 y 1. Un tal punto en la esfera unitaria es un qubit y, al medirlo, éste toma uno de los dos valores de verdad con probablidad dada por el cuadrado de su coeficiente. Toda transformación lineal que transforme la esfera unitaria en ella misma se dice ser una *qucompuerta* y es, precisamente, una matriz unitaria, es decir tal que es invertible y su inversa es su propia transpuesta conjugada.

El producto *tensorial* de dos vectores $x = (x_0,...,x_{n-1})$ e $y = (y_0,...,y_{m-1})$ es el resultado de multiplicar cada entrada y_j por cada x_i, es pues

$$x \otimes y = (x_0y_0,..., x_0y_{m-1}, ... , x_{n-1}y_0,..., x_{n-1}y_{m-1})$$

y, por tanto, consiste de *nm* entradas.

Una *1-qupalabra* es un qubit, y, de manera sucesiva, una *k-qupalabra* es el producto tensorial de una (*k*-1)-qupalabra con un qubit. Así, cada *k*-qupalabra ha de ser un vector complejo de dimensión 2^k. Por ejemplo, multiplicando los vectores básicos en H_1, se obtiene

$$|00\rangle = e_{00} = e_0 \otimes e_0 = (1,0,0,0)$$
$$|01\rangle = e_{01} = e_0 \otimes e_1 = (0,1,0,0)$$
$$|10\rangle = e_{10} = e_1 \otimes e_0 = (0,0,1,0)$$
$$|11\rangle = e_{11} = e_1 \otimes e_1 = (0,0,0,1)$$

y, de manera consecutiva, para $k \geq 2$ y cualquier palabra ε de *k* 0's y 1's, $|\varepsilon\rangle$ denota a la *k*-qupalabra que se obtiene de multiplicar tensorialmente a los qubits correspondientes a los bits en la palabra Đ. Denotemos por H_k al espacio lineal complejo de dimensión 2^k. Entonces los puntos en la esfera unitaria de H_k se dicen ser *k-quregistros*. Naturalmente, toda *k*-qupalabra es un *k*-quregistro pero el recíproco no ocurre: hay *k*-quregistros que no son *k*-qupalabras, es decir, no pueden expresarse como el producto tensorial de *k* qubits. Los quregistros que no son qupalabras se dicen estar *entrelazados* o *enredados*. Por ejemplo, puede verse que los vectores

$$b_{00} = \frac{1}{\sqrt{2}}(e_{00} + e_{11}) \quad b_{10} = \frac{1}{\sqrt{2}}(e_{00} - e_{11})$$
$$b_{01} = \frac{1}{\sqrt{2}}(e_{10} + e_{01}) \quad b_{11} = \frac{1}{\sqrt{2}}(e_{10} - e_{01})$$

son 2-quregistros pero no 2-qupalabras. Ellos forman una base del espacio H_2, llamada *base de Bell*, y son los típicos quregistros entrelazados. Cada 2-quregistro puede ser visto como un sistema consistente de dos qubits, cada uno, digamos, en posesión de una de dos partes comunicantes. Llamemos, como es convencional en la presentación de estos temas, a la primera parte *Alicia* y a la segunda *Beto*. Supongamos pues que Alicia y Beto comparten el quregistro $\mathbf{z}=\mathbf{b}_{00}$. Si Alicia realiza una medición en su qubit, entonces con una probabilidad de un medio puede obtener cada uno de los dos posibles valores $|0\rangle$ o $|1\rangle$. El vector obtenido por Alicia tras la medición será uno de éstos, cuando y sólo cuando el 2-quregistro $\mathbf{z}$ dé como resultado de la medición la qupalabra $\mathbf{e}_{ii}$, por lo cual el segundo qubit ha de dar también el mismo vector obtenido por Alicia. Se ve entonces que si Alicia y Beto comparten el quregistro $\mathbf{b}_{00}$ o $\mathbf{b}_{10}$ entonces cualquier valor que obtenga Alicia en una medición a su qubit hará que el mismo valor lo obtenga Beto al medir su qubit, en tanto que si comparten $\mathbf{b}_{01}$ o $\mathbf{b}_{11}$ entonces cualquier valor que obtenga Alicia en una medición a su qubit hará que el valor opuesto lo obtenga Beto al medir su qubit. Es en este sentido

que se usa el adjetivo "entrelazado" para calificar a cualquier estado de la base de Bell.

Así como se multiplican tensorialmente qubits, se puede multiplicar a las qucompuertas para obtener compuertas que actúan sobre quregistros y qupalabras. Formalmente, el producto tensorial de k-qucompuertas es una transformación lineal unitaria en el espacio complejo de dimensión 2^k. El producto tensorial de qucompuertas es la transformación que resulta al aplicar cada qucompuerta en un correspondiente factor de la qupalabra sobre la que actúa. Por ejemplo, el producto tensorial τ_0, de la transformación identidad en el espacio H_1 y de la correspondiente transformación de Pauli σ_0, definida en la sección anterior, hace que el primer qubit de un 2-quregistro permanezca inalterado mientras que en el segundo se aplica la transformación σ_0. Una propiedad importante de τ_0 es que transforma cada vector en la base de Bell en otro vector de esa misma base, de acuerdo con la tabla 2; vale decir, si fijamos dos vectores en la base de Bell podemos identificar (salvo por un producto por un número complejo unitario) la transformacion que cambia al segundo por el primero y, viceversa, dado un vector en la base de Bell y una transformación τ_0 entonces queda determinado (salvo por un producto por un número complejo unitario) el vector en la base de Bell, resultado de aplicar la transformación al vector dado.

Tabla 2. Cada entrada indica la transformación que convierte al quregistro en la columna en el correspondiente quregistro en el renglón

	b_{00}	b_{01}	b_{10}	b_{11}
b_{00}	τ_{00}	τ_{01}	τ_{10}	$-i\,\tau_{11}$
b_{01}	τ_{01}	τ_{00}	$-i\,\tau_{11}$	τ_{10}
b_{10}	τ_{10}	$-i\,\tau_{11}$	τ_{00}	τ_{01}
b_{11}	$-i\,\tau_{11}$	τ_{10}	τ_{01}	τ_{00}

Si hacemos abstracción de las constantes involucradas y sólo prestamos atención a los índices, a los que podemos reescribir como (0,1,2,3) = (00,01,10,11), entonces la tabla 2 se reescribe a su vez como la tabla 3, la cual describe una estructura de grupo, con dos generadores, cada uno de orden 2. Este grupo es isomorfo a $z_2 \oplus z_2$: si se observa al bloque de 4 cuadros en el extremo superior izquierdo se ve la tabla del grupo z_2 de dos elementos.

Tabla 3. Reescritura de la tabla 2. Ésta es isomorfa a $z_2 \oplus z_2$

	0	1	2	3
0	0	1	2	3
1	1	2	3	2
2	2	3	0	1
3	3	2	1	0

Observamos en este punto que la tabla 1 también determina a la tabla 3 al considerar sólo los índices de las transformaciones. Evidentemente las tablas 1 y 2 están definiendo estructuras isomorfas, es decir, con una misma estructura algebraica: $z_2 \oplus z_2$.

Superdensidad bidimensional. Supongamos que Beto quisiera transmitir dos bits clásicos a Alicia, digamos $\varepsilon_0\,\varepsilon 1$, y que Alicia y Beto comparten uno de los estados entrelazados digamos el estado **b** con índices $\delta_0\,\delta_1$. La comunicación puede realizarse mediante el siguiente protocolo:

Beto aplica la transformación σ correspondiente a los índices $\varepsilon_0\varepsilon_1$ a su qubit, lo cual significa que la correspondiente transformación τ se está aplicando al estado **b** compartido. De acuerdo con la tabla 2, se ha de obtener un quregistro **y** que es un estado **b** correspondiente a dos índices $\eta_0\eta_1$. Beto entonces transmite su qubit a Alicia, quien queda en conocimiento de **y**. Al medirlo respecto a la base de Bell, Alicia podrá conocer

Los bits clásicos se identifican con las direcciones en el espacio de qubits.

los índices de **y**. De la tabla 2 podrá entonces recuperar de manera inequívoca a la pareja $\varepsilon_0\varepsilon_1$.

Así pues, si se comparte un estado entrelazado, con la mera transmisión de un solo qubit se puede comunicar dos bits clásicos. A este fenómeno se le conoce como de *superdensidad*.

Una primera forma de superdensidad de varias partes. Así como el protocolo descrito en la sección anterior se realiza con estructuras formales en el espacio $H_2 = H_1 \otimes H_1$, se puede pasar a un protocolo con varias partes comunicantes, pasando a un espacio de dimensión mayor. Sea $k \geq 2$ un entero positivo y sea H_k la k-ésima potencia tensorial de H_1. El espacio H_k es uno lineal complejo de dimensión 2^k. Definamos, para cada lista de k bits ε, $\mathbf{b}_\varepsilon = \frac{1}{\sqrt{2}}(|\varepsilon\rangle + |\overline{\varepsilon}\rangle)$ (aquí la raya encima significa *complemento bit-a-bit*). Resulta, entonces, que la colección de vectores $\{\, \mathbf{b}_\varepsilon \mid \varepsilon$ es una palabra de k bits$\}$ que forma una base ortonormal, llamada de Bell, del espacio H_k. También cada vector en la base de Bell da lugar a todos los demás cuando se le aplican transformaciones obtenidas como productos tensoriales de la transformación identidad de H_1 y de transformciones de Pauli, digamos, de esta forma:

$$1 \otimes \sigma_{\varepsilon_0^{(1)}\varepsilon_1^{(1)}} \otimes \cdots \otimes \sigma_{\varepsilon_0^{(k-1)}\varepsilon_1^{(k-1)}} \qquad (2)$$

Para explicar brevemente esto, recordemos la función CN llamada *negación controlada*. Ésta recibe dos bits y produce uno solo como resultado; si el primer argumento es cero, deja como valor al segundo argumento pero, en otro caso, deja como valor a la negación del segundo. CN es una de las funciones primitivas del cómputo cuántico, es decir que, junto con las transformaciones de Pauli, puede representar cualquier función computable en el paradigma del cómputo cuántico. Al aumentar el número de argumentos, extendemos a CN iterándola como sigue:

$$CN_1(\delta_1,\delta_2) = CN(\delta_1,\delta_2) \quad , \quad CN_k(\delta_1,\delta_2,\ldots,\delta_{k+1}) = CN(\delta_1, CN_{k-1}(\delta_2,\ldots,\delta_{k+1}))$$

Puede verse que cuando un operador de la forma (2) se aplica sobre el primer quregistro de la base de Bell, se obtiene un quregistro que es paralelo a otro quregistro único $\mathbf{b}_\eta$ de la base de Bell, donde los índices η se obtienen de los índices ε mediante las iteraciones de la función CN. Sin embargo, esta relación no define una correspondencia biunívoca entre los operadores (2) y los quregistros en la base de Bell (hay más operadores del tipo (2) que vectores de Bell). Resulta que para cada vector básico de Bell hay exactamente 2^{k-1} operadores del tipo (2), que aplican al primer vector básico en cada uno de los demás. Se requiere, pues, una condición suplementaria para que la correspondencia sea biunívoca (de manera técnica se dice "para desambiguar la correspondencia"): si el primer índice η es 0 se hace 0 a cada uno de los índices ε excepto al último (el cual depende del operador (2)), y si el primer índice η es 1 se hace 0 a cada uno de los índices ε excepto al penúltimo el cual se hace 1 y al último (el cual depende del operador (2)).

En un estado entrelazado, la medición que realice una parte comunicante, determinará la medición que obtenga la otra parte.

Utilizando la tabla de multiplicación 1, se puede sustituir el primer vector básico de Bell por cualquier otro en la base de Bell y obtener la correspondencia adecuada entre los operadores (2) y los demás vectores básicos. Se obtiene así una generalización de la tabla de multiplicación 1.

La generalización de superdensidad se hace en un escenario en el que una parte, Alicia, es la destinataria de mensajes enviados por k-1 corresponsales B_1, ..., B_{k-1}. Cada uno de tales mensajes consiste de dos bits clásicos Un primer protocolo de superdensidad con varias partes es el siguiente:

1. Alicia y sus corresponsales acuerdan un vector entrelazado $\mathbf{b}_\varepsilon$ en la base de Bell.
2. Cada corresponsal B_j aplica a su qubit la transformación $\sigma_{\varepsilon_0^{(j)}\varepsilon_1^{(j)}}$.

Todas éstas formarán un operador del tipo (2) y harán que el vector entrelazado acordado se transforme en un múltiplo (es decir, en un corrimiento de fase) de otro vector en la base de Bell. Cada corresponsal B_j envía entonces su qubit a Alicia.

3. Conociendo todos los qubits, Alicia toma una medición, respecto a la base de Bell, del estado global entrelazado; y mediante ello y la condición suplementaria reconoce la transformación global aplicada, es decir, identifica dos bits clásicos por cada corresponsal. Mediante este protocolo, Alicia recibe k-1qubits y reconoce el doble de bits clásicos.

Superdensidad en varias dimensiones

Estados cuánticos de dimensión mayor. Sea k un entero positivo mayor que 2. En el plano complejo, consideremos el k-ágono regular inscrito en el círculo unitario con un vértice en el punto 1. En la figura 1 mostramos ese k-ágono para algunos k.

El primer vértice luego del número 1 recorriendo el k-ágono en sentido opuesto a las manecillas del reloj es el número complejo

$$\rho_k = e^{i\frac{2\pi}{k}} = \cos\left(\frac{2\pi}{k}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{k}\right)$$

que no es otro sino la k-ésima raíz primitiva de la unidad. A los vértices del k-ágono regular, es decir, a las potencias de ρ_k, se les ve como valores representativos de varios estados cuánticos.

Sea ahora H_{1k} el espacio lineal complejo de dimensión k y sea $\{\mathbf{e}_1, ..., \mathbf{e}_{k-1}\}$ su base canónica. Sea H_{kk} la k-ésima potencia tensorial de H_{1k} la cual es un espacio lineal complejo de dimensión k^k. En la tabla 4 presentamos algunos de estos últimos valores con el fin de ilustrar su crecimiento.

Tabla 4. Ilustración del crecimiento de k^k

k	k^k	k	k^k
1	1	6	46,656
2	4	7	823,543
3	27	8	16,777,216
4	256	9	387,420,489
5	3,125	10	10,000,000,000

Los estados en la base de Bell se identifican con respectivas transformaciones compuestas de Pauli y éstas con palabras de índices.

La superdensidad comunica dos bits clásicos mediante la transmisión de un qubit.

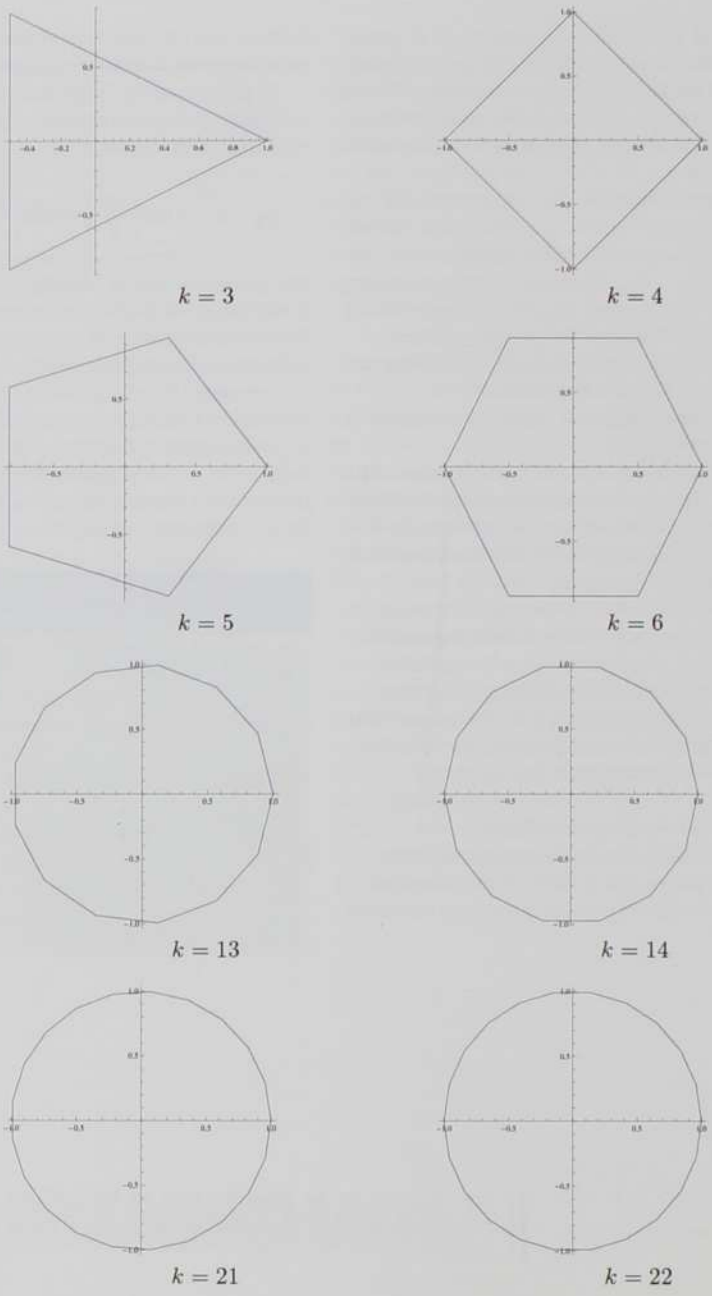

Figura 1. *k*-ágonos regulares inscritos en el círculo unitario del plano complejo.

La superdensidad puede duplicar capacidades de comunicación pero presenta aún complejos problemas técnicos de control para explotarla.

Consideremos el conjunto de índices enteros entre 0 y k^k-1 inclusive, el cual consta de k^k elementos. Al escribir a cada uno de esos índices en base k, obtenemos una cadena única de k dígitos entre 0 y k-1 inclusive y así se identifica al intervalo de enteros entre 0 y k^k-1con las cadenas de longitud k de dígitos entre 1 y k-1. En la tabla 5 presentamos esa correspondencia para el caso $k = 3$.

Tabla 5. Los enteros entre 0 y 33-1 se expresan mediante cadenas de 3 dígitos 0, 1, 2

j	$(j)_2$	j	$(j)_2$	j	$(j)_2$
0	000	9	100	18	100
1	001	10	101	19	101
2	002	11	102	20	102
3	010	12	110	21	110
4	011	13	111	22	111
5	012	14	112	23	112
6	020	15	120	24	120
7	021	16	121	25	121
8	022	17	122	26	122

Para cualquier lista $n=[n_0, n_1, ..., n_{k-1}]$, de k dígitos entre 0 y k-1, y cualquier índice j entre 0 y k-1 definamos

$$\mathbf{x}_{jn} = \mathbf{e}_j \otimes \mathbf{e}_{(j+n_1) \bmod k} \otimes \mathbf{e}_{(j+n_2) \bmod k} \otimes \mathrm{L} \otimes \mathbf{e}_{(j+n_{k-1}) \bmod k}$$

y tomemos el promedio de esos registros bajo un cambio de fase dado por una raíz de la unidad,

$$\mathbf{b}_n = \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \rho_k^{jn} \mathbf{x}_{jn}$$

Cada uno de estos vectores se dice estar entrelazado al máximo, y la colección de todos ellos forma una base, llamada también de Bell, del espacio H_{kk}. Es posible definir transformaciones unitarias en el espacio H_{kk} análogas a las transformaciones de Pauli. Con ellas se tiene transformaciones que cambian entre sí a cualesquiera dos vectores entrelazados al máximo. Surge así la posibilidad de comunicar una $2(k\text{-}1)$-tupla de dígitos entre 0 y k-1enviando sólo k-1 estados cuánticos de k niveles. Esto conlleva sorprendentes procesos de suma eficiencia en las comunicaciones de tipo cuántico.

En resumen, el protocolo de comunicación superdensa surgió en la década de los 90 con la utilización de quregistros entrelazados. Con ella, una parte puede duplicar, en términos de bits clásicos, la información que envíe mediante qubits. Los estados cuánticos involucrados en este caso son superposiciones de dos niveles cada uno. Cuando se extiende a varias partes, podría reiterarse, de manera natural, el procedimiento bipartito. Sin embargo, puede acoplarse en un solo proceso utilizando estados cuánticos de varios niveles. La parte matemática se complica en cuanto a su presentación, pero las ideas son las mismas que en el caso bipartito: los niveles se representan por las raíces de la unidad. No obstante, el aspecto de implementación física puede complicarse aún más que el caso bipartito, ya de por sí difícil con el nivel de desarrollo actual de la tecnología requerida . ●

[Referencias]

[1] C. H. Bennett y S. J. Wiesner. Communication via one and two-particle operators on Einstein-Podolsky-Rosen states. *Phy. Rev. Lett.*, 69:2881-2884, noviembre 1992.

[2] William de la Cruz de los Santos. *Simulación de protocolos de comunicación eficientes basados en estados entrelazados*. Tesis de maestría, dirigida por Guillermo Morales-Luna, Departamento de Computación, Cinvestav-IPN, México, D. F., 2007.

[3] A. Einstein, B. Podolsky y N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777-780, mayo 1935.

[4] Leonid Gurvits. Classical complexity and quantum entanglement. *J. Comput. Syst. Sci.*, 69(3):448-484, 2004.

[5] Michael A. Nielsen e Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, Inglaterra, 2000.

Control cuántico: dos enfoques

DIFERENTES ESQUEMAS DE CONTROL SOBRE SISTEMAS CUÁNTICOS HAN SIDO APLICADOS AL DEMANDARSE MAYORES APLICACIONES ESPECÍFICAS SOBRE SISTEMAS DE VARIABLES CONTINUAS O DISCRETAS, RETOMANDO ALGUNAS IDEAS DEL CONTROL CLÁSICO MODIFICADAS POR LAS LIMITANTES PARA MEDIR Y ALTERAR ESTADOS CUÁNTICOS.

Francisco Javier Delgado Cepeda

La mecánica cuántica está teniendo un número creciente de aplicaciones, las cuales son diversas y han requerido de esquemas tecnológicos más afines a la ingeniería, como lo es la teoría de control. En un esquema tradicional se han formulado procedimientos básicos para controlar propiedades del sistema cuántico en aplicaciones como la microscopía electrónica y los aceleradores de partículas, en donde un proceso dinámico autosostenido se aplica para mantener al sistema bajo cierto estado. Sin embargo, aplicaciones actuales en las áreas de computación e información cuántica requieren un enfoque más detallado hacia la teoría de control, que incluya la retroalimentación del sistema; no obstante, aparecen diferencias dadas las peculiaridades de la mecánica cuántica. En este artículo se hace una presentación de estos dos enfoques que constituyen variantes hacia el objetivo de controlar los parámetros de algunos sistemas cuánticos.

Antecedentes

El control es una rama interdisciplinaria de la ingeniería y las matemáticas, aplicada al comportamiento de los sistemas dinámicos. Un controlador manipula la entrada o estado inicial del sistema para lograr un efecto deseado en un estado posterior o salida [1]. La teoría de control jugó un papel relevante durante la segunda Guerra Mundial, desde sistemas de control de fuego, sistemas de vuelo e incluso la electrónica. Hoy en día, prácticamente todo sistema mecánico y electrónico posee un sistema de control asociado, por sencillo que sea.

Un sistema de control simple consiste en una acción sobre el sistema y la obtención del resultado esperado sobre el mismo. Sin embargo, para evitar un final abierto, los sistemas realizan, por lo regular, mediciones intermedias sobre sus salidas y con esa información el sistema es retroalimentado para modificar la acción de control reiniciando el ciclo de entrada-salida (figura 1).

FRANCISCO JAVIER DELGADO CEPEDA Licenciado en Física (Universidad Autónoma Metropolitana-Iztapalapa), maestro y doctor en Ciencias con especialidad en Física (**Cinvestav**). Desde 1991 es profesor del Departamento de Física y Matemáticas del Tecnológico de Monterrey, Campus Estado de México. Sus áreas de interés son el control cuántico, la computación e información cuánticas, así como los métodos numéricos. Pertenece al grupo de Procesamiento Cuántico de la Información del Tecnológico de Monterrey.
fdelgado@itesm.mx

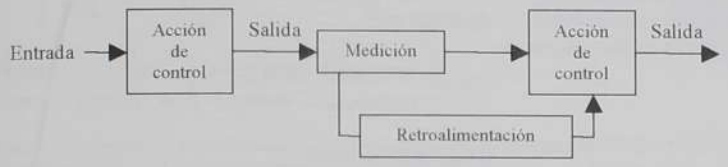

Figura 1. Esquema de control básico.

La mecánica cuántica ha comenzado a invadir nuestras vidas a través de diversas aplicaciones y, por ello, cada vez es más recurrente la necesidad de controlar los sistemas cuánticos. Desde los aceleradores de partículas, que requieren eficiencia y efectividad, hasta los modernos modelos para construir bits cuánticos están exigiendo que la rama del control cuántico se desarrolle. Sin embargo, algunas cualidades de la mecánica cuántica no permiten pasar fácilmente el esquema del control clásico al ámbito cuántico. Clásicamente, es posible adquirir toda la información necesaria y emplearla de manera eficiente para retroalimentar el sistema y especializar la acción de control al estado actual. No obstante, en un sistema cuántico no toda la información es asequible mediante una medición y, adicionalmente, todo intento de medir el sistema lo perturba de manera notable. De este modo, o planeamos un esquema de control que delimite el sistema todo el tiempo desde el inicio (independiente del estado inicial) o buscamos esquemas que permitan circunnavegar las restricciones impuestas por la mecánica cuántica en lo posible.

Para ejemplificar, vamos a presentar dos esquemas de control que siguen cada una de estas ideas y que han surgido desde los terrenos del control en la física de aceleradores, y otro más que ha sido ideado para controlar estados cuánticos discretos.

El control dinámico mediante evolución cuántica

Desde que las primeras aplicaciones teóricas de la teoría cuántica surgieron, se propusieron algunos esquemas que mediante potenciales externos lograban tener un cierto efecto sobre la partícula en él. Un esquema más avanzado y realista ha sido propuesto por diferentes autores [2-6].

En este esquema se explota una peculiaridad de los hamiltonianos que dependen cuadráticamente del momento y la posición, mismos que resultan de forma natural al emplear un campo magnético homogéneo $\vec{B}(t)$ dependiente del tiempo y dirigido en una sola dirección espacial. Si $\vec{A}(\vec{x},t)$ es el potencial magnético, $\vec{x}$ la posición, y $\hat{k}$ el vector unitario a lo largo de la dirección z sobre la que se encuentra el campo magnético:

$$\vec{A}(\vec{x},t) = -\tfrac{1}{2}\vec{x}\times\vec{B}(t) = -\tfrac{1}{2}B(t)\vec{x}\times\hat{k}$$

teniendo como hamiltoniano H y operador de evolución U para una partícula de masa m y carga e:

$$H(t) = \tfrac{1}{2m}\left(\vec{p} - \tfrac{e}{c}\vec{A}(t)\right)^2 = \tfrac{1}{2m}p_z^{\,2} - \tfrac{eB(t)}{2mc}M_z + \\ + \tfrac{1}{2m}\left(p_x^{\,2} + p_y^{\,2} + \left(\frac{eB(t)}{2c}\right)^2(x^2+y^2)\right)$$

$$\Rightarrow U(t,0) = e^{-i\hbar p_z^{\,2}/2m\hbar}e^{i\alpha(t)M_z/\hbar}W_x(t)W_y(t)$$

donde: $\vec{p}$ es el momento, M_z la componente z del momento angular y $\alpha(t) = \frac{e}{2mc}\int_0 B(\xi)d\xi$ el ángulo rotado al tiempo t.

Lo anterior separa la evolución de la partícula en una evolución libre en el eje z, una rotación alrededor de este eje y dos operaciones simultáneas sobre los ejes x y y dadas por:

$$\frac{dW}{d\tau} = -iG(\tau)W(\tau)\ ,\ G(\tau) = \frac{p^2}{2} + \beta(\tau)^2\frac{q^2}{2}$$

donde se redefine:

$$q = \sqrt{\tfrac{m}{\hbar}}q_i, p = \sqrt{\tfrac{\tau}{m\hbar}}p_i \text{ para } i = x,y$$

$$\beta(\tau) = \frac{eTB(T\tau)}{2mc}$$

Son W_x y W_y las que pueden utilizarse como operaciones de control escogiendo los parámetros

libres en $B(t)$ de forma adecuada, ya que es esta elección la que permite lograr efectos selectivos sobre los valores de las coordenadas y sus momentos lineales asociados. T es un parámetro introducido por conveniencia para marcar el periodo temporal de la operación de control y τ será el tiempo en esta nueva escala. Un hecho notable es que el hamiltoniano es cuadrático en p y q, lo que implica que su evolución se pueda expresar en términos lineales de sus valores iniciales como:

$$\begin{pmatrix} q(\tau) \\ p(\tau) \end{pmatrix} = u(\tau)\begin{pmatrix} q \\ p \end{pmatrix}$$

donde:

$$\frac{du(\tau)}{d\tau} = \Lambda(\tau)u(\tau), \quad u(\tau = 0) = 1$$

y:

$$\Lambda(\tau) = \begin{pmatrix} 0 & 1 \\ -\beta(\tau)^2 & 0 \end{pmatrix}$$

Algunas de las operaciones de interés que pueden ser generadas con este esquema se dan a través de la forma de $u(\tau)$:

Operaciones de escala (Squeezing): $u(\tau = 1) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$

Operaciones cíclicas (Evolution Loops): $u(\tau = 1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Operaciones de alteración temporal: $u(\tau = 1) = \begin{pmatrix} 1 & \tau' \\ 0 & 1 \end{pmatrix}$

La primera permite comprimir o expandir las dimensiones de la evolución libre en el plano xy; la segunda permite regresar al sistema a su estado inicial después de un periodo T, en tanto que la tercera podrá alterar el ritmo de evolución libre al tiempo t, acelerándolo hasta un tiempo $\tau' T > t$ o frenándolo hasta un tiempo $\tau' T < t$ (o revirtiéndolo a un estado previo al inicial $\tau' T < 0$). Aunque existen soluciones numéricas para otras formas más plausibles de campo, una solución analítica para las operaciones de escala se presenta para el caso de un pulso cuadrado:

$$\beta(\tau) = \begin{cases} \alpha_1, & 0 \le \tau < \tau_1 \\ \alpha_2, & \tau_1 \le \tau < 1 = \tau_1 + \tau_2 \end{cases}$$

de modo que:

$$u(1) = \begin{pmatrix} \cos(\alpha_2\tau_2) & \sin(\alpha_2\tau_2)/\alpha_2 \\ -\alpha_2 \sin(\alpha_2\tau_2) & \cos(\alpha_2\tau_2) \end{pmatrix}\begin{pmatrix} \cos(\alpha_1\tau_1) & \sin(\alpha_1\tau_1)/\alpha_1 \\ -\alpha_1 \sin(\alpha_1\tau_1) & \cos(\alpha_1\tau_1) \end{pmatrix}$$

dando por solución:

$$\alpha_1\tau_1 = (n + \tfrac{1}{2})\pi, \alpha_2\tau_2 = (k + \tfrac{1}{2})\pi, \; k, n \in Z \quad \Rightarrow \quad u(1) = (-1)^{n+k+1}\begin{pmatrix} \alpha_1/\alpha_2 & 0 \\ 0 & \alpha_2/\alpha \end{pmatrix}$$

La figura 2 muestra el caso de una operación de escala (compresión con $\lambda = -1/3$). Es notable el efecto de "boomerang" intermedio, presente en estos casos [6,7], en el que cada vez la partícula se acerca más al origen pero a un costo intermedio de gran alejamiento.

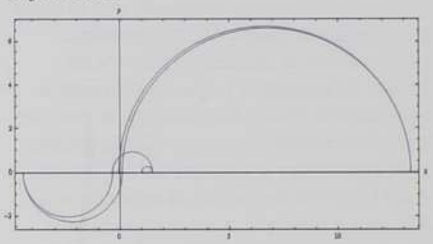

Figura 2. Ejemplo de la trayectoria clásica para los pulsos cuadrados con $\lambda = -1/3$. La trayectoria comienza en el punto (1,0) y termina después de tres repeticiones en el punto (-1/27,0).

El esquema anterior implica controlar también el tamaño del paquete de la partícula:

$$\Delta q = \sqrt{\langle (q - \langle q \rangle)^2 \rangle} = \sqrt{\langle q^2 \rangle^2 - \langle q \rangle^2} =$$
$$= \sqrt{u_{11}^2 \Delta q_0^2 + u_{12}^2 \Delta p_0^2 + u_{11}u_{12}\langle \{p_0, q_0\} \rangle - 2u_{11}u_{12}\langle q_0 \rangle \langle p_0 \rangle}$$

La teoría de control jugó un papel relevante durante la segunda Guerra Mundial, desde sistemas de control de fuego, sistemas de vuelo e incluso la electrónica. Hoy en día, prácticamente todo sistema mecánico y electrónico posee un sistema de control asociado, por sencillo que sea.

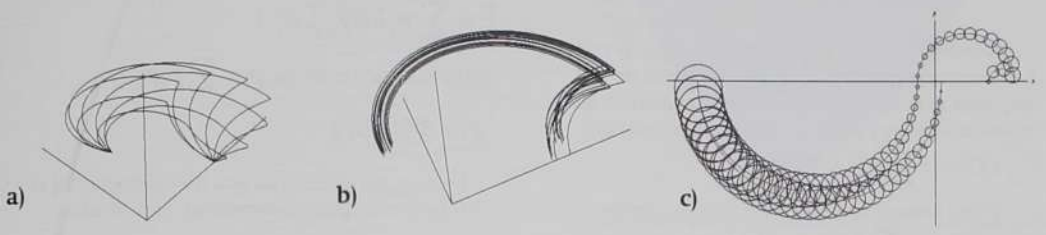

Figura 3. a) Enfoque de un grupo de partículasque parten del mismo punto con diferentes velocidades, b) enfoque de un grupo de trayectorias reduciendo el tamaño de la vecindad que las contiene, y c) comportamiento de la amplitud del paquete de onda alrededor de la trayectoria clásica.

Para un paquete inicialmente gaussiano se obtiene:

$$\langle\{p_0, q_0\}\rangle = 0, \Delta q_0 \Delta p_0 = 1 \Rightarrow$$

$$\Delta q(\tau = n + \delta) = \sqrt{u_{11}(\delta)^2 \lambda^n \Delta q_0^{\ 2} + u_{12}(\delta)^2 \Delta q_0^{\ -2} - 2\lambda u_{11}(\delta) u_{12}(\delta) \langle q_0 \rangle \langle p_0 \rangle}$$

donde $n \in N$ y $\delta \in (0,1)$. La figura 3 muestra algunos efectos colaterales: a) varias partículas con diferentes velocidades partiendo de un mismo punto se enfocan después de un ciclo; b) un grupo de partículas partiendo de una vecindad se enfoca en otra vecindad reducida por el mismo factor de escala, y c) una representación del comportamiento de la amplitud de un paquete esféricamente gaussiano alrededor de la trayectoria clásica.

Un modelo más plausible para el pulso magnético ha sido ya estudiado, aunque no arroja resultados analíticos [6], dando las mismas características aquí mostradas.

El control clásico como método para controlar sistemas cuánticos discretos

El control cuántico aplicado a sistemas discretos ha resultado recientemente de interés a la luz aplicaciones como la computación e información cuánticas, en donde por lo regular se emplean sistemas que pueden tomar sólo un conjunto discreto de estados, particularmente el caso binario. En el sentido anterior resulta de interés discernir entre dos estados no ortogonales que en notación de Dirac escribiremos $|\phi_1\rangle$ y $|\phi_2\rangle$.

Para ello, normalmente se considera la aplicación de una distorsión de lo estados mediante un CPTP (*Completely Positive Trace Preserving*), ε_p, de modo que con cierta probabilidad *p* el estado original resulta alterado. Es claro que la condición de que su aplicación genere un nuevo estado ρ' implica que este sea definido positivo y adicionalmente de traza unitaria:

$$\rho' = \varepsilon_p \rho$$

Lo que se busca ahora es un proceso para revertir el efecto de esta distorsión. En este enfoque se definen los mapeos EBTP (*Entanglement Breaking and Trace Preserving maps*):

$$\Phi(\rho) = \sum_k R_k \mathrm{Tr}(F_k \rho)$$

el símbolo Tr se refiere a la traza, R_k es un conjunto de matrices de densidad y F_k un POVM[1] (*Positive Operador Valued Measure*). Este tipo de mapeos tienen la propiedad de generar estados separables y pueden escribirse siempre como [8]:

La mecánica cuántica ha comenzado a invadir nuestras vidas a través de diversas aplicaciones y, por ello, cada vez es más recurrente la necesidad de controlar los sistemas cuánticos. Desde los aceleradores de partículas, que requieren eficiencia y efectividad, hasta los modernos modelos para construir bits cuánticos están exigiendo que la rama del control cuántico se desarrolle.

$$\Phi(\rho) = \sum_k |\psi_k\rangle\langle\psi_k| \mathrm{Tr}(|\phi_k\rangle\langle\phi_k|\rho)$$

Siendo $\{|\psi_k\rangle\}, \{|\phi_k\rangle\}$ un conjunto de estados no necesariamente ortogonales. Ahora, en un esquema más afín al control clásico se definen dos tipos particulares [9,10], un *mapeo cuántico-clásico*:

$$QC(\rho) = \sum_k |e_k\rangle\langle e_k| \mathrm{Tr}(F_k\rho)$$

y uno denominado un *mapeo clásico-cuántico*:

$$CQ(\rho) = \sum_k R_k \mathrm{Tr}(|e_k\rangle\langle e_k|\rho)$$

donde $\{|e_k\rangle\}$ es una base ortonormal. El primer mapeo es realizado vía una medición para transmitir por un canal clásico el resultado, con lo que posteriormente es sometido al segundo y se "reconstruye" el estado original [10] dando precisamente un mapeo EBTP:

$$CQ \circ QC(\rho) = \sum_k R_k \mathrm{Tr}(F_k\rho)$$

Esto implica que el remitente realiza una medición "conveniente" (es decir, sencilla pero que asume que permite con cierto nivel de confianza detectar cierto estado) sobre un sistema de entrada ρ y lo envía por un canal clásico a un receptor que prepara un nuevo estado establecido R_k. Este es, precisamente, el punto central en relación al control clásico en donde lo mejor es recabar la mayor información sobre el sistema para poder implementar el criterio de control más conveniente.

Posteriormente se define la fidelidad del proceso a través de la operación:

$$F(|\psi\rangle, \rho) = \langle\psi|\rho|\psi\rangle$$

donde ρ es el estado de salida y $|\psi\rangle$ el estado con el que se desea comparar. Esta medida toma claramente valores entre 0 y 1, siendo 1 la máxima fidelidad en donde el estado de salida sería precisamente $\rho = |\psi\rangle\langle\psi|$, y 0 la mínima fidelidad en donde ρ estaría conformado por un estado ortogonal a $|\psi\rangle$. Considerando que el estado original pudiera realmente no ser un estado puro sino una mezcla de estados,[2] se define para ello normalmente la fidelidad promedio:

$$\bar{F} = \sum_k p_k F(|\psi_k\rangle, \rho'_k)$$

siendo el estado original: $\rho = \sum_k p_k \rho_k$, y

$$\rho'_k = \Phi(\varepsilon_p(\rho_k)).$$

Un ejemplo sencillo de esta metodología [10] es considerar con igual probabilidad a los estados:

$$|\psi_{0/1}\rangle = \cos\frac{\theta}{2}|+\rangle \pm \sin\frac{\theta}{2}|-\rangle = \cos\left(\frac{1}{2}\left(\frac{\pi}{2} \mp \theta\right)\right)|0\rangle + \sin\left(\frac{1}{2}\left(\frac{\pi}{2} \mp \theta\right)\right)|1\rangle$$

$$\Rightarrow \rho_{0/1} = |\psi_{0/1}\rangle\langle\psi_{0/1}|$$

que son estados simétricos respecto a los estados $|0\rangle$ y $|1\rangle$. Si los sometemos al CPTP:

$$\rho'_k = \varepsilon_p\rho_k = pZ\rho_k Z + (1-p)\rho_k$$

donde Z es el operador de Pauli correspondiente y posteriormente aplicamos como control el EBTP:

$$\Phi(\rho'_i) = \sum_{k=0}^{1} \rho_k \mathrm{Tr}(|k\rangle\langle k|\rho'_i)$$

en donde se asume que la detección de un estado $|0\rangle$ implica con cierta certeza el estado $|\psi_0\rangle$, y la detección de $|1\rangle$ el $|\psi_1\rangle$. Obtenemos así, por cálculo directo (asumiendo una mezcla homogénea de los estados):

$$\bar{F} = \tfrac{1}{2}F(|\psi_0\rangle, \Phi(\rho'_0)) + \tfrac{1}{2}F(|\psi_1\rangle, \Phi(\rho'_1)) = 1 - \frac{1}{2}\left(\sin^2\theta - \sin^3\theta\right)$$

Hay al menos un par de aspectos relevantes (figura 4). El primero es que, en este esquema sencillo, la fidelidad no depende de la probabilidad p, de modo que por probable que sea la distorsión del estado original, el esquema de control no se ve afectado por ello. Adicionalmente notamos que los valores de la fidelidad están muy próximos a 1, siendo para valores cercanos a $\theta = \pi/4$ que se alcanza el mínimo valor, que es de aproximadamente 0.92. A modo de comparación podemos considerar la fidelidad si no sometiéramos al sistema al mapeo EBTP:

En la medida que las aplicaciones de la mecánica cuántica están surgiendo, el tema de control cuántico comienza a ser un campo cada vez más recurrido, desde aplicaciones experimentales en los aceleradores de partículas y esquemas experimentales para la creación estados cuánticos macroscópicos hasta la florecientes áreas de la computación e información cuántica.

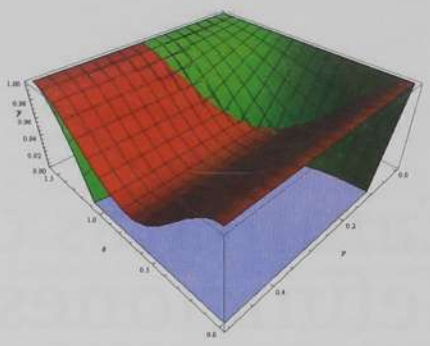

Figura 5. Comparación del valor de la función de fidelidad con (rojo) y sin (verde) esquema de control.

$$\bar{F} = \tfrac{1}{2}F(|\psi_0\rangle,\ \rho_0) + \tfrac{1}{2}F(|\psi_1\rangle,\ \rho_0) = 1 - p\cos^2\theta$$

La figura 5 muestra una comparación de la fidelidad para ambos esquemas. Dado que el no introducir un esquema de control hace que la fidelidad dependa de p, ello muestra que para valores pequeños de este parámetro el esquema de control presentado no es conveniente, no así para valores mayores (p aproximadamente mayor a 0.25) en donde la fidelidad resulta mejor para todo valor de θ. Para p=0.5 vemos que la fidelidad cae para algunos ángulos hasta casi 0.5 (no mostrado en la figura), muy lejos de lo correspondiente para el caso que comprende el control.

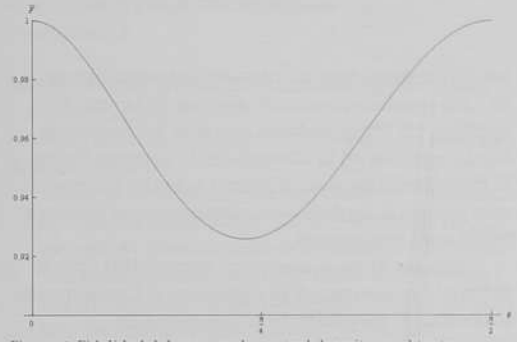

Figura 4. Fidelidad del proceso de control descrito en el texto.

Otros estados a los mostrados aquí pueden ser de interés y con otro conjunto de reglas para el EBTP de control empleado. En añadidura esquemas más realistas de ruido o distorsión dados por otros CPTP deben ser considerados.

En conclusión, el tema de control cuántico comienza a ser un campo cada vez más recurrido, en la medida que las aplicaciones de la mecánica cuántica están surgiendo. Desde aplicaciones experimentales en los aceleradores de partículas y esquemas experimentales para la creación estados cuánticos macroscópicos hasta la florecientes áreas de la computación e información cuántica. No obstante, en la actualidad apenas hemos experimentado con esquemas sencillos de pérdida de superposición cuántica y/o ruido, o con efectos de control lejanos a lo que las aplicaciones pueden darnos, de modo que aún la teoría y la práctica no alcanzan un estado común de desarrollo y, como en todos los aspectos avanzados de la ciencia y la tecnología, será necesaria una evolución todavía más decidida para poder tener en nuestras manos todas las bondades de la teoría cuántica. Algunos aspectos aún no entendidos del todo, como particularmente lo es el colapso del paquete de onda, resultan cruciales para lograr este estado de conocimiento .

[Notas]

[1] En teoría cuántica de la medición, un POVM es un conjunto de operadores hermitianos semidefinidos positivos $\{F_i\}$ tales que $\sum F_i = 1$. Es importante notar que no se requiere que se cumpla la condición de ortogonalidad: $F_iF_j = \delta_{ij}$ habitual para los operadores que representan una cantidad física.

[2] En mecánica cuántica se define un estado mezclado a través de la combinación lineal: $\rho = \sum_i p_i \rho_i, \sum_i p_i = 1$ de estados puros que en contraposición tienen la forma $\rho_i = \phi_i \cdot \phi_i$.

[Referencias]

[1] Franklin, Gene. *Feedback Control of Dynamic Systems*, New Jersey, Prentice Hall, 2002.

[2] Lamb, W.E. Jr., An Operational Interpretation of Non-Relativistic Quantum Mechanics, *Phys. Today* 22, pp. 23-28, 1969.

[3] Lubkin, E., A physical system which can be forced to execute an arbitrary unitary transformation, and its use to perform arbitrary tests, *J. Math. Phys.* 15, pp. 673-674, 1974.

[4] Mielnik, B., Evolution Loops, *J. Math. Phys.* **27**, pp 2290-2305, 1986.

[5] Fernández C., David J., Geometric Phases and Mielnik's Evolution Loops, *Int. J. Theor. Phys.* 33, pp. 2037-2048, 1994.

[6] F. Delgado y B. Mielnik, Magnetic control of squeezing effects, *J. Phys. A* 31, pp. 309-320, 1997.

[7] F. Delgado y B. Mielnik, Squeezed states and Helmholtz spectra, *Phys. Lett. A* 249, pp. 359-364, 1998.

[8] Horodecki M., Shor P. y Ruskai M., Entanglement Breaking Channels, *Rev. Math. Phys.* 15, pp. 629-642, 2003.

[9] Holevo, A.S., Coding theorems for quantum channels, *Russian Math. Surveys* 53, pp. 1295-1331, 1999.

[10] Branczyk A. *et al.*, Quantum Control of a Single Qubit, *Phys. Rev. A* 75, pp. 012329-012340, 2007.

Caminatas cuánticas: definiciones y algoritmos

LAS CAMINATAS CUÁNTICAS FORMAN UNA DISCIPLINA NUEVA Y APASIONANTE, HIJA DE LA UNIÓN DE LA MECÁNICA CUÁNTICA Y LA TEORÍA DE LA COMPUTACIÓN. TANTO LAS PROPIEDADES FÍSICAS Y MATEMÁTICAS DE LAS CAMINATAS CUÁNTICAS COMO SU APLICACIÓN EN EL DESARROLLO DE ALGORITMOS SON CAMPOS DE RECIENTE CREACIÓN EN LOS QUE HAY OPORTUNIDADES DE CRECIMIENTO PARA FÍSICOS, CIENTÍFICOS COMPUTACIONALES E INGENIEROS, EN LAS ÁREAS DE INVESTIGACIÓN Y DESARROLLO.

Salvador Elías Venegas Andraca

La mecánica cuántica y la teoría de la computación son dos cumbres del intelecto humano alcanzadas en el transcurso del siglo XX. Dicho brevemente, la mecánica cuántica es la rama de la física que explica el comportamiento de la naturaleza a escalas muy pequeñas (por ejemplo, el comportamiento de los átomos). La teoría de la computación se encarga de estudiar si un problema es susceptible de ser resuelto utilizando una computadora, así como la cantidad de recursos (tiempo, energía) que se debe invertir en caso de existir solución.

El impacto de estas dos ramas del saber se encuentra no sólo en el trabajo de varias generaciones de científicos, sino también en la vida cotidiana del hombre, desde la guerra hasta la literatura (ejemplos recientes de esta influencia en la literatura y la historia contemporánea se encuentran en [1-3]). Una de las razones que explican la poderosa influencia que la mecánica cuántica y la teoría de la computación han tenido en la vida moderna es que los paradigmas, teorías y desarrollos tecnológicos de cada una han provocado avances en la otra. Por ejemplo, las computadoras han sido herramientas fundamentales en la simulación de sistemas físicos, y la creación de las computadoras actuales fue posible sólo gracias al profundo conocimiento que tenemos sobre semiconductores.

Entre las últimas aventuras emprendidas por la física y la computación se encuentra la Computación Cuántica. El propósito de la Computación Cuántica es utilizar las teorías de las que nace para incrementar sustancialmente la capacidad de los ordenadores para procesar información y resolver problemas. Esta nueva capacidad se traduce en aumentar la rapidez con la que se ejecuta un algoritmo o bien en añadir elementos de seguridad a transmisiones de datos. El cómputo cuántico no sólo adopta modelos matemáticos para la creación de algoritmos, también usa las propiedades de la materia con la que se procesa información.

Un procedimiento que utiliza mecánica cuántica

SALVADOR ELÍAS VENEGAS ANDRACA Profesor investigador en el Tecnológico de Monterrey, Campus Estado de México. Egresado del Tecnológico de Monterrey y la Universidad de Oxford. Actualmente, sus intereses de investigación se relacionan con los algoritmos cuánticos y los aspectos computacionales de la proteómica.

Dirige un grupo de investigación en procesamiento cuántico de la información y es un apasionado de la política, la historia y la literatura. Grupo de Procesamiento Cuántico de la Información, Tecnológico de Monterrey Campus Estado de México, http://www.mindsofmexico.org/sva • svenegas@itesm.mx

para hallar una solución se llama algoritmo cuántico, en tanto que un algoritmo convencional (también llamado clásico) es un procedimiento programado en una computadora como las que usted y yo ocupamos a diario. Crear un algoritmo cuántico no es tarea fácil, pues dicho algoritmo debe resolver el problema para el que fue diseñado y, además, ser más rápido que cualquier algoritmo convencional pensado para resolver el mismo problema. Entre las técnicas utilizadas para construir algoritmos cuánticos están la Transformada Cuántica de Fourier y las Caminatas Cuánticas. El objetivo principal de este artículo es presentar a usted los elementos fundamentales de las caminatas cuánticas y su empleo en el desarrollo de algoritmos.

Comenzaremos nuestra exposición repasando de manera sucinta las tres componentes fundamentales de la teoría de la computación, además un área de la algorítmica esencial para nuestro análisis: los algoritmos estocásticos, esto es, los procedimientos que emplean distribuciones de probabilidad en su ejecución. Esta información servirá para presentar el concepto de caminata aleatoria y luego extenderlo al mundo de la mecánica cuántica, y así plantear los modelos discreto y continuo de las caminatas cuánticas. La penúltima parte de este artículo consiste en la presentación de algoritmos basados en caminatas cuánticas, seguida de algunas conclusiones.

Modelos computacionales determinísticos y no-determinísticos

La teoría de la computación se divide en tres áreas de estudio, a saber:

1. Teoría de autómatas, cuyo objetivo es la creación de modelos matemáticos de computadoras. Un ejemplo de estos modelos es la máquina de Turing.
2. Teoría de la computabilidad. Dado un problema P y el modelo matemático M de una computadora, esta disciplina estudia si dicho problema P puede ser resuelto, en principio, con el modelo M, siendo válido suponer que se cuenta con una cantidad ilimitada de recursos (por ejemplo, tiempo o memoria).
3. Teoría de la complejidad. Suponga que tenemos un modelo computacional M y un problema P que se puede resolver con un algoritmo *A* implantado en el modelo M. La pregunta que debe responder esta rama de la computación es: ¿cuántos recursos hay que invertir para ejecutar *VVVVAA* en M? En otras palabras, la teoría de la complejidad cuantifica el costo (tiempo o energía, por ejemplo) de ejecutar un algoritmo.
4. Existen varias formas de ejecutar algoritmos en modelos computacionales. Uno de estos métodos, llamado *cómputo determinístico*, consiste en crear algoritmos que obedezcan la siguiente regla: para cualquier paso S_{i+1} de un algoritmo *A*, siempre es posible determinar, con toda certeza, el paso S_{i+1}. En otras palabras, un algoritmo determinístico tiene un comportamiento predecible y exacto (visto desde las matemáticas, la relación entre un nodo y sus hojas es siempre una función, pues sólo hay una hoja por nodo).

Otro método, llamado *cómputo no-determinístico*, consiste en obedecer la siguiente regla: para un paso S_i arbitrario del algoritmo *A*, existen *varios* pasos siguientes s_{i+1}^j, donde $j \in \{1,2,...,m\}$ es un índice que corre sobre el conjunto de los *m* pasos que siguen a S_i. En este caso, el nodo tiene una relación no funcional con sus hojas, pues *en general* hay más de una hoja por nodo.

Estos tipos de cómputo se pueden visualizar como árboles al estilo de la figura 1, en la que el método determinístico se representa con un árbol con una sola derivación, en tanto que los procedimientos no-determinísticos permiten que, de un nodo dado, aparezcan varias ramificaciones. Cada ramificación representa un proceso computacional que se ejecuta *al mismo tiempo* que todos los demás.

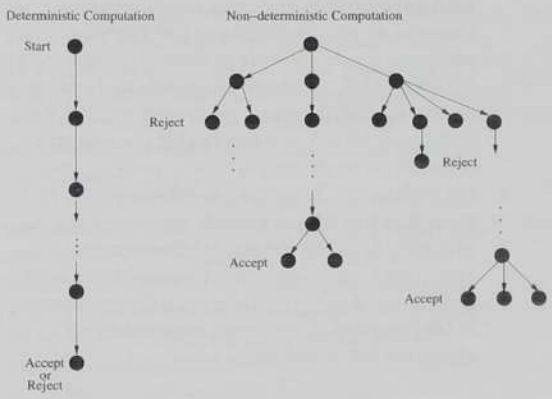

Figura 1. Cómputo determinístico y no-determinístico.

De los dos métodos presentados, el cómputo determinístico se ajusta perfectamente a la noción de disponibilidad de recursos, en tanto que en este mismo rubro, el cómputo no-determinístico se antoja irreal. Luego, ¿porqué es este método un tema de estudio en la ciencia computacional? La respuesta es que el cómputo no-determinístico no escatima la cantidad de recursos disponibles pues su objetivo es averiguar si es posible, al menos en principio, ejecutar un algoritmo dado, aunque ello implique suponer el uso de una cantidad infinita de recursos. No es lo mismo no poder resolver un problema que sólo tener que invertir muchos recursos en lograrlo.

Entre los diversos modelos computacionales sobresalen las *máquinas de Turing*, consideradas como

el modelo computacional más poderoso creado a la fecha por las siguientes razones:

- Cualquier problema resuelto por un modelo computacional distinto de la máquina de Turing (como los autómatas finitos) puede ser también resuelto por una máquina de Turing.
- En consecuencia, cualquier problema resuelto con una computadora construida al día de hoy también puede ser resuelto por una máquina de Turing.

Existen versiones determinística y no-determinística de las máquinas de Turing. Estas versiones son equivalentes en su capacidad para ejecutar algoritmos, pero difieren en el tiempo que tardan en hacerlo:

1. Aquellos algoritmos que al ejecutarse en una máquina **determinística** de Turing efectúen una cantidad de pasos acotada superiormente por una *función polinomial* $f(n)$ *en el número de datos de entrada, i.e.* $f(n)=\sum \alpha_i n^i$, donde n es el número de datos de entrada del algoritmo, reciben el nombre de algoritmos **P** (un problema es **P** si encuentra solución en un algoritmo **P**).
2. Los algoritmos que al ejecutarse en una máquina **no-determinística** de Turing consumen una cantidad de pasos acotada por una *función polinomial g(n) en el número de datos de entrada, i.e.* $g(n)=\sum \beta_i n^i$, donde n es el número de datos de entrada del algoritmo, reciben el nombre de problemas **NP** (un problema es **NP** si encuentra solución en un algoritmo **NP**).
3. Por último, un algoritmo L es **NP-completo** si y sólo si L es **NP** y se cumple que, para todo problema L_i en **NP**, es posible transformar al algoritmo L_i en el algoritmo L usando solamente una cantidad polinomial de pasos (un problema es **NP-completo** si encuentra solución en un algoritmo **NP-completo**).

Los algoritmos **P** son vistos con muy buenos ojos por la comunidad de científicos computacionales, pues utilizan una cantidad aceptable de tiempo en su ejecución. Para compr ender mejor este concepto, analicemos el caso contrario, el de los algoritmos **NP**.

Dada la disparidad de recursos disponibles entre los modelos determinístico y no-determinístico, la ejecución de un algoritmo **NP** en una máquina determinística de Turing requiere una cantidad de recursos que crece exponencialmente (o factorialmente) en el número de datos de entrada[1]. La explicación de este fenómeno radica en el hecho de que, para un problema **NP** y un **NP-completo**, el espacio de soluciones posibles es muy grande, y explorarlo *exhaustivamente* requiere muchos recursos.

Para el lector interesado en los fundamentos matemáticos de la teoría de la computación, se recomienda ampliamente consultar las referencias [4-6].

Algoritmos estocásticos

Se han propuesto diversos caminos para hacer del cómputo no-determinístico algo más cercano a lo que es posible hacer con una computadora real. En uno de ellos, la computadora escoge *aleatoriamente* (i.e. usando una distribución de probabilidad) una de las ramas del árbol no-determinístico y la ejecuta. Esto es, si el algoritmo está en el paso S_i, entonces el siguiente *y único* paso S_{i+1} se escoge (usando una distribución de probabilidad) del conjunto de pasos $\{s^j_{i+1} | j \in \{1,...,m\}\}$. Este proceso se conoce con el nombre de *cómputo probabilístico* y, aunque no es precisamente equivalente al cómputo no-determinístico, su gran ventaja es que es posible implantarlo en una computadora convencional (el único problema práctico es que no es posible generar números totalmente aleatorios en una computadora convencional, mas los números pseudo-aleatorios son, en general, suficientemente buenos para muchas aplicaciones).

Estamos ya en posibilidad de definir un concepto crucial: un *algoritmo estocástico* es un algoritmo cuya sucesión de pasos (i.e. cuya evolución en el tiempo) se produce usando una distribución de probabilidad. Dicho de otra forma, un algoritmo estocástico es un procedimiento ejecutado en una máquina capaz de hacer cómputo probabilístico.

Los algoritmos estocásticos juegan un papel central en el estudio de los problemas NP-completos, pues gracias a ellos es posible encontrar soluciones, para dichos problemas, que consumen menos pasos que los que requeriría un algoritmo de fuerza bruta, i.e. un algoritmo que explorase, exhaustivamente, el espacio completo de posibles soluciones.

Un ejemplo de los problemas beneficiados por la existencia de algoritmos estocásticos es el **3-SAT**, definido de la siguiente manera:

Problema 3-SAT. Sea $S=\{x_1,x_2,...,x_n\}$ un conjunto de variables booleanas (i.e. $x_i \in \{0,1\} \forall i \in \{1,2,...,n\}$) y $C=\bigcap_i \left[\bigcup_{j=1}^{3} x_i\right]$, esto es, C es una conjunción de disyunciones. El problema 3-SAT consiste en encontrar, si existe, un conjunto de valores para las variables x_i tales que C sea verdadera ($C=1$).

El mejor algoritmo conocido a la fecha para la solución de 3-SAT fue propuesto por U. Schöning en 1999 [7], el cual se construyó empleando un proceso estocástico (i.e. cuya evolución es función de una distribución de probabilidad) conocido bajo el nombre de *caminata aleatoria*. En [8] se presentó una mejora de [7], pero la idea fundamental es la misma: usar una caminata aleatoria para construir el algoritmo.

Para cerrar este capítulo y estar en condiciones de presentar las ideas fundamentales de las caminatas cuánticas, permítame mostrar en detalle las ideas fundamentales de una caminata aleatoria.

Caminatas aleatorias

El modelo básico de las caminatas aleatorias es el movimiento de una partícula (llamado caminante) sobre puntos discretos distribuidos en una línea sin restricciones. El sentido del movimiento del caminante (izquierda o derecha) depende de un sistema bivaluado (como una moneda) cuyos valores, para cada paso, dependen de la probabilidad.

Para ejemplificar jocosamente el concepto anterior, suponga que tenemos a la rana Froggy y una moneda, como se muestra en la Fig. 2.

Froggy se desplazará sobre una línea y su movimiento dependerá del resultado de tirar volados (Froggy es una rana obediente). Si el resultado del volado es 'sol' entonces Froggy da un brinco a la derecha (por ejemplo, si la rana está en '0' antes del volado, entonces se mueve al sitio marcado con '1') y si el resultado es 'águila' entonces Froggy se mueve a la izquierda (del sitio '0' al sitio '-1'). Después de muchos volados (digamos, un millón), uno puede hacer varias preguntas interesantes, por ejemplo: ¿cuál es la probabilidad de que Froggy esté en el lugar '100'?

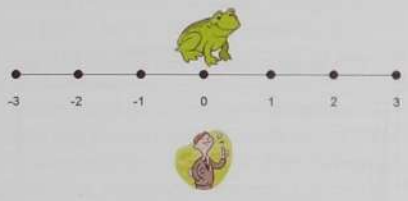

Figura 2. Cada paso de la caminata consiste en que Froggy se mueva a la izquierda o derecha. El sentido de este movimiento depende del resultado del volado.

La ecuación que nos permite calcular la probabilidad de encontrar a nuestra rana en el lugar k, suponiendo que el movimiento comenzó en la posición 0 y que Froggy se ha movido n veces (esto es, que se han tirado n volados) está dada por la distribución binomial

$$P_{0k}^{n} = \binom{n}{\frac{1}{2}(k+n)} p^{(n+k)/2} q^{(n-k)/2}$$

la cual se muestra en la figura 3.

Dos propiedades importantes de la caminata aleatoria sobre una línea son: 1) la varianza de la distribución binomial es proporcional al número de pasos ejecutados, i.e. $\sigma^2 = O(n)$; 2) *la forma* de la distribución binomial *no* depende del punto de partida. Lo que sucede al cambiar el punto de partida (por ejemplo, poner a Froggy en 10 en vez de 0), es que la gráfica se desplazará a la izquierda o derecha,

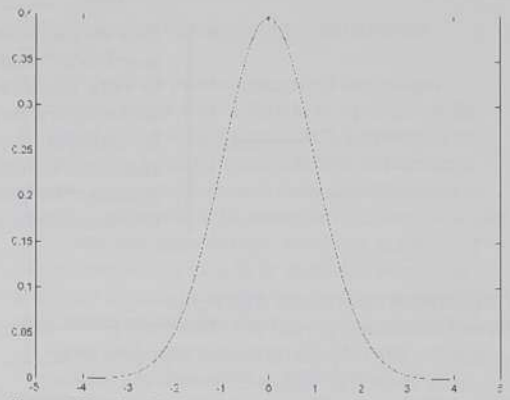

Figura 3. Distribución binominal.

pero la forma será la misma. Esta invariancia de la forma de la distribución respecto del punto de partida es una característica fundamental de las cadenas de Markov, de las cuales las caminatas aleatorias son un caso especial.

Naturalmente, las caminatas aleatorias se pueden extender de varias maneras. Por ejemplo, es posible definir caminatas sobre líneas con barreras absorbentes o reflejantes, sobre grafos y, además, con movimientos hechos en tiempos infinitesimales ($t \geq 0$), en vez de tiempos discretos. Para el lector interesado en la formulación de procesos estocásticos en grafos y su aplicación en algoritmos, se recomienda consultar [9-12] y demás fuentes citadas en el capítulo III de [12].

El éxito de varios algoritmos estocásticos en la solución de problemas NP, en particular algoritmos que emplean caminatas aleatorias, ha sido una importante fuente de inspiración para desarrollar nuevos modelos de caminatas, ahora bajo las leyes de la mecánica cuántica. En la siguiente sección exploraremos las definiciones y características principales de las caminatas cuánticas.

Caminatas cuánticas

La existencia de caminatas aleatorias discretas (cadenas de Markov) y continuas (procesos de Markov) ha llevado también a sugerir dos tipos de caminatas cuánticas: discretas y continuas.

Antes de entrar en materia, subrayo que, a pesar de su aplicación común, existe una diferencia primera y fundamental entre las caminatas aleatorias y las cuánticas: las caminatas aleatorias son entes matemáticos que se utilizan para modelar fenómenos físicos, en tanto que las caminatas cuánticas son representaciones matemáticas de procesos físicos. Este origen físico de las caminatas cuánticas permite pensar en ellas no sólo como herramientas para la construcción de algoritmos, sino también como elementos de prueba para determinar si una computadora tiene, en efecto, propiedades cuánticas.

Una de las razones que explican la poderosa influencia que la mecánica cuántica y la teoría de la computación han tenido en la vida moderna es que los paradigmas, teorías y desarrollos tecnológicos de cada una han provocado avances en la otra. Así, las computadoras han sido herramientas fundamentales en la simulación de sistemas físicos y la creación de las computadoras actuales fue posible sólo gracias al profundo conocimiento que tenemos sobre semiconductores.

Caminatas cuánticas discretas

En este modelo participan dos elementos: el caminante y la moneda (la misma idea que con la caminata aleatoria). Ambos elementos son sistemas físicos cuyo comportamiento se modela y cuantifica mediante los principios y leyes de la mecánica cuántica [13,14].

El modelo más sencillo de este tipo de caminata se ejecuta sobre un espacio discreto unidimensional (esto es, una recta con nodos). La evolución de esta caminata se lleva a cabo aplicando un *operador de evolución* consistente en dos operaciones cuánticas (dos operadores unitarios): la primer operación hace que la moneda entre en un estado cuántico que asemeja un volado, y la segunda operación hace que los componentes cuánticos de la moneda interactúen con el caminante, de tal suerte que la probabilidad de encontrar al caminante en distintos puntos de la línea sea una función del tiempo. La aplicación de las dos operaciones cuánticas es equivalente a un paso algorítmico, una operación elemental. La ecuación que define una caminata cuántica discreta es:

$$|\psi\rangle_n = U^{\otimes n}|\psi\rangle_0$$

Donde $|\psi\rangle_0$ es el símbolo que representa el estado inicial total de la moneda y el caminante, $U^{\otimes n}$ representa n aplicaciones del operador de evolución U (i.e. de las dos operaciones cuánticas: volado más desplazamiento) y $|\psi\rangle_n$ es el símbolo que representa el estado de la caminata cuántica (moneda más caminante) después de n pasos.

La ejecución de varias caminatas cuánticas discretas con estados iniciales idénticos y operaciones cuánticas iguales permite generar distribuciones de probabilidad como las mostradas en las figuras 4 y 5. Estas gráficas ejemplifican algunas propiedades importantes de las caminatas cuánticas, a saber:

1. Las caminatas cuánticas discretas tienen una varianza que crece proporcionalmente al cuadrado del número de pasos, i.e. $\sigma_q^2(n) = O(n^2)$ [13-15]. Este hecho es importante por dos motivos: 1) la varianza de una caminata clásica es proporcional sólo al número de pasos ejecutados (i.e. $\sigma_q^2(n) > \sigma^2(n)$), y 2) esta diferencia entre las varianzas clásica y cuántica puede ser utilizada para aumentar la velocidad de ejecución de un algoritmo basado en caminatas cuánticas, respecto del correspondiente algoritmo clásico diseñado con una caminata aleatoria.
2. La forma de la distribución de probabilidad generada con una caminata cuántica depende del estado inicial. Este hecho es importante pues el estado inicial del caminante y la moneda puede ser utilizado como un parámetro computacional. De hecho, la interacción de la moneda con el medio ambiente puede generar la distribución "top-hat" [16], una gráfica cuasi uniforme muy agradable a la vista de un científico computacional.

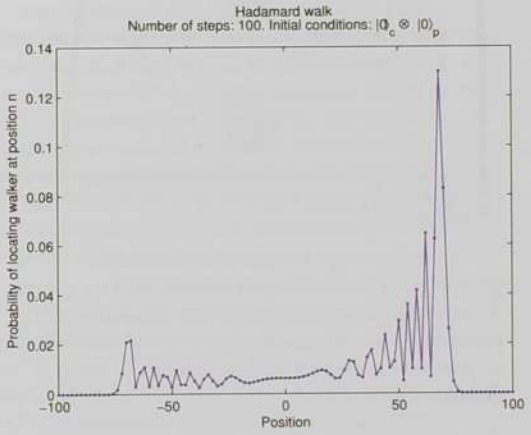

Figura 4. Distribución de probabilidad (posición vs probabilidad de encontrar al caminante en dicha posición) generada con $|\psi\rangle_0 = |0\rangle_{moneda} \otimes |0\rangle_{camino}$.

El operador de evolución de esta caminata cuántica es

$$U = \left[\left\{\frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right)\right\} \otimes I\right]\left[|0\rangle\langle 0| \otimes \sum_i |i+1\rangle\langle i| + |1\rangle\langle 1| \otimes \sum_i\right.$$

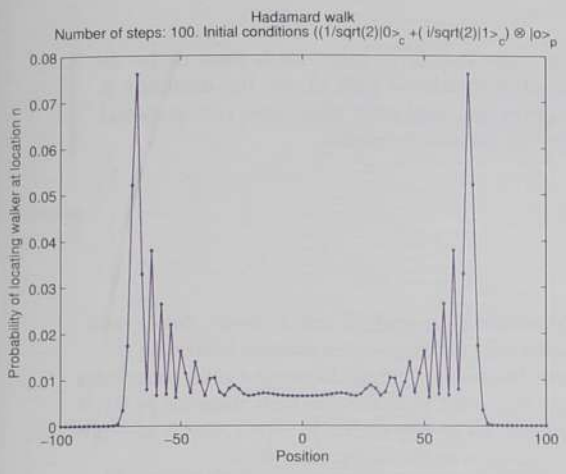

Figura 5. Distribución de probabilidad (posición vs probabilidad de encontrar al caminante en dicha posición) generada con

$$|\psi\rangle_0 = \frac{1}{\sqrt{2}}\left(|0\rangle_{mon} + i|1\rangle_{mon}\right) \otimes |0\rangle_{cam},$$

El operador de evolución de esta caminata cuántica es el mismo que el de la figura 4.

Caminatas cuánticas continuas

Este tipo de caminatas requiere un solo sistema físico, el caminante. La partícula que hace las veces de la moneda no es necesaria en este esquema.

En este modelo, se aplica una operación cuántica (un Hamiltoniano, para los lectores expertos en mecánica cuántica) en cualquier momento, i.e. el tiempo de ejecución de la caminata no es más una variable discreta, sino una variable real positiva [17]. Las caminatas cuánticas continuas para las cuales se han encontrado aplicaciones algorítmicas están definidas para grafos bidimensionales (más sobre esto en la siguiente sección).

La ecuación que define a una caminata cuántica continua es

$$i\frac{d\langle a|\psi(t)\rangle}{dt} = \sum_b \langle a|H|b\rangle\langle b|\psi(t)\rangle$$

Donde H es una representación matricial del operador Hamiltoniano, los escalares a, b representan nodos de un grafo bidimensional G, $\langle a|H|b\rangle$ es un coeficiente relacionado con la probabilidad de que el caminante realice una transición entre a y b, y $|\psi\rangle$ representa al caminante.

Propiedades varias de las caminatas cuánticas

Posiblemente la primera pregunta que surge en torno a las caminatas cuánticas es: ¿por qué se ha eliminado el adjetivo "aleatorias"? La razón es que la evolución de un sistema cuántico cerrado (esto es, que no interactúa con el medio ambiente) es un proceso *determinístico*. Lo probabilístico llega cuando se intenta averiguar el lugar en el que se encuentra el caminante (o la cara de la moneda), pues en la lógica de la mecánica cuántica, conocer la posición del caminante es equivalente a *medir* una propiedad de la partícula que hace las veces del caminante, y la medición en mecánica cuántica es un proceso inherentemente probabilístico. El mismo argumento se aplica a la moneda.

¿Qué significa que la medición en mecánica cuántica sea un proceso inherentemente probabilístico? Que los resultados posibles de una medición aparecerán (serán revelados al científico) de acuerdo a una distribución de probabilidad, sin importar lo cuidadoso que sea el investigador ni la precisión o calibración de los instrumentos.

Esta naturaleza probabilística de la mecánica cuántica dista mucho de ser una propiedad intuitiva para el científico computacional o cualquier otro humano; de hecho, ha sido motivo de controversia desde el nacimiento de la teoría cuántica hasta nuestros días (por ejemplo, revisar [18-21]). Para un científico computacional interesado en desarrollar algoritmos cuánticos, aprender estas nuevas formas de razonar será parte fundamental de su proceso educativo.

Otra pregunta que generalmente surge tiene que ver con la estricta necesidad de monedas en las caminatas cuánticas discretas. Publicaciones recientes [22,23] prueban que, si el investigador está interesado solamente en la varianza de la distribución de probabilidad generada por la caminata cuántica, entonces la moneda no es necesaria. Más aún, y esto es de llamar la atención, para obtener la mejora en la varianza basta con usar un sistema físico clásico (por ejemplo, una onda electromagnética [24]). Gracias a estos análisis, ha sido posible demostrar que existe una forma analítica de conversión entre caminatas cuánticas discretas y continuas [23].

Sin embargo, si uno está interesado en propiedades distintas de la varianza, el uso de monedas y el carácter cuántico de las caminatas que hemos estudiado es indispensable. Ejemplos de estas propiedades son la forma específica de las distribuciones de probabilidad generadas y la generación de correlaciones cuánticas entre moneda y caminante o entre caminantes (ver, por ejemplo, las referencias [12,25]).

Crear un algoritmo cuántico no es tarea fácil, pues dicho algoritmo debe resolver el problema para el que fue diseñado y, además, ser más rápido que cualquier algoritmo convencional pensado para resolver el mismo problema.

Por último en esta sección, deseo mencionar que el estudio de caminatas cuánticas se ha extendido a diversos espacios (grafos) y modalidades de interacción. Para el lector interesado, se recomienda consultar las fuentes citadas en [12].

Algoritmos basados en caminatas cuánticas

Al día de hoy, los algoritmos basados en caminatas cuánticas resuelven diversas instancias de un problema de búsqueda, que en forma abstracta se plantea así: dado un espacio de estados traducible a un grafo G, encuentre un estado particular, *el cual tiene una marca distintiva*, a través de la ejecución de una caminata cuántica en G. El planteamiento se generaliza fácilmente para localizar un conjunto de estados marcados, en vez de uno solo.

Por supuesto, con la lectura del párrafo anterior, una pregunta asalta la mente: ¿es razonable suponer que el nodo buscado tendrá siempre una marca distintiva? La respuesta se puede dar en dos planos distintos:

1. Para aplicaciones concretas de algoritmos de búsqueda, en común estar en posibilidad de distinguir el nodo que buscamos del resto.
2. En algunos problemas cuya solución algorítmica está inspirada en procesos físicos, es posible garantizar que el nodo buscado está marcado por el valor mínimo (o máximo) de la propiedad física incorporada en el algoritmo.

A efecto de caracterizar estos problemas en los que hay que buscar elementos reconocibles (i.e. marcados), la ciencia computacional provee de una abstracción llamada oráculo. Un *oráculo* es una máquina abstracta utilizada para estudiar problemas de decisión. A esta máquina se le puede pensar como una caja negra. Los oráculos son elementos utilizados ampliamente en la construcción de algoritmos basados en caminatas cuánticas. A continuación, se presentan algunos algoritmos basados en caminatas cuánticas y que emplean oráculos.

Viaje a través de un hipercubo. Para estudiar este algoritmo, definimos antes lo siguiente: un hipercubo es un grafo G con 2^n nodos, donde cada nodo lleva por etiqueta un número binario de n bits. Dos nodos a, b del hipercubo están conectados por una arista (a,b) si y sólo si las etiquetas de a y b difieren en un solo bit, i.e. $|a-b|=1$, donde $|a-b|$ es la distancia de Hamming entre a, b.

Un ejemplo de hipercubo con $n=3$ se muestra en la figura 6.

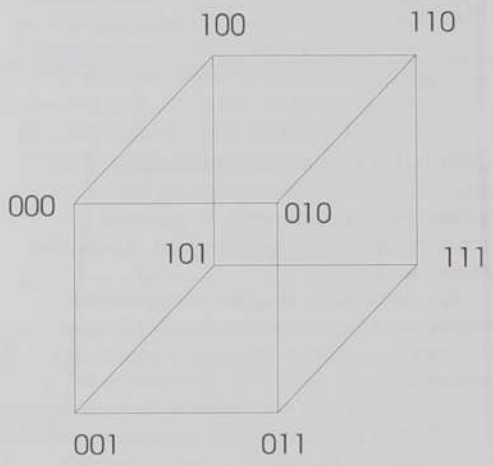

Figura 6. Hipercubo con $n=3$.

Pensemos ahora en el siguiente problema: dado un hipercubo, calcule el tiempo (i.e. el número de pasos) que tardaría un algoritmo en cruzar la distancia entre dos nodos arbitrarios (a,b). Este problema tiene solución a través de un algoritmo clásico [17] y otro cuántico [26], en ambos casos polinomiales (i.e. son algoritmos **P**). El algoritmo cuántico propuesto en [26] emplea una caminata cuántica discreta y un oráculo.

Otro problema de búsqueda, propuesto y solucionado en [27] empleando una caminata cuántica discreta, se define en el siguiente párrafo.

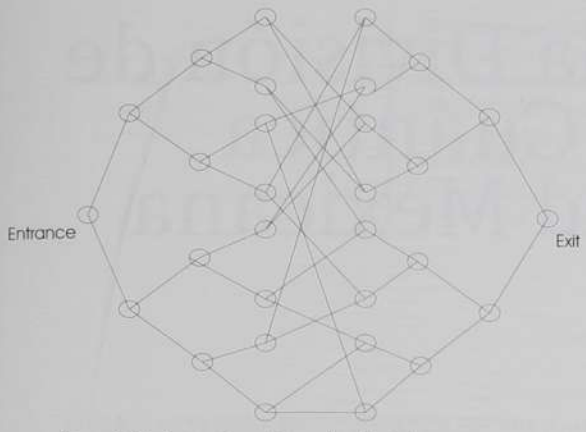

Figura 7. Árbol con uniones intermedias aleatorias.

Elementos distintos (en inglés, *element distinctness problem*). Sea S una lista de cadenas de caracteres (*strings*) definidos sobre el conjunto $\{0,1\}$ separados entre sí por el símbolo $\#$, i.e. $S = s_1 \# s_2 \# s_3 \# \ldots$, donde $s_i \in \{0,1\}$. Determine si todos los *strings* son distintos entre sí.

Aceleramiento exponencial usando una caminata cuántica. Para terminar esta sección, deseo presentar a usted un último algoritmo, éste basado en una caminata cuántica continua y desarrollado en [17]. El problema a resolver se puede visualizar en la figura 7 y consiste en comenzar una caminata en el nodo "entrance" para terminar en el nodo "exit". Dada la estructura irregular del centro de este grafo, formada por uniones aleatorias entre las hojas de los árboles izquierdo y derecho, es posible demostrar dos cosas [17]: 1) no es posible construir un algoritmo clásico que haga el recorrido solicitado en tiempo polinomial, y 2) es posible construir un algoritmo que con alta probabilidad, logre hacer el recorrido solicitado en tiempo polinomial

Finalmente, y a manera de conclusión, destaquemos que las caminatas cuánticas forman una disciplina nueva y apasionante, hija de la unión de la mecánica cuántica y la teoría de la computación. Tanto las propiedades físicas y matemáticas de las caminatas cuánticas como su aplicación en el desarrollo de algoritmos son campos de reciente creación en los que hay oportunidades de crecimiento para físicos, científicos computacionales e ingenieros, en las áreas de investigación y desarrollo . ●

[Notas]

[1] La excepción a esta regla es que se descubra que el problema asociado al algoritmo NP encuentra también solución con un algoritmo P. En este caso, el problema deja de pertenecer a la esfera de los NP y se vuelve un problema P.

[Referencias]

[1] Brown, Julian. *The quest for the quantum computer*. USA. Touchstone, 2001.
[2] Volpi, Jorge. *En busca de Klingsor*. México. Seix Barral, 1999.
[3] Aczel, Amir D. *Entanglement*.USA. Plume (Penguin group), 2003.
[4] Sipser, Michael. *Introduction to the theory of computation*. USA. PWS Publishing, 2005.
[5] Papadimitriou, Christos. *Computational Complexity*. USA. Addison-Wesley, 1995.
[6] Savage, John. *Models of Computation*. USA. Addison-Wesley, 1998.
[7] Schöning, Uwe, 1999, "A probabilistic algorithm for k-sat and constraint satisfaction problems", Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS), IEEE, pp. 410–414.
[8] Iwama, Kazuo y Tamaki, Suguro, 2003, "Improved upper bounds for 3-SAT", Electronic Colloquium on Computational Complexity, report 53.
[9] Lovász, László. *Random walks on graphs: a survey*. Combinatorics, Paul Erdös is eighty, vol. 2 (Ed. D. Miklóz, V.T. Sós y T. Szönyi). János Mathematical Society, Budapest, pp. 353-398, 1996.
[10] Motwani, Rajeev y Raghavan, Prabhakar. *Randomized algorithms*. Cambridge University Press, 1995.
[11] Woes, Wolf. *Random walks on infinite graphs and groups*. Cambridge tracts in mathematics (138), Cambridge University Press, 2000.
[12] Venegas Andraca, Salvador Elías. *DPhil thesis: Discrete Quantum Walks and Quantum Image Processing*. The University of Oxford, 2006. Disponible en http://www.mindsofmexico.org/sva/dphil.pdf
[13] Meyer, David, 1996, "From quantum cellular automata to quantum lattice gases", *Journal of Statistical Physics*, vol. 85, pp. 551-574.
[14] Nayak, Ashwin y Vishwanath, Ashvin, 2000, "Quantum walk on the line", *quant-ph/0010117*.
[15] Kempe, Julia, 2003, "Quantum random walks - an introductory overview", *Contemporary Physics*, vol. 44(4), pp. 302-327.
[16] Kendon, Vivian, 2006, "A random walk approach to quantum algorithms", *Philosophical Transactions of the Royal Society A*, vol. 364, pp. 3407-3422.
[17] Childs, Andrew, Cleve, Richard, Deotto, Enrico, Farhi, Edward, Gutmann, Sam y Spielman, Daniel, 2003, "Exponential algorithmic speedup by quantum walk", *Proceedings of the 35th Association for Computing Machinery Symposium on Theory of Computing (STOC 2003)*, pp. 59-68.
[18] Einstein, Albert. *Ideas and Opinions*. Wings Books, 1954.
[19] Heisenberg, Werner. *Physics and Philosophy*. Penguin Books Ltd, 2000.
[20] Nielsen, Michael and Chuang, Isaac. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
[21] Feynman, Richard, Leighton, Robert y Sands, Matthew. *The Feynman Lectures on Physics, Vol. III: Quantum Mechanics*. Addison-Wesley, 1965.
[22] Patel, Apoorva, Raghunathan, K y Rungta, Pranaw, 2005, "Quantum random walks do not need a coin toss", *Physical Review A*, vol. 71, 032347.
[23] Strauch, Frederick, 2006, "Connecting the discrete and continuous-time quantum walks", *Physical Review A*, vol. 74, 030301.
[24] Knight, Peter, Roldán Eugenio y Sipe, John, 2003, "Quantum walk on the line as an interference phenomenon", *Physical Review A* 68, 020301.
[25] Kendon, Vivian, y Maloyer, Olivier, 2007, "Decoherence vs entanglement in coined quantum walks", *New Journal of Physics* 9, 87.
[26] Shenvi, Neil, Kempe, Julia y Whaley, Birgitta, 2003, "A Quantum Random Walk Search Algorithm", *Physical Review A*, vol. 67(5), 050237.
[27] Ambainis, Andris, 2004, "Quantum walk algorithm for element distinctness", *Proceedings of the 45th IEEE Symposium on Foundations of Computer Science*, pp. 22-31.

Creación de la División de Información Cuántica de la Sociedad Mexicana de Física

HASTA AHORA, EN MÉXICO SE HAN HECHO ESFUERZOS AISLADOS PARA REALIZAR INVESTIGACIÓN EN EL ÁREA DE LA INFORMACIÓN CUÁNTICA, SIN EMBARGO, ESTA TENDENCIA ESTÁ CAMBIANDO. ASÍ LO MUESTRA, POR UNA PARTE, LA FUNDACIÓN DE LA DIVISIÓN DE INFORMACIÓN CUÁNTICA DE LA SOCIEDAD MEXICANA DE FÍSICA Y, POR OTRA, MOVILIZACIONES CONJUNTAS DE ACADÉMICOS PARA REALIZAR PROYECTOS DE GRAN IMPORTANCIA, COMO ES EL MEGAPROYECTO TITULADO INFORMACIÓN CUÁNTICA Y FOTÓNICA EN EL QUE PARTICIPAN ONCE INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL PAÍS. TODO ELLO PARA LOGRAR LA INCORPORACIÓN DE MÉXICO A LA LLAMADA SEGUNDA REVOLUCIÓN CUÁNTICA, QUE ACTUALMENTE TIENE LUGAR EN EL MUNDO DE LA CIENCIA.

Octavio Castaños Garza

Las investigaciones actuales muestran que fenómenos cuánticos característicos, que causan enorme sorpresa desde el punto de vista clásico, pueden utilizarse para realizar tareas de interés práctico e incluso ser más eficientes que cualquier otro método conocido en el área. Estos hechos han llamado la atención a investigadores de diversos campos del conocimiento como son: físicos, científicos de la computación, matemáticos e ingenieros eléctricos.

Por ejemplo, en criptografía cuántica,[1] la propiedad de no-clonación de los estados cuánticos y el fenómeno del entrelazamiento ayudan a lograr el intercambio seguro de claves secretas entre las partes, de manera que en la actualidad se reconoce como una alternativa viable a los métodos convencionales de encriptación. No está lejano el día en que la seguridad de una transacción dependerá tanto de la criptografía tradicional, basada en la dificultad de encontrar los factores de números muy grandes, como de la mecánica cuántica para asegurar que no haya habido espías en la transmisión.

La tecnología de la computación se ha transformado de acuerdo con el tipo de realización física que se utiliza. Se ha transitado de computadoras mecánicas a las de bulbos y transistores y, finalmente, a las de circuitos integrados. El tamaño de los componentes de estas últimas se ha reducido considerablemente, por lo que se piensa que a este ritmo de miniaturización pronto alcanzaremos tamaños o escalas en que necesariamente se verán involucrados sistemas atómicos y ópticos, cuya dinámica es gobernada por las leyes de la mecánica cuántica. Deberán entonces aparecer nuevas tecnologías basadas en aspectos mecánico cuánticos. Es necesario mencionar que, al menos potencialmente, la computación cuántica

OCTAVIO CASTAÑOS GARZA Investigador titular C de tiempo completo del Instituto de Ciencias Nucleares (UNAM). Presidente fundador de la División de Información Cuántica. Director del ICN-UNAM de 1996 a 2004. Premiado en 1993 con la Medalla Marcos Moshinsky por sus contribuciones en el área de la física teórica. ocasta@nucleares.unam.mx

La investigación teórica y experimental en computación cuántica ha despertado un gran interés en todo el mundo. Aunque faltan todavía muchos años de trabajo y desarrollo para tener una computadora cuántica comercial, el avance en la comprensión de los fenómenos del mundo cuántico será de gran relevancia tanto para la ciencia básica como para la aplicada. Manifestaciones de las tecnologías cuánticas por medio de la criptografía son ya una realidad.

tiene una gran capacidad para almacenar una mayor cantidad de datos y resolver problemas, principalmente los no polinomiales, denominados así por los expertos en teoría de la complejidad.[2]

En consecuencia, la investigación teórica y experimental en computación cuántica ha despertado un gran interés en todo el mundo. Aunque faltan todavía muchos años de trabajo y desarrollo para tener una computadora cuántica comercial, el avance en la comprensión de los fenómenos del mundo cuántico será de gran relevancia tanto para la ciencia básica como la aplicada. Manifestaciones de las tecnologías cuánticas por medio de la criptografía son ya una realidad. La respuesta de otros países latinoamericanos ha sido de un decidido apoyo a este campo de investigación mediante la creación de institutos de investigación. En Chile, por ejemplo, ya existe el *Center for Optics and Quantum Information*, y en Brasil, el *Institute of Quantum Information*. Estos grupos ya han incidido internacionalmente tanto por su trabajo teórico como por su trabajo experimental.

Información cuántica

Para realizar cualquier proceso de cómputo o manipulación de información es necesario codificar la información en los estados de un sistema físico. Desde 1961, año en que fue establecido el principio de Landauer, se reconoce que son las leyes de la física las que nos dictan cómo guardar, manipular y leer información [1]. Actualmente, en todo proceso de información se utilizan las leyes de la física clásica. Si el mecanismo físico subyacente al protocolo con el que se maneja la información tiene un carácter cuántico, se habla de información cuántica y se deben cumplir las leyes de la mecánica cuántica. Es importante que en México participemos en la llamada segunda revolución de la mecánica cuántica, esto es, se contribuya al desarrollo de la física cuántica de la información.

La teoría de la información clásica maduró el siglo pasado con consecuencias evidentemente trascendentes y conocidas por todos; la posibilidad actual de caracterizar y controlar el estado cuántico de sistemas ópticos y atómicos nos abre la posibilidad de desarrollar la teoría cuántica de la información, que consideramos será la vía natural de progreso y esto, por supuesto, incluye el desarrollo de tecnologías de la comunicación y computación cuánticas. Para participar en ese desarrollo con posibilidades de éxito es necesario impulsar las áreas experimentales de la óptica cuántica y del control atómico. Por otra parte, la tecnología láser asociada ha estimulado fuertemente el desarrollo de las espectroscopias atómica y molecular, y el de la óptica no lineal con aplicaciones en comunicaciones, microelectrónica, medicina y biología.

El establecimiento de la computadora clásica fue el resultado de una discusión importante sobre las ventajas de utilizar una aproximación analógica o una digital en la manipulación de la información. La lógica binaria se impuso y ha resultado sumamente provechosa por su inmunidad al ruido, su simplicidad en las operaciones y la universalidad de sus compuertas. Hoy en día, dicha lógica se lleva a cabo sobre la base de la física del silicio y está vinculada íntimamente a esas limitaciones.

La información, si bien es independiente del proceso físico que la genera y la transforma, no existe sin un ente físico.

La teoría de la información nos dice que, dadas estas leyes físicas, los problemas, en principio, son computables. Sabemos que, por ejemplo, la factorización de números primos se vuelve prohibitivamente difícil al aumentar el número de dígitos y que aún la computadora más rápida que procese de manera clásica la información tomaría tiempos más largos que la edad del Universo para factorizar un número de 100 dígitos. Pero desde principios del siglo pasado aprendimos que existe una descripción más fundamental de la naturaleza: la mecánica cuántica. En los años ochenta, primero R. Feynman y un poco más tarde D. Deutsch concibieron los orígenes de la teoría de la información cuántica

[1]. En 1994, P. Shor mostró que usando las leyes de la mecánica cuántica se puede factorizar números en tiempos exponencialmente menores a los tiempos clásicos [1]. La posibilidad de implementar el algoritmo de Shor ha sido de suma importancia para todas las actividades públicas y privadas que dependen de la encriptación de mensajes con los protocolos tradicionales. Esto a su vez ha dado un nuevo impulso al estudio de la criptografía y a sus posibles conexiones con la mecánica cuántica. Desde entonces, puede decirse, nació el sueño de construir una computadora cuántica y de investigar si con ella será factible encontrar la solución de problemas que clásicamente no ha sido posible resolver. Recientemente, las computadoras cuánticas y la teoría de la información cuántica han recibido gran atención y difusión pública debido a su gran potencial de aplicación para resolver problemas complejos o quizás insolubles en computación clásica.

La tecnología actual está empezando a permitirnos manipular más y no sólo observar sistemas cuánticos individuales; de hecho, puede considerarse que la criptografía cuántica es la primera aplicación de la mecánica cuántica al nivel de sistemas cuánticos individuales. Se han realizado experimentos que nos indican que cuando dos sistemas interactuaron en el pasado, generalmente no es posible asignarles un solo vector de estado a cualquiera de los dos subsistemas. Esta no separabilidad de un sistema cuántico fue primero reconocida por Einstein-Podolsky-Rosen y formulada matemáticamente por Schrödinger, quienes, a partir de los principios de localidad y realidad local, llegaron a la conclusión de que la mecánica cuántica no es una teoría completa [2].

Uno de los avances más significativos para resolver este problema fue realizado por Bell, quien probó que el realismo local implica predicciones sobre las correlaciones de espín en la forma de desigualdades, actualmente llamadas desigualdades de Bell, que pueden ser violadas cuánticamente. Esta última propiedad de la mecánica cuántica también suele llamarse no-localidad. Violaciones de las desigualdades de Bell se han encontrado experimentalmente desde principios de los años setenta por Freedman y Clauser, quienes midieron las correlaciones de la polarización lineal de dos fotones emitidos en cascada por átomos de calcio, y también a inicios de la década siguiente en experimentos de Aspect [2], permitiendo en estos últimos que los polarizadores tengan orientaciones dinámicas. Más recientemente se han ido eliminando los posibles problemas tanto de localidad como de eficiencia de los detectores para considerar la violación del realismo local como un hecho establecido [3].

Se ha demostrado que el entrelazamiento tiene aplicaciones importantes, ya que puede usarse como recurso para comunicaciones de estados cuánticos, un proceso que ha sido llamado teletransportación cuántica [3]. En este proceso, un estado cuántico es transmitido por el uso de un par de partículas en un estado de Bell compartido por un mensajero y un destinatario. El fenómeno llamado entrelazamiento, junto con el principio de superposición, constituyen los elementos clave para la utilización de sistemas cuánticos en la teoría de la información.

La evolución de la tecnología electrónica hacia una tecnología cuántica no es inmediata; dentro de este proceso, el desarrollo de la tecnología fotónica está jugando un papel fundamental. El área de comunicaciones es un claro ejemplo de este hecho, como lo demuestra el revolucionario avance que implicó el reemplazo de cables conductores de cobre por la fibra óptica. Del mismo modo se prevé que, en términos prácticos, el desarrollo de una computadora óptica o fotónica precederá al de una computadora cuántica. Sin embargo, sólo llevando a cabo investigación teórica y experimental paralela en ambas áreas, fotónica y cuántica, será posible llegar a un progreso tecnológico.

Uno de los avances más espectaculares de la óptica atómica en las últimas décadas es el logro de la condensación Bose-Einstein. Ésta fue posible gracias a previos desarrollos, igualmente importantes, de técnicas para la manipulación tanto de partículas cuánticas como de partículas macroscópicas. En particular, el enfriamiento láser y las trampas ópticas y magnéticas han permitido enfriar átomos neutros a energías lo suficientemente pequeñas para que puedan atraparse con campos electromagnéticos. En las trampas ha sido posible evaporar los átomos más calientes en forma controlada y así alcanzar la temperatura y densidad críticas para la formación del condensado de Bose-Einstein. Éstos son ahora utilizados como una fuente de átomos coherentes por excelencia, útiles para diversas aplicaciones como la metrología, la investigación de estados enredados, la interferometría atómica, la teletransportación y el procesamiento de información cuántica [4].

La realización en el laboratorio de procesadores de información cuántica requiere la creación de estados con enredamiento, propiedad definida por Schrödinger que se ha vuelto fundamental en esta segunda revolución. Se distinguen entre los principales sistemas físicos que son candidatos para realizar computación cuántica los siguientes: de óptica cuántica con fotones individuales, de átomos ultra fríos, de iones atrapados, y de uniones Josephson. Estos sistemas satisfacen en mayor o menor medida los criterios de DiVincenzo [1].

La ingeniería de estados cuánticos requiere manipulaciones coherentes de los sistemas.

El establecimiento de la computadora clásica fue el resultado de una discusión importante sobre las ventajas de utilizar una aproximación analógica o una digital en la manipulación de la información. La lógica binaria se impuso y ha resultado sumamente provechosa por su inmunidad al ruido, su simplicidad en las operaciones y la universalidad de sus compuertas. Hoy en día, dicha lógica se lleva a cabo sobre la base de la física del silicio y está vinculada íntimamente a esas limitaciones. La información, si bien es independiente del proceso físico que la genera y la transforma, no existe sin un ente físico.

Para realizarlas es necesario tener un control suficiente sobre los campos y términos de interacción que caracterizan al sistema físico. Esto es tradicionalmente realizado con el operador hamiltoniano asociado a la energía total del modelo propuesto. Así, un hamiltoniano utilizado para realizar computación cuántica debe tener tres términos, un término de control que puede representarse por partículas de espín ½ interactuando con un campo magnético dependiente del tiempo más un término de acoplamiento que realiza operaciones entre dos qubits; el acoplamiento con el medio ambiente se toma en cuenta con los términos que caracterizan el instrumento de medición y los procesos de relajación.

Los grupos de investigación de la información cuántica y fotónica requieren la colaboración de varias disciplinas, siendo las más importantes la física, la química, la ciencia de la computación, la ingeniería y las matemáticas. La óptica cuántica juega aquí un papel relevante ya que muchas de las implementaciones de cómputo cuántico requieren de un conocimiento profundo en estos sistemas.

Los físicos experimentales e ingenieros aprenden a manipular sistemas físicos para desarrollar una computadora cuántica. Los matemáticos, teóricos del cómputo y la información estudian cómo hacer algoritmos cuánticos y qué problemas serán computables por las computadoras cuánticas.

Es indispensable para México que invierta en la creación de grupos de información cuántica y fotónica. Estas áreas han estado desarrollándose en el mundo desde aproximadamente veinte años, pero consideramos que aún estamos a tiempo para consolidar grupos de investigación de alto nivel en estos temas y que tengan impacto en la economía nacional. Estas áreas de investigación han generado ya grandes avances tecnológicos y generarán, sin duda, muchos más. Si estamos en condiciones de ser parte de este proceso, esto redundaría en un gran beneficio, tanto científico como tecnológico, industrial y de seguridad nacional para nuestro país.

En los últimos años, y en forma recurrente, los avances en las investigaciones en las áreas de óptica cuántica, metrología óptica y control cuántico han sido reconocidos con la distinción Premio Nobel. En 1989 fue otorgado a Norman F. Ramsey, Hans G. Dehmelt y Wolfgang Paul; en 1997 a Steven Chu, Claude Cohen-Tannoudji y William D. Phillips; en 2001 a Eric A. Cornell, Wolfgang Ketterle y Carl E. Wieman, y en 2005 a Roy J. Glauber, John L. Hall y Theodor W. Hänsch.

Estas distinciones tienen en común los desarrollos de nuevas tecnologías para manipular y controlar sistemas cuánticos. Las repercusiones de estas investigaciones han impulsado la creación de centros especializados en todas las regiones del mundo, muchos de ellos creados en la última década. Estos centros buscan utilizar la luz láser y su interacción con sistemas cuánticos elementales como, por ejemplo, átomos, moléculas, fotones y nanoestructuras electrónicas, con el propósito de innovar tecnologías asociadas a comunicaciones y sistemas de información, nanofotónica, biofotónica y otras áreas de la ingeniería cuántica.

Antecedentes

El primer antecedente en la formación de la división puede asociarse a la celebración de la XXXI Escuela Latinoamericana de Física (ELAF98) en las instalaciones del Colegio Nacional entre el 27 de julio y 14 de agosto de 1998. El tema de la Escuela fue *New perspectives on Quantum Mechanics*, y para ello se presentó un panorama general del

estado actual de los fundamentos y aplicaciones de la mecánica cuántica. Entre los temas expuestos destacan los relacionados con las técnicas modernas de enfriamiento de átomos, las trampas atómicas y la manipulación de átomos en cavidades, todos ellos enfatizando los experimentos pensados por los pioneros de la mecánica cuántica y relacionados con los fenómenos de enredamiento y decoherencia. Se presentaron también nuevos procedimientos teóricos para estudiar fenómenos mesoscópicos y nuevas representaciones como la tomografía cuántica. Todos estos son temas fundamentales en el desarrollo de la teoría de la información cuántica.

El segundo antecedente se relaciona con la convocatoria del Conacyt en el año 2000 para la presentación de megaproyectos. En ese entonces, un grupo de académicos de la UNAM sometimos a consideración del Conacyt un proyecto de investigación con el objetivo de establecer un laboratorio de átomos de Rydberg ultra fríos. Los átomos de Rydberg tienen una vida media y un momento dipolar grandes, condiciones necesarias para que sean confinados en trampas magnetoópticas.

En este laboratorio se estudiaría la producción y las propiedades de átomos de Rydberg fríos, utilizando para ello el tránsito adiabático de un proceso Raman estimulado de tres fotones.[3]

Un tercer evento importante relacionado con la promoción y desarrollo del área de la información cuántica fue la realización de la Primera Escuela Mexicana de Verano en Computación e Información Cuántica, llevada a cabo en la ciudad de Mérida (Yucatán), entre el 24 junio y 2 de julio de 2004. La escuela fue organizada por el Dr. Alberto Muñoz Ubando de la Universidad Autónoma de Yucatán, el Dr. Romeo de Coss de Cinvestav-Mérida, el Dr. Juan Luis Díaz de León del Centro de Investigación en Computación del IPN y el M. en C. Salvador Venegas Andraca del Centro de Computación Cuántica de la Universidad de Oxford, con el patrocinio de las instituciones mexicanas ya mencionadas y del Consejo Nacional de Ciencia y Tecnología. La Escuela tuvo por objetivo presentar una introducción a la computación cuántica y procesamiento cuántico de la información.

A principios de 2006, en colaboración con Rocío Jáuregui y Jorge G. Hirsch, decidimos participar en una nueva convocatoria del CONACyT, con un megaproyecto titulado *Información cuántica y fotónica*, para el cual contamos con la participación de académicos de once instituciones de educación superior del país (CICESE, Cinvestav, CIO, INAOE, IPICyT, ITESM, UG, UGTO, UASLP, UAM, UNAM)[4] junto con personal del Centro Nacional de Metrología (Cenam) que establece los patrones de tiempo, masa, tensión eléctrica y resistencia eléctrica para las industrias nacionales. El protocolo del mismo surgió finalmente de una reunión de trabajo realizada a principios de febrero de 2007 y que a continuación se describe.

Reunión de trabajo

Los días 8 y 9 de febrero de 2007 organizamos la primera reunión de trabajo de los participantes en el megaproyecto que fue sometido a consideración del Conacyt.

Asistieron al evento 30 académicos de 9 instituciones diferentes; se hicieron 18 presentaciones orales de aproximadamente 15 minutos cada una con cinco minutos para preguntas o comentarios.

Los objetivos fundamentales aprobados fueron:

1. La creación del Centro Nacional de Ingeniería Cuántica.
2. El establecimiento de una red que agrupe a las instituciones del país alrededor del Centro, que fomente y permita el intercambio de información, recursos humanos e infraestructura para la consecución de proyectos conjuntos de investigación.
3. Fortalecimiento de la investigación existente en las disciplinas básicas para el desarrollo de la teoría de la información cuántica en las diferentes instituciones del país, mediante la contratación de personal académico y la compra de equipo especializado.

En la reunión de trabajo se mencionó que el proyecto tuviera dos fases. La primera, dedicada a fortalecer los grupos teóricos y experimentales, principalmente los relacionados con el desarrollo de laboratorios ya establecidos y los que se encuentran en etapa de construcción pero que cuentan ya con un investigador responsable a la cabeza. Al mismo tiempo se acordó el establecimiento de una red de investigadores que tienen interés en el desarrollo de la información cuántica. La segunda fase contempló la construcción del Centro Nacional de Ingeniería Cuántica, que tendría como misión realizar investigación en:

1. Tecnologías de la comunicación y la computación cuánticas.
2. Estados cuánticos útiles en procesos de información cuántica: a) átomos y gases ultra fríos y b) sistemas ópticos.
3. Metrología cuántica.

Muy pronto, el nuevo Centro debería ser reconocido por sus actividades en investigación, en la formación de recursos humanos y su participación en el desarrollo de tecnologías para la industria nacional pública o privada. La red de instituciones formada en la primera etapa podría evolucionar en la creación del Centro Nacional de Ingeniería Cuántica

> Los grupos de investigación de la información cuántica y fotónica requieren la colaboración de varias disciplinas, siendo las más importantes la física, la química, la ciencia de la computación, la ingeniería y las matemáticas. La óptica cuántica juega aquí un papel relevante ya que muchas de las implementaciones de cómputo cuántico requieren de un conocimiento profundo en estos sistemas.

con un espacio físico determinado y recursos para atraer nuevos investigadores.

En la reunión se indicaron algunas actividades que tenían una atención inmediata, entre otras, solicitar a la Sociedad Mexicana de Física (SMF) la creación y establecimiento de la División de Información Cuántica (DICU). Esto conllevó el diseño de un reglamento y la redacción de un acta de la sesión. Para llevar a cabo sus fines se eligió a un presidente, un vicepresidente, un tesorero y dos responsables de difusión. Finalmente, para establecer la División fue necesario hacer un plan de actividades para el año en curso incluyendo las necesidades presupuéstales. Se plantearon las siguientes acciones principales: organizar una reunión anual para presentar los avances en investigación logrados en las diferentes instituciones del país (fecha y lugar por determinarse); participar en las actividades académicas que realiza la SMF para organizar el Congreso Nacional de Física; darle una mayor difusión al área y establecer una página electrónica.

Hasta ahora, en México se han hecho esfuerzos aislados para realizar investigación básica de frontera en el área de la información cuántica, en su mayoría de carácter teórico. Consideramos que es indispensable impulsar el desarrollo experimental en esta área para poder participar en los desarrollos tecnológicos que están siendo generados. Algunos temas de potencial impacto tecnológico son: relojes atómicos (indispensables en telecomunicaciones), nuevos protocolos de procesamiento, almacenamiento, lectura y transmisión de información, formación de imágenes y caracterización de sistemas biomédicos.

La Mesa Directiva de la Sociedad Mexicana de Física (SMF), en su reunión ordinaria celebrada el 23 de agosto de 2007, después de analizar nuestra propuesta decidió aprobar la creación de la División de Información Cuántica de la SMF. Además formamos parte de la Red Temática de Tecnologías de la Información establecida por el Conacyt.

Los miembros de la División de Información Cuántica compartimos el interés y la preocupación por evitar que continuemos rezagándonos en el conjunto de líneas de investigación que son claves para el desarrollo de la física de la información. Recomendamos hacer esfuerzos para lograr la incorporación de México a la segunda revolución cuántica. Creemos que esto puede lograrse mediante la optimización de esfuerzos ya hechos, tanto con el apoyo a laboratorios ya existentes en el país, como en la construcción de nuevos laboratorios y la contratación de jóvenes investigadores que están iniciando su carrera tanto en México como en el extranjero.

Agradecemos a los Drs. Rocío Jáuregui, Jorge G. Hirsch y Luis Orozco su colaboración en la preparación de gran parte del material presentado en esta contribución .

[Referencias]

[1] G. Benenti, G. Casati y G. Strini, *Principles of Quantum Computation and Information*
Volume I: Basic Concepts (2004), 256 pp., Volume II: *Basic Tools and Special Topics*, (2007), 424 pp., Singapore: World Scientific.

[2] Einstein, B. Podolsky y N. Rosen, *Phys. Rev.*, 47 (1935) 777; E. Schrödinger, *Naturewissenschaften* 23 (1935), 807, 823, 844; Las traducciones al inglés aparecen en *Quantum theory and measurement*, Editores J.A. Wheeler y W.H. Zurek, Princeton University, New York (1983).

[3] D. Bouwmeester, A. Ekert y A. Zeilinger, Eds., *The physics of quantum information* (2000), 314 pp. Berlin, Germany: Springer.

[4] Ho-Kim Q., Kumar N., y Lam C.S. (2004), *Invitation to Contemporary Physics*, 482 pp. Singapore: World Scientific.

[Notas]

[1] La criptografía es el arte de la comunicación secreta, que actualmente nos provee de las llaves y candados de la era de la información digital.

[2] La teoría de la complejidad es la rama de la computación que estudia los recursos requeridos para resolver un problema.

[3] Es un instrumento que permite controlar y cambiar las poblaciones de los estados vibracionales y electrónicos de las moléculas con gran eficiencia.

[4] CICESE (Centro de Investigación científica y de Educación Superior de Ensenada); Cinvestav (Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional); CIO (Centro de Investigaciones en Óptica, A.C.); INAOE (Instituto Nacional de Astrofísica, Óptica y Electrónica); IPICyT (Instituto Potosino de Investigación Científica y Tecnológica); ITESM (Instituto Tecnológico y de Estudios Superiores de Monterrey); UG (Universidad de Guadalajara); UGTO (Universidad de Guanajuato); UASLP (Universidad Autónoma de San Luis Potosí); UAM (Universidad Autónoma Metropolitana) y UNAM (Universidad Nacional Autónoma de México).

Noticias Cinvestav

"Rejas Microscópicas" en Cinvestav

Se inauguró en la Unidad Zacatenco del Cinvestav la Galería Abierta con la exposición fotográfica del artista Raúl González, llamada "Microgramas". Para la inauguración de esta obra estuvieron presentes por el Cinvestav, el Dr. René Asomoza Palacio, Director General; el Dr. Arnulfo Albores Medina, Secretario Académico; el Dr. Marco Antonio Meraz Ríos, Secretario de Planeación; y el C. P. Guillermo Tena y Pérez, Secretario Administrativo. Por el gobierno del Distrito Federal, acudieron la Sra. Elena Cepeda de León, Secretaria de Cultura; la Dra. María Esther Orozco Orozco, Directora General del Instituto de Ciencia y Tecnología; el Lic. Manuel Martínez Salazar, Director General de Desarrollo Social de la Delegación Gustavo A. Madero; además de Raúl González Pérez creador de la obra.

Inauguración de las nuevas instalaciones de la Unidad Monterrey

El 18 de febrero de este año se llevó a cabo la inauguración de las nuevas instalaciones del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional (Cinvestav), en el Parque de Investigación e Innovación Tecnológica (PIIT) de la ciudad de Monterrey, Nuevo León. La Unidad está equipada con 10 laboratorios de punta dedicados a la investigación en: biofísica de canales iónicos y nanotecnología, biología computacional y de sistemas, estudios en fisiología de la fecundación, educación de ciencias, farmacología y fisiopatología del sistema cardiovascular, física teórica, medicina molecular de cáncer, microfluidez, procesamiento de señales biomédicas, radiación y dosimetría.

En la inauguración estuvieron presentes la Lic. Josefina Vázquez Mota, Secretaria de Educación Pública, el Lic. José Natividad González Parás, Gobernador Constitucional del Estado de Nuevo León, el Dr. René Asomoza Palacio, Director General del Cinvestav, y el Dr. Bruno Escalante Acosta, Encargado de la Unidad Monterrey.

El Gobernador de Nuevo León, José Natividad González Parás, mencionó que la construcción del nuevo plantel del Cinvestav en el PIIT representa el primero de varios pasos para constituir una alianza estratégica entre los gobiernos federal, estatal y municipal, la academia y el sector empresarial en materia de desarrollo de ciencia y tecnología.

Visita de la Comisión de Ciencia y Tecnología de la Cámara de Diputados al Cinvestav.

La Comisión de Ciencia y Tecnología de la Cámara de Diputados visitó las instalaciones del Cinvestav con el fin de conocer la investigación que se realiza en la institución y el impacto que tiene a nivel social, ambiental y económico.

El Dr. René Asomoza, Director General, les dio la bienvenida y les presentó al Cinvestav donde destacó la importancia de cada una de las unidades y el desarrollo regional que han promovido en los lugares donde se han asentado.

Posteriormente los directores de la unidades foráneas presentaron los principales proyectos desarrollados en sus unidades.

Para cerrar la sesión, la Presidenta de la Comisión de Ciencia y Tecnología, la diputada Silvia Luna Rodríguez, agradeció al Dr. Asomoza su invitación y mencionó que "sólo con comunicación podemos llegar a acuerdos" también destacó la importancia de contar con centros como el Cinvestav para asesorarlos.

Firma del Convenio de Cooperación Cinvestav – CNRS de Francia

Como resultado de más de cinco años de colaboración entre investigadores del Departamento de Control Automático e investigadores franceses, y debido a los buenos resultados obtenidos, se logró avanzar en el nivel de cooperación para integrar una Unidad Mixta Internacional (UMI) en la Unidad Zacatenco del Cinvestav.

De acuerdo con el Dr. René Asomoza, Director General, el convenio del Cinvestav con el Centro Nacional de Investigación Científica (CNRS, por sus siglas en francés), es muy importante en cuanto a las perspectivas que genera, pues abre las puertas a colaboraciones con miembros de la Comunidad Europea para programas de intercambio y ofrece la oportunidad a nuestros estudiantes de lograr experiencias internacionales.

Entrega de Diplomas a los graduados en 2006 y 2007

La Lic. Josefina Vázquez Mota, Secretaria de Educación, entregó sus diplomas de grado a los 632 estudiantes de maestría y 321 de doctorado que se graduaron en 2006 (298 maestros y 168 doctores en ciencias) y 2007 (323 maestros y 142 doctores en ciencias) en el Cinvestav. El evento tuvo lugar en el Patio del Trabajo de la Secretaría de Educación Pública y se transmitió a todas las unidades foráneas vía satélite y a todo el mundo por Internet.

En su mensaje a los presentes la Lic. Vázquez Mota dijo que era un honor compartir esta ceremonia ya que "para México la educación pública es una apuesta porque mientras que en países como Suecia, Japón o Alemania, 10 de cada 100 habitantes son científicos, en México esta cifra se reduce a uno entre 100".

Premios Arturo Rosenbleuth

El pasado 18 de abril se entregaron los Premios Arturo Rosenbleuth a las mejores tesis doctorales del año 2006. El Dr. René Asomoza dijo que el Premio Arturo Rosenbleuth es un reconocimiento a la calidad de las investigaciones que se realizan en el doctorado y que los trabajos ganadores son muestra clara de la vitalidad y superación de sus creadores que ratifican el espíritu del fundador del Cinvestav.

El Dr. Barranco, portavoz de los premiados, dijo que es un honor recibir el premio Rosenbleuth de la misma forma que es un honor formar parte del Cinvestav y contribuir al desarrollo de la ciencia.

En esta ocasión los galardonados fueron:

- Dr. Juan Barranco Monarca en el Área de Ciencias Exactas y Naturales (Física).
- Dra. Diana Luque Contreras, en el Área de Ciencias Biológicas y de la Salud (Biomedicina Molecular).
- Dr. Lenin Sánchez Calderón, en el Área de Ciencias Biológicas y de la Salud, (Biotecnología de Plantas - Unidad Irapuato).
- Dr. Emmanuel Carlos Dean León, en el Área de Tecnología y Ciencias de la Ingeniería (Ingeniería Eléctrica).

Nuevos Miembros de la Academia Mexicana de Ciencias

Recientemente se hizo el anuncio de los nuevos miembros de la Academia Mexicana de Ciencias, a donde ingresaron seis investigadores del Cinvestav de reconocido mérito en sus disciplinas y que han contribuido de manera importante al desarrollo de la investigación en México.

- Dr. Luís Manuel Montaño Zetina
- Dr. Eduardo Santillán Zerón
- Dr. Carlos Vázquez López
- Dr. Daniel Robledo Ramírez
- Dr. Mario Alberto Rodríguez Rodríguez
- Dra. María de Ibarrola Nicolin

Contribuciones

Las contribuciones para la revista *Cinvestav* deberán enviarse a las oficinas centrales o a la dirección de correo electrónico: revista@cinvestav.mx

Textos

- Deben entregarse en formato de Word con extensión .doc o .rtf, vía correo electrónico o en CD-ROM.
- Cuando se trate de artículos de investigación; la extensión máxima será de 15 cuartillas, los artículos de difusión tendrán 10 cuartillas y Noticias un aproximado de 50 palabras por nota.
- Si el texto incluye tablas, éstas se entregarán en archivo por separado, en texto corrido y con una impresión adjunta que muestre la forma en que debe quedar la tabla. Además, en el original debe señalarse su ubicación. La indicación también es válida para esquemas y cuadros.
- Todo artículo requiere ilustraciones o fotografías para su inserción (ver imágenes y gráficas), acompañadas de un comentario que las identifique.
- Las notas se incluirán al final del trabajo, antes de la bibliografía o de las referencias debidamente numeradas.
- Todas las siglas y los acrónimos empleados deben venir en su forma desatada (p. ej. Conacyt, Consejo Nacional para la Ciencia y la Tecnología).
- Las referencias deben apegarse a los modelos siguientes:

Libro:

Wiener, Norbert, *Cibernética: o el control y la comunicación en animales y máquinas*, Barcelona, Tusquets, 2003.

Artículo de revista:

Ádem, José, 1991, "Algunas consideraciones sobre la prensa en México", *Avance y Perspectiva*, vol. 10, abril-junio, pp. 168-170.

Se sugiere que las referencias sean cuidadosamente revisadas por los autores y que los títulos de los artículos y los nombres de las publicaciones no se abrevien.

Resumen curricular

Todos los textos deben incluir datos del autor: nombre completo, grado académico, adscripción y cargo que desempeña, teléfono y correo electrónico. El resumen no debe rebasar más de 50 palabras.

Imágenes y gráficas

Deben venir en archivos por separado tipo JPG o TIFF, a 300 dpi de resolución con tamaño de 20 cm de base (como mínimo). Las imágenes tomadas con cámaras digitales deberán tener la resolución máxima.
NO SE ACEPTARÁN IMÁGENES DE INTERNET.

Cinvestav
revista@cinvestav.mx
T/F (55) 57 47 33 71
www.cinvestav.mx/publicaciones
Av. Instituto Politécnico Nacional 2508
San Pedro Zacatenco, C.P. 07360
México, DF, México

Ciudad México
Gobierno del Distrito Federal
las personas son las que cuentan
Secretaría de Cultura
Ciudad de México
Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional
Cinvesta

Oraciones en Piedra

Templos y Palacios Mesoamericanos

El águila grazna,
el ocelote ruge,
aquí es México,
donde tu gobernabas Itzcóatl.
Por él, tienes tú ahora estera y solio.
Donde hay sauces blancos
sólo tú reinas.
Donde hay blancas cañas,
donde se extiende el agua de jade,
aquí es México.

Nezahualcóyotl (fragmento)

Galería abierta

Cinvestav

ELECTRON DEVICES SOCIETY®

IEEE

Mexico City, Mexico
November 12 - 14, 2008

2008 5th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)

(Formerly known as ICEEE)

KEYNOTE SPEAKERS

Alexandar M. Stankovic
Northeastern University
Boston, MA, USA

François Guillemin
Centre Régional de Lutte Contre le Cancer
Nancy, France

Georgios B. Giannakis
University of Minnesota,
Minnesota, USA

Magnus Egerstedt
Georgia Institute of Technology
Atlanta, GA, USA

Marcelo Antonio Pavanello
Centro da universitario da FEI
Sao Paulo, Brasil

Piero Bonissone
General Electric Global Research
New York, USA

GENERAL CHAIRS

Alexander Poznyak Gorbatch
Carlos A. Coello Coello
José Antonio Moreno Cadena

Topics of interest included, but are not limited to:

+ Automatic control
+ Biomedical engineering
+ Communications systems
+ Computer science and computer engineering
+ Mechatronics
+ Solid-state materials, electron devices and integrated circuits

CCE 2008

Calendario Azteca

IMPORTANT DATES

+ Conference: November 12-14, 2008.
+ Tutorial courses: November 10-11, 2008.
+ Paper submission: June 16, 2008.
+ Notification of acceptance: August 4, 2008.

FOR FURTHER INFORMATION CONTACT
Judith Esparza Azcoitia
Cinvestav-IPN,
Electrical Engineering Dept.,
Av. Instituto Politécnico Nacional 2508,
Mexico City, 07360, Mexico
Phone: 52 (55) 5747-3800 ext-6503
E-mail: cce@cinvestav.mx