Información cuántica

por

Carlos Pineda

Este es un capítulo separado que integra el libro

Fronteras de la Física en el Siglo XXI

Octavio Miramontes y Karen Volke (Editores)

CopIt-arXives, 2013
México, D.F.
ISBN: 978-1-938128-03-5

http://scifunam.fisica.unam.mx/mir/copit/TS0011ES/TS0011ES.html

Índice general

Información cuántica

Carlos Pineda, Instituto de Física, UNAM, México

1. Historia y algunos prerrequisitos

En este capítulo presentaremos una perspectiva de la situación actual de la información cuántica, tanto para físicos como para estudiantes de disciplinas afines y de ciencia en general. Introduciremos algunos conceptos necesarios para entender el problema a tratar y para poder maravillarse con los obstáculos y las soluciones que se han dado durante el desarrollo de esta área. En la primera parte, daremos una breve introducción a la mecánica cuántica y a algunas de sus más increíbles consecuencias. Así mismo, hablaremos de como entendemos la *información* y a continuación relacionaremos esta idea matemática con el mundo en que vivimos. Posteriormente comentaremos algunos de los desarrollos teóricos y experimentales que se han dado en el área, para proceder a dar una idea de hacia donde se desarrollará esta línea en el futuro cercano.

Mecánica cuántica. La teoría de la mecánica cuántica nació en 1900, cuando Max Planck explicó una contradicción de las teorías físicas establecidas en ese entonces mediante la adición de un pequeño postulado. Dichas teorías predecían que un cuerpo que absorbiera toda la luz y energía que incidiera sobre él[1], emitiría una cantidad *infinita* de energía. El fenómeno recibe el nombre de la *catástrofe ultravioleta* y se solucionó asumiendo que la energía no puede tener valores arbitrarios, sino que esta viene por paquetes de determinado tamaño, es decir, que está *cuantizada*. Dicha explicación resulta tan extraña, que a pesar de dar solución al problema, no se reconoció inmediatamente como un aspecto fundamental de la naturaleza y fue necesario que Albert Einstein aclarara la situación (trabajo que le valió el premio Nobel). Más adelante, cuando vino un desarrollo teórico más profundo a cargo de Erwin Schrödinger, Paul Dirac y otros, incluso el mismo Einstein, se resistió a creer algunas de las consecuencias de la mecánica cuántica por considerarlas demasiado exóticas [1].

En el formalismo cuántico, toda la información relevante de un sistema físico se abstrae a un espacio matemático sencillo llamado espacio vectorial, o para ser más precisos,

[1] Un objeto con dichas características es llamado *cuerpo negro* por los especialistas.

un espacio de Hilbert. Esta abstracción es extremadamente cómoda, ya que permite tratar sistemas físicos muy diferentes usando exactamente las mismas herramientas matemáticas. El sistemas físico más simple contiene un solo estado, lo cual lo hace poco interesante, puesto que no posee dinámica y entonces no lo podemos modificar. En resumidas cuentas, no podemos jugar con él. El siguiente sistema físico, en cuanto a complejidad, tiene dos estados diferentes. Éste, resulta tan importante que recibe el nombre de *qubit* en analogía con la unidad básica de información clásica: el bit. El qubit encierra ya una gran riqueza, pues aunque el bit solo puede estar en uno de dos estados, el qubit puede estar en una superposición de estos dos estados. Las formas de implementar un qubit son tan abundantes como animales en un zoológico. Algunos ejemplos incluyen, bajo ciertas condiciones, la polarización de un fotón, el espín de un núcleo, la posición de un átomo neutro y la energía de un electrón en un átomo. Todos ellos están descritos por los mismos objetos matemáticos y por consiguiente todas las ideas que se expondrán, pueden ser implementadas en dichos sistemas.

Una de las consecuencias más extrañas de la estructura matemática subyacente de la mecánica cuántica es la posibilidad de tener superposiciones coherentes de soluciones. Esto significa que si para determinado problema físico tenemos dos soluciones, estas pueden coexistir simultáneamente. Por ejemplo, si es posible que en un experimento un gato encerrado en una caja este vivo, pero también es posible que este muerto, otra solución admisible es que se encuentre simultáneamente vivo y muerto. ¡Estos comportamientos "exóticos" ya han sido observados experimentalmente!, ciertamente no con gatos sino con átomos y objetos microscópicos, aunque ya hay propuestas de hacer superposiciones con organismos vivos.

Este par de principios tienen como consecuencia alucinante la posibilidad de realizar teleportación. Para comprender algunas sutilezas de este procedimiento es crucial entender el rol que tiene la información en la naturaleza. En un objeto dado, como una silla, no es importante únicamente la masa que lo compone, sino también la forma en que ésta está organizada. Por ejemplo, moléculas cuyos átomos tienen diferente distribución espacial (isómeros estructurales) tienen propiedades diferentes (como los diferentes tipos de pentano). De igual manera, lo único que diferencia al autor de una vaca (con la misma masa) es la forma en que están organizados los átomos que los constituyen. *De esta forma, lo que se desea teleportar no es la masa, sino la información que alberga dicha masa.* Aclarando este punto, estamos listos para precisar en que consiste la teleportación. Este proceso se realiza entre dos partes, llamadas con frecuencia *Alice* (quien tiene el objeto a teleportar) y *Bob*, quien va a recibir dicho objeto. Inicialmente Alice y Bob deben tener cada uno una partícula (o cualquier sistema físico) en un estado *enlazado*[2]. En general, Alice y Bob pueden estar separados una distancia arbitraria (a 2012 la distancia más larga a la que se ha logrado una teleportación exitosa es de 143 kilómetros y fue hecha en las Islas Canarias).

[2]Un estado enlazado es aquel, para el cual no es posible dar una descripción individual de cada uno de los sistemas, a pesar de que el estado colectivo está perfectamente definido.

Alice, en el momento en que ella quiera, inicia el protocolo de teleportación realizando operaciones físicas sobre el objeto y su mitad del estado enlazado, incluyendo algunas mediciones. Al realizar dichas operaciones, el estado que tiene Bob se va a ver afectado. Para completar la teleportación es necesario que Alice envíe, usando métodos convencionales como un correo electrónico, los resultados de las mediciones para que Bob realice sobre su sistema algunas operaciones y aparezca "mágicamente" el estado a teleportar en su sistema.

Para el lector curioso, que desee profundizar en la excitante historia de la mecánica cuántica, puede referirse a uno de los textos más aclamados de divulgación científica [2], o simplemente a navegar en la red donde encontrará muchos recursos de los desarrollos más actuales.

Teoría de la información. Para comprender la información cuántica debemos entender un poco de la teoría de la información *clásica*, es decir la que no involucra conceptos cuánticos. La teoría de información (clásica y cuántica) se dedica a catalogar problemas de acuerdo a la dificultad de resolverlos. Una excelente introducción un poco más extensa, pero aún al alcance del público general, se puede encontrar en [3].

En general la dificultad de resolver problemas se puede medir mediante el número de pasos que se requieren para completarlo. En otras ocasiones, el recurso importante no es el número de pasos (tiempo) sino el espacio o la energía requerida. La pregunta relevante es como crece el tiempo (o cualquier recurso) requerido para resolver el problema, cuando el tamaño del problema aumenta. Aclaremos esta confusa situación mediante un ejemplo. Considere sumarle 132 a un número arbitrario x. El tamaño del problema es naturalmente el *tamaño* del número a sumar y será aproximadamente $n \approx \lceil \log_{10} x \rceil$. Supongamos que $x = 5883$, y en este caso $n = 4$. Al querer sumar 132, aplicaríamos el algoritmo que aprendimos en la escuela,

$$\begin{array}{r} 5983 \\ +\ 132 \\ \hline 6115 \end{array}.$$

Este resultado es obtenido con poco más de 4 operaciones. Si consideramos un número de 30 dígitos, el número de operaciones a realizar será poco más de 30. Es decir, conocemos un algoritmo capaz de resolver un problema de tamaño n en cerca de n operaciones. La multiplicación de dos número de longitud n, se realiza con cerca de n^2 operaciones. Estos dos problemas, se consideran "fáciles" puesto que la solución se puede obtener con un esfuerzo polinomial en el tamaño del problema. Existen varios problemas que no tienen una solución sencilla (polinomial) a simple vista, pero que con algo de ingenio pueden encontrarse métodos de solución eficientes. Un ejemplo es determinar si un número es primo o no[3].

[3] El descubrimiento de este algoritmo, sólo se produjo hasta el 2004.

Existen algunos problemas para los cuales no se conoce ningún algoritmo "corto" para resolverlos. Por ejemplo, encontrar un itinerario que nos lleve exactamente una vez por cada una de las ciudades, dado un mapa con las ciudades y los caminos con los que se encuentran conectadas. En este caso, el tamaño del problema n es el número de ciudades. Un algoritmo para encontrar la solución puede ser el de probar todos los posibles itinerarios y ver si hay alguno conveniente. El número de itinerarios será aproximadamente $n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$. Éste es un número muy grande: si usamos una computadora que requiera lo que le toma a la luz atravesar un átomo, por revisión de cada itinerario, no podríamos estudiar mapas ni con 35 ciudades aunque tuviéramos todo el tiempo del universo (literalmente). Nótese, sin embargo, que si nos dan una posible solución al problema será fácil evaluar si es una solución correcta[4].

Del ejemplo anterior podemos ver que existen, *grosso modo*, dos familias de problemas. En una de ellas, al aumentar el tamaño del problema, el esfuerzo requerido para resolverlo aumenta también moderadamente (para ser más precisos, el esfuerzo, o número de operaciones, es polinomial en el tamaño del problema). Este tipo de problemas se conoce como **P**. En el otro caso, el esfuerzo requerido para resolver el problema aumenta *muy* rápidamente con el tamaño del problema, al punto de hacerlo literalmente intratable con todos los recursos que tenemos a la mano (incluso suponiendo que tenemos, por ejemplo, todas las computadoras de la tierra disponibles). El tipo de problemas que requieren una cantidad exponencial (por ejemplo 2^n) de recursos (y por consiguiente es "difícil" de resolver), pero cuya solución es "fácil" (que requiere una cantidad polinomial de recursos) de verificar como correcta, se conocen como **NP**. Dentro de la familia de problemas **NP**, hay una subfamilia muy famosa e importante. Son los problemas **NP**-completos. Su característica es que hallar una solución para uno solo de estos problemas, equivale a solucionar *todos* los problemas **NP**. Ésta es una familia grande, y el lector interesado no tendrá dificultad en encontrar ejemplos de dichos problemas. Sin embargo, hasta donde se sabe, no todos los problemas **NP** son **NP**-completos.

Más allá de las clases **P**, **NP** y **NP**-completos hay todo un zoológico de jerarquías de problemas. Lo que se ha logrado comprobar rigurosamente es una parte ínfima de los límites de este mapa. Incluso, no se ha comprobado que **P** y **NP** son diferentes y esto constituye uno de los grandes problemas de la matemática actual. Para animar al lector a intentar solucionar este interesante problema, sería bueno añadir que aquel que encuentre la prueba de que **P**$\neq$**NP** (o **P**$=$**NP**) se hará acreedor de un millón de dolares por parte del Clay Mathematics Institute [4].

Algunos desarrollos teóricos. La idea fundamental detrás de la información cuántica nació de Richard Feynman, quien en 1982 y 1985 escribió un par de artículos en donde

[4] Vale la pena anotar que existen algoritmos ingeniosos que han simplificado el problema, sin embargo, éste sigue siendo intratable en el sentido de que aún requiere un tiempo exponencial en el número de ciudades.

se planteaba el usar un sistema cuántico para *(i)* realizar cómputos similares a los que se hacen en una computadora de escritorio [5] y *(ii)* usar un sistema cuántico para realizar un cálculo particular que no es posible realizar con una computadora de escritorio [6]. Estos dos trabajos cimentaron el terreno para que Peter Shor, en 1994, publicara un trabajo donde se demostraba que las computadoras cuánticas, propuestas por Feynman, tenían un poder tal, que a la luz de la teoría de información, es mayor al de las computadoras clásicas.

La idea clave es observar que una computadora no es más que un sistema físico que evoluciona bajo ciertas reglas. Aprovechamos estas reglas para fabricar una condición inicial que codifica nuestra pregunta. Después de hacer la evolución, la condición final contiene codificada la respuesta a nuestra pregunta. Feynman detalló de que manera se pueden reproducir los cálculos que se han en una computadora compuesta de los elementos básicos de cómputo (compuertas OR, AND, etc) en un dispositivo cuántico [5]. De igual manera, él notó que la simulación de sistemas cuánticos es muy difícil en una computadora clásica, debido a los requerimientos exorbitantes de memoria que se tendría. Para ganar un poco de perspectiva acerca de la cantidad de memoria requerida para la simulación de un problema cuántico, imaginemos una computadora clásica (es decir, que manipula la información en forma clásica) que como memoria usa *todos* los átomos del universo. Cada uno de los 10, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000 = 10^{82} átomos [7] que, se estima, contiene el universo observable guardará un bit de información. La memoria de esta computadora sería insuficiente incluso para simular un sistema de tan solo 300 de las partículas cuánticas más sencillas, ya que 2^{300} es mucho mayor que 10^{82}. Sin embargo, si empleamos una computadora cuántica compuesta, por ejemplo, por 300 fotones, no tendríamos problema en almacenar el estado del sistema.

Sin embargo, poca atención fue prestada a estos desarrollos (aparentemente de un interés meramente académicos), hasta que Peter Shor hizo el avance más espectacular hasta la fecha. Shor encontró una forma eficiente de factorizar números usando una computadora cuántica. A primera vista este es un avance de nuevo académico; sin embargo, hoy en día la mayoría de intercambio de información que se realiza en forma secreta es usando el hecho de que multiplicar dos números es un problema fácil (como fue definido en secciones anteriores) mientras que el proceso inverso, el de factorizar es difícil[5]. Esto hace que la solución de este problema tenga un impacto profundo en el mundo de la comunicación digital. La creencia popular es que el problema de la factorización es un problema NP. Lastimosamente, este parece ser un problema "especial": la solución de dicho problema usa características particulares del problema que no se pueden aprovechar para resolver algún problema de la familia **NP**-completos.

La existencia de dicho algoritmo crea una nueva categoría en el conjunto de todas las

[5] Aún no se tiene una prueba matemática de este hecho, sin embargo la comunidad lo cree y ha confiado en esta creencia para encriptar una buena parte de sus comunicaciones.

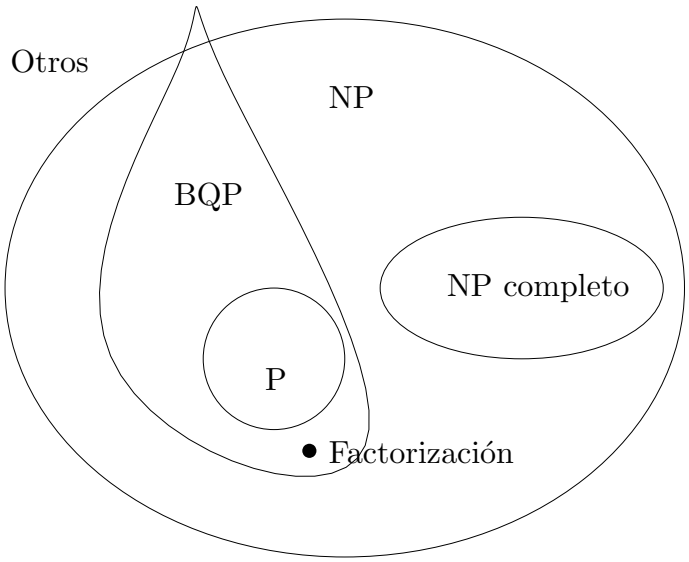

Figura 1: Ilustración de la clasificación de problemas de acuerdo a su complejidad. Los problemas más simples, y que se pueden resolver en un tiempo polinomial con respecto a su tamaño son del tipo **P**, por ejemplo la multiplicación de dos números. Problemas **NP** son los que no se pueden resolver fácilmente, pero una vez que se tiene la solución, verificarla es simple (como encontrar un tour que visite exactamente una vez un pueblo de un mapa con unos caminos predeterminados). Problemas **NP**-completos son aquellos que al resolverlos, podríamos resolver cualquier otro problema **NP**. Un ejemplo de dicho problema "universal" es el Sudoku. Naturalmente existen problemas más difíciles que catalogamos como "otros" y para los cuales no exponemos su estructura acá. Las computadoras cuánticas, se cree, ayudarán a resolver algunos problemas de gran importancia, dentro de la familia de problemas **NP** y quizá ayuden a resolver problemas más difíciles. La factorización es un problema "difícil" para computadoras clásicas, pero "simple" para computadoras cuánticas.

familias de problemas. Ilustramos esta nueva clase en la figura 1. Ésta está compuesta por los problemas que pueden ser resueltos en una computadora cuántica eficientemente (es decir con un número polinomial de pasos, en el tamaño del problema). Un elemento de este conjunto es el problema de factorización, que con el algoritmo de Shor se puede resolver eficientemente en una computadora cuántica. Aún está por probarse que dicho punto está por fuera del área de los problemas tipo **P**.

Nótese sin embargo, que una computadora cuántica, hasta donde se sabe, no puede resolver cualquier problema **NP**; en particular no puede resolver problemas **NP**-completos. Una línea de investigación muy activa se dedica a encontrar problemas que se encuentren fuera de **P** pero dentro de **BQP** y se han encontrado aplicaciones incluso en el ámbito de sistemas complejos, doblamiento de moléculas, etc, para los cuales una computadora

cuántica proveería respuestas que una computadora clásica sería incapaz de obtener en un tiempo razonable.

También debemos mencionar que hay problemas para los cuales la existencia de una computadora cuántica no cambia la clase a la que pertenece el problema, sin embargo sí provee una ventaja real. Dicho es el caso del problema de búsqueda en listas sin estructura. Para ilustrar el problema, imaginemos que nos es dado un directorio telefónico (con n entradas). Dado un nombre, podemos encontrar el correspondiente número fácilmente. Sin embargo si nos es dado un número telefónico y queremos encontrar el correspondiente nombre, no tendremos más alternativa que revisar una a una las entradas del directorio hasta encontrarlo. Este último ejemplo (números telefónicos desorganizados) es un ejemplo de una lista sin estructura, y está claro que nos tocará revisar en promedio $n/2$ entradas para encontrar el elemento deseado en dichas listas. Se descubrió, sin embargo, que con una computadora cuántica se necesitan solo del orden de $\sqrt{n}$ pasos para solucionar el problema. Buscando en listas gigantes (por ejemplo que incluyan los registros médicos de una nación grande) una computadora cuántica sería 1000 veces más rápida que una clásica, y si la lista es más grande, la ganancia sería aún mayor. El algoritmo que realiza la tarea en forma cuántica, de manera efectiva, se llama algoritmo de Grover.

Después del descubrimiento del algoritmo de Shor, se notó que la tarea de construir una computadora cuántica no era nada fácil. El principal enemigo era (y continúa siendo) la decoherencia. Ésta cambia el estado del sistema y es debido a interacciones indeseadas con el ambiente que rodea al sistema físico o entre los constituyentes de la computadora cuántica. Este fenómeno es bastante común en los sistemas experimentales que se desarrollan en el área, y hay un cierto consenso de que, hasta cierto grado, la decoherencia es inevitable. En sistemas clásicos, se puede combatir este fenómeno usando códigos que corrijan el estado de la computadora en el transcurso del cálculo, pero el procedimiento cuántico análogo pareciera en un principio imposible. Para comprender la dificultad de correcciones de errores cuánticos, consideremos una forma de corrección de errores, en un dispositivo clásico. En cierto punto del cómputo, vamos a codificar la información triplicándola. Por ejemplo, para codificar un "0", en vez de tener un solo cero guardado en memoria, se podrían tener tres ceros: "000".

$$0 \to 000$$

Por ejemplo, si queremos representar la secuencia "0 1 0", en nuestro registro de nueve bits codificaríamos:

estado del bit :	1	2	3	4	5	6	7	8	9
número del bit :	0	0	0	1	1	1	0	0	0

.

Así un error de un solo bit se vuelve fácil de detectar. Por ejemplo, si después de hacer algunos cálculos reviso el estado de mi registro y es:

estado del bit :	1	2	3	4	5	6	7	8	9
número del bit :	1	1	1	0	1	0	0	0	0

.

Entonces, sé que tengo un error en el bit número cinco, y puedo corregirlo cambiando el estado de este bit a "0".

No se puede emplear esta técnica en cómputo cuántico por dos motivos fundamentales. El primer motivo es que no es posible copiar información cuántica. Este divertido resultado, cuyos detalles se encuentran al alcance de estudiantes de física [8], se conoce como el *teorema de no clonación* y tiene muchas consecuencias importantes, incluida la imposibilidad de transmisión de información a una velocidad más rápida que la de la luz. Así, el procedimiento análogo, para triplicar un estado desconocido (denotado por ψ) es imposible:

$$\psi \nrightarrow \psi\psi\psi.$$

El segundo motivo es que es imposible determinar en qué estado está el sistema sin modificarlo (ver por ejemplo el excelente libro [2]). Estos dos obstáculos supusieron por algún tiempo una dificultad insuperable para el cómputo cuántico. En 1995 y 1996, Peter Shor y Andrew Steane descubrieron métodos totalmente innovadores para proteger la información sobre algunos tipos de errores. La idea es codificar los qubits en espacios de muchas partículas, y realizar mediciones que conserven la estructura de dichos espacios. Una explicación a fondo, requiere algunos elementos de mecánica cuántica, pero sigue siendo accesible al lector interesado, con algunos fundamentos en la materia [9].

Algunos otros desarrollos teóricos que se deben mencionar incluyen la simulación de sistemas cuánticos (quizá la aplicación más popular en el futuro de las computadoras cuánticas). Esto cobra una gran importancia puesto que nos permitirá explorar sistemas físicos inaccesibles, numérica y experimentalmente, y así desarrollar tecnología basada en sistemas cuánticos de muchos cuerpos. También se pueden usar estas computadoras para resolver sistemas gigantes de ecuaciones lineales y otros problemas como el doblamiento de proteínas o comportamientos preferidos en sistemas complejos.

Algunos desarrollos experimentales. La implementación experimental del cómputo cuántico ha sido una parte importante del campo debido a tres motivos. El primero es la necesidad de las agencias patrocinadoras (típicamente gubernamentales) de estar a la vanguardia en cuanto a tecnología de comunicaciones y encriptación. Segundo, el interés de estar a la vanguardia en cuanto a todo el desarrollo que conlleva el control de sistemas cuánticos individuales. Por último se encuentra la curiosidad de los físicos del campo por comprobar experimentalmente las predicciones, con frecuencia en contra del sentido común, de la mecánica cuántica.

Dado que los fundamentos de cómputo cuántico se encuentran formulados en términos de espacios de Hilbert abstractos, los sistemas físicos en los que se pueden implementar son muy diversos. Sin embargo, cada uno de los sistemas debe cumplir con cinco condiciones propuestas por David DiVincenzo en 1996 para poder implementar una computadora cuántica. Éstas son:

- Tener unidades de información cuántica (qubits) bien definidos.

- Poder preparar el estado inicial de la computadora con precisión.
- Tener poca decoherencia (errores por interacciones indeseadas).
- Implementar con precisión compuertas de una y dos partículas.
- Realizar mediciones sobre partículas individuales.

Si bien aún no existe el sistema físico que cumpla cabalmente con todos estos requerimientos, se están explorando varias posibilidades. Listamos a continuación algunas de las propuestas más importantes, bien sea por razones históricas o por el optimismo que se tiene frente a ellas.

*Resonancia magnética nuclear y factorización.*Uno de los sistemas físicos en donde fueron implementados por primera vez protocolos de información cuántica es el de resonancia magnética nuclear (NMR, por sus siglas en inglés). NMR es un sistema físico que consiste de un conjunto de moléculas inmersas en un líquido. Algunos de los núcleos de dichas moléculas interactúan entre si, y éstos (los núcleos) son los objetos que se utiliza para procesar la información. El premio Nobel de física fue dado a Isidor Rabi por el desarrollo de esta técnica, que ha sido usada para comprender la composición química y la estructura de moléculas. En los años 90, se comprendió que se podía usar toda la infraestructura no solo para mirar dentro de las moléculas, sino también para manipular los estados de la molécula. Lo anterior hizo que el campo creciera rápidamente y la primera demostración experimental de una factorización usando una computadora cuántica se logró justamente en este sistema en el 2001 por el equipo de Isaac Chuang en los laboratorios de Standford. A pesar de su éxito inicial, se sabe que es muy difícil escalar este tipo de sistemas, es decir agrandar la computadora (lo que equivale a agrandar la molécula) es una tarea demasiado complicada. Más aun, dado que la señal sobre el ruido intrínseco del sistema es muy baja, se tiene poca fe en que al aumentar el tamaño de la molécula siga siendo posible hacer las operaciones con la precisión requerida.

*Trampas de iones y teleportación.*Otro sistema físico con notables avances tecnológicos respecto al procesamiento de información cuántica es la cadena de iones. Este sistema consiste de un conjunto de iones que se encuentran atrapados en una trampa electromagnética y se auto organizan en una recta. En este sistema se usa la estructura interna de cada átomo para guardar la información. Para ser más precisos, usa dos niveles de energía (escogidos a conveniencia del experimento) como qubit. Aparte de eso, para hacer interactuar los diferentes átomos, se usa el movimiento colectivo de todos los átomos a manera de bus. Desde el planteamiento teórico, varios grupos han logrado avances muy importantes, como la demostración de que es realmente posible hacer operaciones de uno y dos qubits. Quizá el experimento más espectacular, para el público general, fue la realización de teleportación de partículas con masa en forma determinista, en contraste con esquemas previos, en donde la teleportación era exitosa solo una fracción de las veces. Gracias, entre otros, a estas demostraciones, fue dado el premio Nobel 2012 a David Wineland (compartido con Serge Haroche), líder de un grupo de investigación en el National Institute of

Standards and Technology, en Colorado, USA. Así mismo, han logrado demostraciones de muchas de las propuestas teóricas, como la simulación de sistemas cuánticos, la creación de estados de muchas partículas enlazados y la realización de códigos de corrección de errores.

Electrodinámica cuántica en cavidades y decoherencia. Otro sistema cuántico, del que se ha aprendido mucho en el siglo pasado es la luz. La manipulación de fotones individuales ha abierto la posibilidad de realizar experimentos fundamentales de mecánica cuántica (y por ende de información cuántica) con ellos. Una forma de "guardar" un fotón para observar su evolución y hacerlo interactuar con otro sistema es ponerlo entre dos espejos con cierta geometría (la cavidad). Quizá uno de los aspectos más innovadores ha sido la observación de como actúa el mayor enemigo del cómputo cuántico sobre sistemas cuánticos, la decoherencia. Lo que hicieron fue poner un átomo de Rubidio en una superposición cuántica dentro de una cavidad, y al interactuar el átomo y los fotones de la cavidad, se creó una superposición de estados del sistema completo. Al no ser la cavidad perfecta, los fotones comenzaron a escapar, destruyendo esta superposición cuántica. En el experimento, fueron capaces de observar como ocurría dicho proceso y marcó el inicio del estudio experimental de la decoherencia[6]. Otro espectacular avance es el de observar como se lleva a cabo el proceso de medición, uno de los aspectos más intrigantes de la mecánica cuántica.

Otros. Existen muchos otros sistemas en los cuales se han implementado tareas de información cuántica, como fotones libres, fotones en fibras ópticas, circuitos superconductores, centros de nitrógeno en diamantes, solo por mencionar algunos. El lector interesado puede navegar en revistas de divulgación como Scientific American, en donde encontrara recursos para alimentar su curiosidad.

2. Desarrollo actual y perspectivas

La cantidad de dinero que se está invirtiendo en esta área, hace que sea una de las más activas en la actualidad. Se está pasando de los experimentos demostrativos a una etapa más practica, donde se esta cosechando todo lo que se ha aprendido.

Comunicación cuántica comercial. Una de las aplicaciones de la información cuántica que han visto el mercado recientemente es la comunicación cuántica. Hemos notado que los estados "especiales" de sistemas cuánticos (como las superposiciones, o los estados enlazados) son extremadamente frágiles, dificultando su manipulación. Sin embargo, se puede explotar esta fragilidad. Si enviamos un estado "frágil", cualquier intento por descubrir este estado, por parte de un tercero, va a ser notado, ya que perturbará fuertemente el sistema. Esto se debe a motivos fundamentales: de acuerdo a uno de los postulados de

[6] El líder del grupo que realizó dicho experimento, Serge Haroche en l'Ecole Normale Supérieure de París, fue uno de los ganadores del premio Nobel en 2012.

la mecánica cuántica, al realizar una medición en general modificaremos el sistema. La comunicación cuántica se basa en dicha propiedad para enviar mensajes secretos entre dos partes. En la práctica, lo que se hace es que se usa la comunicación cuántica para establecer una clave secreta que se usa en esquemas de comunicación clásica. Ya existen empresas que ofrecen la instalación de estos sistemas a nivel comercial[7] y han impulsado la retroalimentación entre el sector académico y el industrial. Sin embargo, se ha demostrado que a pesar de la leyes de la mecánica cuántica, este tipo de sistemas presentan algunas vulnerabilidades intrínsecas. Resulta en la práctica, sin embargo, desde un punto de vista técnico, una forma de comunicación extremadamente segura, pues las demostraciones de "hackeo" solo han sido realizadas en laboratorios y bajo condiciones muy controladas. Estas vulnerabilidades no han detenido el desarrollo teórico y experimental de una nueva área de las telecomunicaciones.

Muchos cuerpos cuánticos. Otra de las áreas donde hay mucho interés es en la simulación de sistemas cuánticos. Hoy en día, algunos de los experimentos más avanzados requieren el uso de semanas de cómputo para analizar los resultados obtenidos. Es decir, ya hoy por hoy en simulación cuántica se comienzan a poder hacer cosas que no son susceptibles de ser simuladas en computadoras clásicas. Más aún, para algunos de estos experimentos hay un entendimiento de la física que lo gobierna, mientras que para algunos otros experimentos no se sabe qué comportamientos esperar. Por ejemplo, ya es posible controlar las interacciones de partículas cuánticas individuales en arreglos de dos dimensiones. Se espera que esta herramienta brinde nueva información de fenómenos como la superconductividad de alta temperatura, de la cual tenemos un pobre entendimiento, y que además se puedan aprovechar las herramientas desarrolladas para crear nuevas tecnologías basadas en la riqueza de los fenómenos cuánticos. Cabe aclarar que la comunicación cuántica, a pesar de involucrar muchas partículas, está basada en fenómenos de una o dos partículas.

Sistemas híbridos. De las décadas anteriores hemos aprendido las bondades y dificultades de algunos sistemas cuánticos. Por ejemplo, al trabajar con fotones, estos son fáciles de llevar de un sitio a otro, sin embargo son muy difíciles de poner a interactuar entre si. Por otro lado, por ejemplo, en las cadenas de iones se pueden producir interacciones entre las diferentes compuertas con mucha facilidad, pero protegerlos de decoherencia puede resultar difícil. Debido a ésto se cree que el camino a seguir para la implementación de una computadora cuántica universal implica la utilización de diversas tecnologías en diferentes pasos del cómputo. Para esto necesitamos que, por ejemplo, un ion en una cadena pueda interactuar eficientemente con fotones individuales, o que sistemas nanomecánicos puedan transferir su información a átomos neutros. Este es precisamente el campo de

[7] Por ejemplo, id Quantique, con página http://www.idquantique.com/ a Octubre de 2012.

los sistemas híbridos, cuyo mayor reto es lograr una comunicación fiel entre diferentes sistemas físicos, cada uno con sus ventajas y sus desventajas.

Computadoras cuánticas. Uno de los objetivos del cómputo cuántico es solucionar problemas que no sean posibles solucionar en una computadora clásica. Para esto no basta con controlar un par de qubits. Ni diez, ni cien. Los problemas que se pueden solucionar con computadoras cuánticas de este tamaño, también se pueden solucionar con computadoras basadas en tecnología actual. Se calcula que el punto de inflexión ocurrirá cuando se logren controlar del orden de mil qubits. ¿Que tan lejos estamos de este objetivo? Nadie tiene la respuesta a esa pregunta. Algunos pesimistas afirman que nunca llegará ese día mientras que otros están trabajando (con mucho optimismo) para que así sea. Algunos logros como la simulación eficiente de sistemas cuánticos, o incluso la factorización de 15 han servido para dar un impulso a esta línea. Desde el punto de vista del autor, sin embargo, la prueba más contundente a la fecha de la próxima realidad de las computadoras cuánticas es que la empresa privada ya se encuentra vendiendo prototipos de dichas máquinas con algunos cientos de qubits[8]. No solo eso, sino que ya se han vendido varias unidades, principalmente a instituciones dedicadas a la investigación. Incluso ya se han publicado resultados en el campo de biología, donde se analizaron una cantidad gigantesca de patrones de doblamiento de proteínas y se buscaron aquellas favorecidas por la naturaleza, es decir aquellas que minimizaban la energía. Se prevé que en unos 5 años ya se cuente con el control de un número tal de qubits que estas máquinas superen a las clásicas y por consiguiente nos comiencen a dar respuestas inalcanzables de otra manera.

3. Desarrollo a futuro

El futuro inmediato de la información cuántica se centra tanto en implementar físicamente las ideas desarrolladas, como en entender los alcances teóricos de una computadora cuántica. Se sabe muy poco de los límites prácticos que separan cada una de las regiones de la figura 1. El mayor interés desde el punto de vista de ciencias de la computación consiste en encontrar problemas para los cuales una computadora cuántica resulte útil. Esta tarea no es fácil, sin embargo, los pocos problemas que se conocen en la región de interés (dentro de **BQP**y fuera de **P**) tienen un gran número de aplicaciones inmediatas. Cuando se descubran más problemas en dicha región, la aplicabilidad que tendrán las computadoras cuánticas será mayor.

Las perspectivas con respecto a la simulación de sistemas cuánticos también son excitantes. Para resaltar el impacto que tendrá el entendimiento de fenómenos cuánticos

[8]La compañía es D-Wave, y su página de internet es http://www.dwavesys.com. Cabe anotar que dichos prototipos no son capaces de solucionar problemas fuera del alcance del cómputo clásico, por lo que el apelativo "computadora cuántica" para dichos dispositivos puede resultar controversial. El paradigma en el que se basan se llama *cómputo cuántico adiabático*, pero su explicación requeriría algunos tecnicismos que están fuera del alcance de este texto.

colectivos en nuestra vida diaria, conviene hacer una retrospectiva de como ha afectado el entendimiento de las leyes de la física en nuestro mundo actual. Una gran cantidad de objetos que usamos no serían posibles sin un entendimiento aceptable de las leyes de la electrodinámica. Las leyes de la termodinámica han jugado un rol profundo en la revolución industrial y el estudio del estado sólido ha propiciado todo el desarrollo de la computación. Por eso, quizá la perspectiva más emocionante para la información y cómputo cuántico esta en la profundización del entendimiento de fenómenos cuánticos colectivos. Este tipo de fenómenos han probado ser de los problemas más difíciles a tratar y el hecho de que no haya un buen entendimiento de superconductividad a altas temperaturas lo demuestra. La exploración de fenómenos colectivos cuánticos sin duda propiciará una avalancha de desarrollos tecnológicos como metrología, litografía de alta resolución y detectores de altísima sensibilidad. La mayoría de las aplicaciones, sin embargo, aún ni siquiera las imaginamos y tendremos que esperar a que futuras generaciones, ocupando las herramientas que hoy estamos creando, desarrollen la tecnología del futuro.

Otro avance que veremos en el futuro es la generalización de la comunicación cuántica. Este avance puede ser aumentando las distancias en las cuales es posible implementarla o aumentando el número de participantes en algún intercambio de información. En cuanto a las distancias, ya están en proceso proyectos para usar satélites para realizar dicha comunicación. Esto abre toda una serie de posibilidades no solo desde el punto de vista tecnológico sino también fundamental: la exploración de la interacción entre mecánica cuántica y gravedad. Excitantes experimentos como hacer superposiciones del campo gravitatorio y por ende explorar los límites de dichas teorías ya se encuentran en los planes de algunos visionarios.

Agradecimientos

Este capítulo se escribió con apoyo de los proyectos CONACyT 57334 y UNAM-PAPIIT IA101713.

4. Referencias

[1] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Physical Review*, vol. 47, no. 10, pp. 777–780, May 1935. [Online]: http://prola.aps.org/abstract/PR/v47/i10/p777_1

[2] J. Gribbin, *In Search of Schrodinger's Cat: Quantam Physics And Reality*, ser. A Bantam new age book. Random House Publishing Group, 1984. [Online]: http://books.google.com.mx/books?id=hs72XL_dS-AC

[3] S. Aaronson, "The Limits of Quantum Computers:," *Scientific American*, p. 62, 2008.

[4] "The millennium prize problems," http://www.claymath.org/millennium/, accesado: 02/10/2012.

[5] R. P. Feynman, "Quantum Mechanical Computers," *Optics News*, vol. 11, no. 2, p. 11, Feb. 1985.

[6] ——, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6-7, pp. 467–488, Jun. 1982.

[7] Wikipedia, "Observable universe — Wikipedia, the free encyclopedia," 2004, [Online; accessed 22-Oct-2012]. [Online]: http://en.wikipedia.org/wiki/Observable_universe

[8] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, October 1982.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge University Press, 2000.