Capítulo del libro: *Tendencias actuales de la Física en México*, Editado por M. Santillan et al, Publicaciones del IPN (México DF, 2007)

¿Computación Cuántica?

Oscar Rosas-Ortiz

Resumen

La Computación Cuántica ha despertado el interés de científicos e investigadores en todo el mundo. La repercusión que tendría la construcción de la primera computadora cuántica comercial se antoja sorprendente. En este capítulo discutiremos algunas de las nociones básicas que son de utilidad para una consulta posterior a la literatura más avanzada.

El Universo más cercano a mi mundo es mi pensamiento
Manuscrito encontrado en Puebla de Zaragoza a finales del Siglo XX

Introducción

Gordon Moore no es mundialmente conocido por ser uno de los fundadores de Intel. Su renombre surge en 1965, después de publicar un artículo en la edición del 35 aniversario de la revista *Electronic Magazine*. Moore reportó que la cantidad de componentes (transistores) en un circuito integrado de silicón (chip) se había duplicado cada año desde 1959 hasta 1965. Considerando que los chips más complejos de ese entonces consistían de alrededor de 60 transistores, predijo que para 1975 se podrían incluir 65,000 de estos en un solo chip [1]. Hoy, a más de medio siglo de la invención del transistor, el número de componentes en un chip de silicón ha aumentado a cerca de un mil millones [2]. La propuesta empírica del cofundador de Intel se verifica día con día y ahora se conoce como la *Ley Moore*.

Conforme se van agrupando más y más transistores en un circuito integrado, las longitudes de los chips más pequeños se tornan milimétricas, e incluso nanométricas. En 1988, Robert Keynes usó esta observación para estudiar el número de átomos que se requieren para almacenar un bit (la unidad más pequeña de información que registra, almacena y procesa una computadora convencional). Imitando a Moore, Keynes analizó la variación anual de este número y extrapoló sus resultados para concluir que, en el 2020, se alcanzaría el límite de un bit por átomo [3]. A este respecto, en la actualidad, los cálculos más optimistas sitúan el límite operacional de los chips de silicón en una longitud de cerca de 30 veces las dimensiones de un átomo [2] (todavía por debajo de la predicción Moore-Keynes). Para alcanzar dicho límite, cabe decirlo, se requiere de las innovaciones que podrían producirse durante los diez o quince años siguientes. Está claro que, si se ha de obtener un bit por átomo, la física a la que estamos habituados no es suficiente. Una vez que los dispositivos alcancen dimensiones atómicas será necesario usar la Mecánica Cuántica para registrar, almacenar y procesar bits.

Las computadoras se encuentran por doquier debido a su sorprendente y acelerado desarrollo; son el símbolo de nuestra era. Se les usa, inclusive, como metáfora para explicar el comportamiento del cerebro humano. Es notable que, en el desarrollo de estos instrumentos, la teoría ha antecedido a la práctica. Pensando que la miniaturización de los chips es imparable, es sólo cuestión de tiempo el contar con dispositivos de cálculo tan pequeños que requieran ser llamados *computadoras cuánticas*. La historia se repite: actualmente se desarrolla el *software* para un *hardware cuántico* que todavía no existe.

La historia que nos lleva desde los primeros artefactos de cálculo hasta las computadoras convencionales y los primeros prototipos (en papel) de las computadoras cuánticas es fascinante; incluye nombres como el de Blaise Pascal, Gottfried Leibniz, Charles Babbage, John von Neumann, Alan Turing, Albert Einstein, Wolfgang Pauli, Werner Heisenberg, Erwin Schrödinger, Richard Feynman, Peter Shor, Charles Bennet, David DiVicenzo, Michael Nielsen y José Cirac, entre otros. A lo largo de este capítulo revisaremos algunos eventos interesantes. El objetivo es dar un panorama global (que no exhaustivo) de los conocimientos que se requieren para acercarse, por primera vez, a los conceptos de la computación cuántica. Al mismo tiempo se sugieren lecturas adicionales para que el lector profundice sus conocimientos en los temas discutidos.

1900: Un año de manivelas y resortes

Una historia de fantasmas

Nada hay como ver a los fantasmas de cerca
Denis Diderot: Cartas a Sophie Volland

Año de 1900, mar Egeo. Los pescadores de esponjas están atemorizados, la tormenta no amaina y deben buscar refugio. Finalmente desembarcan en la isla de Anticitera, a medio camino entre Creta y Grecia. Pasan las horas y en el rostro de Elías Stadiatos se refleja la preocupación; en pocas ocasiones ha visto tan embravecido al mar. Su piel, bronceada por el Sol (su eterno compañero en las travesías marítimas), se torna gris bajo los litros de agua que el cielo deja caer. Decide dormitar un poco. Cuando despierta, la tormenta se ha ido. Envalentonado le grita a Héctor que le acompañe, se darán un chapuzón mientras buscan esponjas. Héctor es nuevo en el grupo pero ya siente el mismo respeto por Elías que el resto de sus compañeros; un respeto ganado como consecuencia de haber sobrevivido a 22 naufragios... aunque bien pensado, su sobrevivencia podría estar asociada más con la mala suerte que con sus habilidades de marinero. Una vez en el agua, Elías llena sus pulmones de aire y se sumerge completamente para bucear evitando los arrecifes; sabe que es el mejor buceador de su camarilla y con el rabillo del ojo observa con desdén que Héctor se rezaga. De repente, Elías se queda como petrificado, abre desmesuradamente los ojos y soltando una bocanada de aire emprende el regreso a la superficie... sus pulmones apenas resisten. Tan pronto aspira un poco de aire, de su boca sale un grito despavorido. Sus compañeros, alarmados, se lanzan al agua en su ayuda.

Una vez en tierra, el Capitán zarandea a Elías por los hombros (no puede permitirse el lujo de que los pescadores se le amotinen, atemorizados por Dios sabe que asunto) y con los ojos inyectados de autoridad le grita:

–¿Qué demonios te ocurre? ¡Habla ya, antes de que te haga colgar del mástil!

–Las mujeres... las mujeres, –alcanza a decir Elías en un balbuceo mientras Héctor se encoge de hombros ante la mirada interrogante de sus compañeros. Enfurecido, el Capitán cruza el rostro de Elías con un par de bofetadas, éste cae de rodillas cubriéndose los ojos con las manos y casi llorando de terror aúlla:

–¡Hay una pila de mujeres muertas a un lado de los arrecifes!

A pesar de lo dramático de nuestra historia, el lector debe saber que tiene un final feliz. Las "mujeres muertas" eran realmente estatuas de bronce de tamaño natural que resultaron ser parte de la carga de un barco que se había hundido en ese sitio al rededor del año 80 a.C.[1] [4]. Entre los hallazgos se encontraba un enigmático dispositivo que recibió el nombre de *mecanismo de Anticitera*. De acuerdo con las conclusiones de los investigadores que han estudiado este artefacto, se trata nada menos que de una computadora analógica cuya construcción podría remontarse al 87 a.C., aunque esta interpretación ha causado controversia. No cabe duda que los Antiguos estaban, igual que nosotros, interesados en construir dispositivos que efectuasen por si mismos ciertas tareas, ya fuese para maravillar a sus coetáneos con artefactos que tuvieran 'movimiento propio' o bien para sustituir de alguna forma aquellas actividades realizadas por los hombres. Éstas no tienen por qué ser sólo mecánicas, también involucran operaciones de cálculo.

El afán del hombre por entender el medio que le rodea ha implicado, en algunos momentos de su historia, inventar símbolos que representen no sólo su lenguaje sino también las abstracciones que su cerebro desarrolla en el proceso del entendimiento. Los ejemplos convencionales son la escritura, los números, y las operaciones que con éstos se realizan. El proceso de almacenar los resultados ha estado, además, tomado de la mano con estos símbolos. En el camino, el hombre ha diseñado también dispositivos que le ayudan a 'calcular' más fácilmente; el ábaco, las reglas de cálculo y las calculadoras contemporáneas (incluyendo a las computadoras) son sólo algunos de los ejemplos más inmediatos. Sin embargo, en 1960, a orillas del Lago Eduardo en África, se encontró un artefacto que es conocido como el *hueso Ishango* [4]. El hueso está datado en el 6500 a.C. y no se corresponde con los ejemplos mencionados líneas arriba. Lo más chocante es la serie de marcas que presenta y que, se sospecha, fueron creadas con al menos 39 herramientas diferentes. Los historiadores concuerdan en que se usó para llevar el registro de alguna actividad; quizás alguna mujer lo diseñó para llevar un conteo de sus ciclos menstruales (las marcas están dispuestas en series que incluyen números primos y que parecen coincidir con las fases lunares). Lo que importa en este ejemplo es el grado de sofisticación que las culturas previas a la era moderna alcanzaron para calcular y registrar eventos (¡descartando, desde luego, una caprichosa coincidencia numerológica con las marcas en un hueso que bien pudieron hacerse al azar!).

El conjunto de eventos históricos relacionados con la actividad (intrínsecamente humana) de registrar, almacenar y procesar información es, como vemos, muy variado. Desde las marcas del primitivo (pero sofisticado) hueso de Ishango hasta las manivelas del mecanismo de Anticitera. El desarrollo de la computación, tal y como la conocemos y disfrutamos hoy en día, ha sido largo; aunque en las últimas décadas se nota un desarrollo inusitado. El lector interesado encontrará bastante provechoso consultar la referencia [4].

Una historia de espectros

Así como una piedra arrojada al agua se convierte
en el centro y la causa de muchos círculos...
así también cada cuerpo... llena el aire que lo rodea
con infinitas imágenes de sí mismo.
Leonardo Da Vinci [5]

Año de 1900, diciembre 14, el físico Max Planck, de 42 años, se enfrenta a una de las disyuntivas más importantes de su vida científica. Todavía puede declinar la presentación de sus resultados ante la comunidad de expertos de la Sociedad Alemana de Física. La razón es que su propuesta

[1] La historia es verdadera, la dramatización y el personaje de Héctor, así como la fama de Elías, son invención del autor. Basado en los datos proporcionados por Carlos A. Coello en su libro *Breve historia de la computación y sus pioneros*.

teórica, además de inusual, a él mismo le resulta grotesca y difícil de creer. Ese maldito espectro no lo ha dejado dormir durante los últimos meses. Le persigue por todas partes, incluso en la ducha, acorralándolo sin apenas darle tiempo de pensar en otra cosa. Tan sencillo que sería, en otra época, olvidarse del asunto. Pero algunos aseguran haberlo visto, incluso le han fotografiado. Así que no cabe la menor duda de su existencia. A muchos otros ya los ha vencido, y los pocos que lograron un primer acercamiento a su explicación no cejan en el intento. ¿En verdad la solución es tan sencilla? ¿Quién va a creerle que el espectro aparece como consecuencia de hacer vibrar armónicamente un conjunto de resortes? Peor aún, de verificarse su propuesta, se necesitaría un conjunto enormemente grande de tales resortes.

Max traga saliva. Está convencido de que sus cálculos no son errados. Los reprodujo una y otra vez, buscando un posible error en el procedimiento, hasta convencerse de que esa era la solución. No podía confiar en nadie, por miedo a ser ridiculizado, hasta no constatar que sus resortes no podrían ser sustituidos por algún otro modelo.

–Los resortes 'respiran', inhalan luz que luego terminan por expeler de la misma forma –se dice Max a sí mismo–, pero igual que los seres humanos sólo pueden aspirar pequeñas cantidades de aire, aún cuando éste llena todo el espacio en la superficie de la Tierra, los resortes solo pueden 'aspirar' pequeñas porciones de luz. ¡No existe otra explicación! La luz es absorbida y emitida por la materia en pequeños paquetes (cuantos) aún cuando llena todo el espacio. Sólo esta interpretación justifica el espectro de radiación que emiten los cuerpos al ser calentados.

Max menea la cabeza en un gesto de negación. –Ni qué decir que esto contraviene las hipótesis de James Clerk Maxwell, quien interpretó a la luz como un conjunto de ondas que se desplazan en el vacío en forma similar a como lo hacen en el agua. El *éter* –seguía el monólogo– se propuso como medio de propagación de la luz, éste serviría como el "agua" de las ondas electromagnéticas. Si bien Albert Michelson y Edward Morley desecharon con su experimento el concepto del éter –recuerda Max mientras limpia sus gafas– también es cierto que las ondas electromagnéticas son apropiadas para describir casi todos los fenómenos de la luz que conocemos. Pero... ¿y el espectro? ¿Será posible que el viejo Maxwell se hubiera equivocado?

Entonces Max cobra valor. ¡Debe exponer sus ideas! ¡Debe correr el riesgo! Llegó su turno... el presentador lo anuncia y la sala queda en silencio...

–Estimados Colegas, permítanme, antes que nada, mencionar que en mi propuesta a la solución del problema de la radiación del cuerpo negro requeriré de ciertas hipótesis que se plantearán como mera herramienta matemática, sin que hasta este momento tenga una interpretación física para ellas; sin embargo, los resultados son satisfactorios si consideramos...[2]

La presentación de Planck, aquel 14 de diciembre, provocó la excitación de la audiencia... y del mundo entero. Antes de 1900 se pensaba que la física, como medio para explicar el comportamiento de la naturaleza, estaba agotada. El enorme edificio construido por Isaac Newton parecía inextendible e inmodificable, su visión del Universo como un gigantesco diseño de relojería había permeado en la mayoría de los físicos quienes, para ese entonces, se acercaban más al ámbito de la ingeniería que al de la física. Existían, sin embargo, algunos detalles que no cuadraban. Uno de ellos era precisamente el desajuste entre la teoría y el experimento relacionados con la luz que emiten los cuerpos al calentarse. La interpretación ondulatoria de

[2]Nuevamente, hasta este punto, la dramatización es una libertad del autor. En ningún momento se pretende suponer que lo descrito en los párrafos anteriores de esta sección corresponde a las disquisiciones de Planck. El lector debe tomar en cuenta que se busca una explicación amena de los conceptos que se requieren.

Maxwell fallaba para explicar el fenómeno. La hipótesis de Planck dio un vuelco a la física del Siglo XIX. Su modelo consistía en suponer que la materia está compuesta por una cantidad infinita de 'resortes' independientes entre sí. Al calentar la materia, estos resortes se excitarían y empezarían a oscilar, emitiendo finalmente radiación. Los resortes tienen ciertos 'modos' de oscilación que requieren de energías específicas para vibrar armónicamente. La luz, entonces, debería proporcionar exclusivamente estas energías.

Aparte del escándalo causado por la propuesta de Planck, ésta solo quedó latente como modelo durante cinco largos años hasta que un joven desconocido, en 1905, decidió tomarla en serio e investigar qué más se podría hacer con ella. Aquel joven llamaría la atención del mundo entero y transformaría para siempre la forma de entender al Universo. Hablamos de Albert Einstein.

Usando las ideas de Planck, Einstein logró explicar otro de los enigmas de la Mecánica Clásica: el efecto fotoeléctrico. Al hacer incidir luz de determinados colores sobre ciertos materiales, éstos emiten un *chorro* de electrones. El fenómeno ha significado una pléyade de aplicaciones tecnológicas que abarcan desde las simples calculadoras de bolsillo, hasta sistemas electrónicos de identificación que sirven, entre otras cosas, como mecanismos de seguridad. Lo que Einstein hizo fue generalizar la idea de los cuantos de luz de Planck y suponer que la luz no sólo se absorbe y se emite en pequeños paquetes. ¡La luz está compuesta por cuantos de radiación! Cada uno de ellos es portador de una cierta energía que define el color de la luz. De esta forma, sólo los cuantos de luz que sean portadores de una determinada energía (i.e., de un determinado color) serán absorbidos por los electrones que conforman la materia. A mayor energía de los cuantos de luz, más profundos en el material estarán los electrones que finalmente le serán "arrancados". Los cuantos de luz son como 'galletitas' energéticas para los perezosos electrones, que se resisten a abandonar el material.

Con la interpretación de Einstein, a su vez, se logró entender otro de los fenómenos que no cuadraban con la Mecánica Newtoniana: un haz de luz se dispersa si se le hace pasar por una nube de electrones (dispersión Compton). Al considerar a la luz simplemente como un conjunto de ondas resulta muy complicado explicar esta propiedad. Sin embargo, al pensar en la luz como un chorro de partículas (cuantos) se puede asumir que cada una de ellas, tarde o temprano, chocará con alguno (o varios) de los electrones; en la misma forma que los niños hacen colisionar canicas en sus juegos infantiles. Como resultado de la colisión, los cuantos de luz cambian de dirección produciendo, en conjunto, el fenómeno de la dispersión.

En la actualidad asumimos que los entes cuánticos manifiestan propiedades duales; decimos que en algunas ocasiones se comportan como ondas (difracción de electrones cuando se les hace pasar por una red cristalina) y en otras se comportan como partículas (cuantos de luz colisionando con los electrones en la dispersión Compton). Independientemente de la controversia que esta interpretación genera, lo cierto es que en algunos experimentos es más sencillo considerar a la luz como partícula mientras que en otros lo mejor es considerarla como onda. El sentido práctico del asunto es que, finalmente, no importa la 'verdadera' naturaleza de los fotones (y demás entes cuánticos) tanto como el carácter fuertemente predictivo de la teoría cuántica. Hasta el momento no logramos entender al cien por ciento cómo es que la teoría funciona, pero sabemos que funciona.

En el camino, desde 1900, hemos aprendido que los sistemas cuánticos tienen otras propiedades que les son singulares. Mencionaremos tres de ellas. Primero, los electrones pueden atravesar "paredes" (*efecto túnel*). Si el lector intentase atravesar la pared que separa su habitación del resto del edificio (¡sin usar puerta alguna!), terminaría adolorido sin lograr su objetivo. Pero, si el

lector tuviese las dimensiones de un electrón, lo que normalmente entiende por 'pared' carecería de sentido. En su lugar, el electrón-lector detectaría una barrera de potencial (un reservorio de energía) que le sería más transparente mientras más rápido se moviese. Dependiendo de su rapidez, algunas veces pasaría la región del potencial sin apenas enterarse de su existencia mientras que en otras saldría 'rebotado' en la dirección opuesta, como si se hubiese estrellado con una enorme membrana elástica. Esta característica tan peculiar es compartida con los electrones por todos los entes cuánticos (incluyendo los cuantos de luz, ahora conocidos como *fotones*) y es considerada como la 'huella digital' de la Mecánica Cuántica. Su descripción data de 1928 y se le adjudica al físico George Gamow (ver por ejemplo [6]). El efecto túnel es lo que permite que los transistores funcionen como funcionan y representó la primera aplicación de la teoría cuántica a la explicación de fenómenos que, originalmente, no estaban en su campo de acción.

Segundo. Los átomos de plata se comportan como pequeños imanes ante la presencia de campos magnéticos. Esta propiedad fue descubierta por los físicos Walther Gerlach y Otto Stern durante 1921 y 1922. Hicieron pasar un haz de átomos de plata a través de un campo magnético y detectaron que el haz se dividía en dos; uno de estos nuevos haces se deflectaba en la dirección del campo mientras que el otro lo hacía en sentido opuesto. Como los átomos de plata son eléctricamente neutros (su carga eléctrica total es cero), la explicación de este fenómeno debería buscarse en el ámbito magnético. Se propuso entonces que el *momento magnético* de los átomos de plata podría tomar sólo uno de dos posibles valores, lo que explicaría la alineación o anti-alineación de los haces de salida con el campo. Este resultado era bastante chocante ya que, antes de los experimentos de Gerlach y Stern, no había evidencia experimental contundente que permitiera sospecharlo; el momento magnético, según la teoría electromagnética de Maxwell, no está constreñido a tomar tales o cuales valores. Posteriormente se entendió que el momento magnético de los átomos de plata está directamente relacionado con una propiedad cuántica de la materia, ahora conocida como *espín*. El espín es independiente de cualquier otra variable física que se le pueda adjudicar a un sistema cuántico, siempre existe, y puede tomar los valores 0, $\pm 1/2$, ± 1, $\pm 3/2$, etc. (por sencillez hemos omitido las unidades). El espín total de los átomos de plata es, por ejemplo, 1/2, igual que el de los electrones. Desde el punto de vista matemático, el espín puede representarse por un vector, igual que el momento angular (cantidad asociada con la rotación de los sistemas físicos). Para el caso de espín 1/2, no importa en qué dirección lo midamos, siempre encontraremos uno de dos posibles valores: 1/2 o -1/2.

Tercero. Los sistemas cuánticos obedecen el *principio de incertidumbre*. Para clarificar este punto notemos que el lector puede medir, si así lo desea, con precisión arbitraria la posición y la rapidez de todos y cada uno de los vehículos que circulan por Avenida Insurgentes. Su frustración, por el contrario, se hará patente al pretender medir simultáneamente la posición y la rapidez de tan sólo uno de los átomos del aire que respira. Al medir la posición del átomo se sabrá poco acerca de su rapidez y viceversa, no importando el equipo de medición que se use.

Como hemos visto a lo largo de esta sección, los sistemas cuánticos parecen incontrolables. Los electrones, fotones, protones y demás entes cuánticos son eternamente adolescentes, tan rebeldes que difícilmente se les puede "obligar" a definirse por un comportamiento específico.

Para saber más de la historia de la teoría cuántica, el lector puede consultar los libros de Gamow [6-8]. El libro de Eisberg y Resnick representa una buena introducción a la Mecánica Cuántica [9], mientras que el de Cohen-Tanoudji, Diu y Laloë es más avanzado [10].

Una lista interminable de ceros y unos

¡Mi computadora Boole-bucea!

–Señor Edison ¿no le desaniman tantos fracasos?
–¿Fracasos? No sé de que me hablas. Ahora, definitivamente, conozco más de mil maneras de cómo NO hacer una bombilla.

El lenguaje de las computadoras está desarrollado por medio de un balbuceo de ceros y unos. Simbólicamente se trata de variables binarias (o booleanas, nombre heredado de su precursor George Boole), las cuales toman sólo uno de dos posibles valores: 0 y 1. Estas variables pueden representarse por cualquier cosa: una bombilla eléctrica encendida puede significar 1 mientras que una apagada significaría 0. Si una determinada corriente pasa a través de una resistencia significa 1, de otra forma tendremos un cero.

Supongamos que tenemos una sola variable, digamos un foco. Cualquier operación que se efectúe sobre esta variable sólo puede modificar su valor de 0 a 1, o viceversa (sólo podríamos encender el foco si éste está apagado, y viceversa). Esta operación es conocida como *negación*. Si nos preguntamos ¿está encendido el foco?, al símbolo 1 le podemos asignar el valor de *cierto* y a 0 el de *falso*. Al aplicar la negación después de obtener una respuesta a nuestra pregunta observamos que lo cierto se transforma en falso y viceversa. La iteración de la negación deja a la variable intacta (la negación de la negación es una afirmación). Denotemos por x, y, z a las variables booleanas, la negación de x se simboliza como $\bar{x}$ y la doble negación como $\bar{\bar{x}}$. Así $y = \bar{x}$ significa que y es la negación de x y la doble negación se lee $\bar{\bar{x}} = x$.

Compliquemos el asunto y asumamos que ahora contamos con dos focos. Supongamos que la contingencia ambiental de fase 1 se regula por la presencia de estos dos focos; si ambos están encendidos los autos pueden circular libremente, de otra forma deben detenerse de inmediato. Ante la pregunta ¿puede circular mi auto? la respuesta (variable de salida) es afirmativa (cierto) si y sólo si ambos focos (variables de entrada) están encendidos (ambas variables de entrada son ciertas). Esta operación es conocida como *y lógica* y será denotada por $\wedge$. Podemos ahora construir una *tabla de verdad* como sigue:

foco 1	foco 2	$\wedge$
0	0	0
1	0	0
0	1	0
1	1	1

El programa de contingencia ambiental de fase 2, como sabemos, es más relajado. En este caso, los autos podrán circular si ambos focos, o sólo uno de ellos, están encendidos. Esta operación es conocida como *o lógica* y será denotada por $\vee$. La tabla de verdad en este caso es

foco 1	foco 2	$\vee$
0	0	0
1	0	1
0	1	1
1	1	1

Notemos que con sólo un foco podemos establecer una sola operación, mientras que con dos focos el número de operaciones aumenta; ya tenemos, al menos, dos operaciones independientes. Podemos ahora preguntarnos cómo sumar variables booleanas. Tenemos una complicación ya que, al parecer, nos faltarán símbolos. Si *x* e *y* representan, en efecto, a los números 1 y 0, está claro que 0+0 = 0 y 1+0 = 0+1 = 1. Pero, ¿qué pasa con 1+1? Recordemos lo que sabemos. En la notación de base diez (i.e., tenemos diez dígitos: 0,1,2,3,4,5,6,7,8 y 9), cualquier variable ξ se representa por

$$\xi = \sum_{k=0}^{n} (\xi_k \times 10^k) = \xi_n \times 10^n + \xi_{n-1} \times 10^{n-1} + \ldots + \xi_1 \times 10^1 + \xi_0 \times 10^0$$

donde los coeficientes ξ_k pueden tomar cualquiera de los valores 0, 1,...,9, y $10^0 \equiv 1$, $10^1 \equiv 10$, $10^2 \equiv 100$, etc. Así, por ejemplo, el número 8 se expande sólo con el primer coeficiente $\xi_0 = 8$ y los demás ξ_k son cero; el número 4967, por el contrario, tiene como únicos coeficientes diferentes de cero a $\xi_3 = 4, \xi_2 = 9, \xi_1 = 6, \xi_0 = 7$, es decir:

$$4967 = 4 \times 10^3 + 9 \times 10^2 + 6 \times 10^1 + 7 \times 10^0.$$

Con estas mismas reglas, en notación de base dos tenemos:

$$x = \sum_{k=0}^{n} (x_k \times 2^k) = x_n \times 2^n + x_{n-1} \times 2^{n-1} + \cdots + x_1 \times 2^1 + x_0 \times 2^0$$

donde los coeficientes x_k son booleanos (valen 0 o 1) y $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, etc. De esta forma, el número 2 tiene sólo los dos primeros coeficientes diferentes de cero: $x_1 = 1, x_0 = 0$, así que debemos representarlo por $2 = 10 = 1 \times 2^1 + 0 \times 2^0$. El número 5 quedaría como 101 y el 22 como 10110.

Por otro lado, recordemos que en la suma convencional se requiere del 'acarreo'. Por ejemplo, en la siguiente operación

$$\begin{array}{cccc} & & 1 & \\ & & 8 & 7 \\ + & 9 & 0 & 4 \\ \hline & 9 & 9 & 1 \end{array}$$

la línea superior corresponde a los números de acarreo que resultan por que la suma parcial de alguna de las columnas se ‘desborda’, dando como resultado un número de más de un dígito. En este caso, el número 1 de la segunda columna (de derecha a izquierda) surge de sumar 7+4, que resulta 11. Entonces ‘ponemos’ 1 en la casilla de resultado de la primera columna y ‘llevamos’ 1 a la casilla de acarreo de la segunda. Esta última no se desborda ya que 1+8+0=9, así que no se requiere de acarreo en la tercera.

Ahora denotemos a la suma booleana con el símbolo ⊕. En base dos tendremos 1⊕1=10, y el resultado se desborda. Debemos ‘poner’ 0 y ‘llevar’ 1. Nuestra regla de sumar resulta entonces en:

$$\begin{array}{cccc} & 1 & & \\ & & 1 & 0 \\ \oplus & & 1 & 1 \\ \hline & 1 & 0 & 1 \end{array}$$

El lector puede constatar que esta suma corresponde a 2+3=5 en base 10. Para realizar esta operación con focos necesitaremos al menos cuatro hileras horizontales de tres focos cada una. La hilera superior corresponderá a los ‘focos de acarreo’, las siguientes dos (de arriba hacia abajo) a los sumandos y la cuarta al resultado. La operación es sencilla: en un principio la hilera de acarreo tiene todos los focos apagados. Si la primera columna de sumandos (de derecha a izquierda) tiene al menos un foco prendido, entonces prenderemos el foco correspondiente al resultado. Si los dos sumandos están apagados, el foco del resultado se dejará apagado. Si esta columna, por el contrario, tiene los dos focos prendidos, mantendremos el foco del resultado apagado y prenderemos el foco de acarreo de la columna siguiente, y así sucesivamente. Para terminar, la suma booleana, igual que la suma convencional, es una operación que se realiza ‘a pares’. Es decir, sólo podemos sumar dos dígitos a la vez. Así que, en las columnas donde los focos de acarreo estén encendidos, se tendrán que hacer tantas sumas como sean necesarias. La tabla de verdad para la suma booleana de dos variables es como sigue:

foco 1	foco 2	⊕
0	0	0
1	0	1
0	1	1
1	1	0

donde, como es costumbre, sólo hemos representado a la variable ‘poner’ y hemos omitido la variable ‘llevar’.

Ahora que hemos aprendido cómo realizar operaciones lógicas con un conjunto de focos podemos ir a la tienda de la esquina (¡si todavía existen!) y comprar tantos focos como podamos. Los necesitaremos para armar un dispositivo al que ‘entrenaremos’ para hacer operaciones cada vez más complejas. La *resta* será fácil, la multiplicación es un poco más complicada y la división nos dará dolores de cabeza. Pero, con un poco de optimismo y mucha paciencia, lograremos que

nuestro dispositivo 'aprenda' a integrar, diferenciar, calcular áreas y límites. Después le enseñaremos a graficar y a realizar todas las cosas que nos han maravillado de las computadoras convencionales. Así se construyó la primera de ellas, era un armatoste tan grande que requería el espacio de un enorme salón para hospedarla, y ni qué decir del calor que se producía. Afortunadamente, muchos científicos e ingenieros ya hicieron la tarea antes que nosotros y han resuelto todos los problemas que esto involucraba para obtener un dispositivo útil y portable. Lo cual es un alivio... y aún siguen trabajando en el diseño de equipos cada vez más eficientes y prácticos.

Para terminar esta sección diremos algo acerca de la nomenclatura estándar. La cantidad mínima de información que se puede almacenar en el disco duro de una computadora se representa por una variable booleana: 0 o 1, y recibe el nombre de *bit* por su acepción en inglés *binary digit* (dígito binario). Mientras más bits se tengan a la mano mayor será la información que se puede representar. Un *byte* equivale a 8 bits y representa $2^8 = 256$ diferentes opciones, un *word* (palabra) corresponde a 16 bits y representa $2^{16} = 65536$ opciones diferentes. Poniéndonos exigentes tenemos que un *kilobyte* son $1024 (= 2^{10})$ bytes, mientras que el prefijo *mega* corresponde a 2^{20}, un *giga* a 2^{30} y un *tera* a 2^{40}. Cada operación independiente que se realice sobre los bits será llamada *compuerta lógica*. Por independiente entenderemos que no se puede realizar como una secuencia de cualesquiera otras operaciones. Así, las operaciones $\bar{x}$, $x \wedge y$, $x \vee y$, y $x \oplus y$ son ejemplos de compuertas lógicas.

El lector interesado en profundizar en el lenguaje y la estructura de las computadoras convencionales puede consultar el libro de Miguel Lindig Bos, citado en la referencia [11].

El canto de las sirenas cuánticas

Se me debe exigir que busque la verdad,
pero no que la encuentre
Denis Diderot: Pensées Philosophiques

En la sección anterior aprendimos que podemos usar prácticamente cualquier cosa para representar una variable booleana en un dispositivo de cálculo. ¿Qué tal si usamos átomos?, ¿qué tal electrones?, ¿fotones? ¿Qué nos lo impide?

Pongamos orden a estas preguntas. Primero, necesitamos identificar cómo sustituir los focos de nuestro armatoste por entes cuánticos. Para ello recordemos la segunda de las propiedades listadas en nuestra *historia de espectros*. Los entes cuánticos tienen espín, y algunos de ellos, como el electrón y los átomos de plata, tienen espín 1/2. Esto significa, como ya sabemos, que sólo pueden manifestarse dos posibles alineaciones del espín 1/2 en presencia campos magnéticos. Denotemos por $|0\rangle$ al estado de espín ½ que se alinea paralelamente con el campo y por $|1\rangle$ al que se alinea antiparalelamente. La notación $|\cdot\rangle$ es llamada *notación de Dirac* y es común para representar el estado físico de un sistema cuántico. Como vemos, los estados de espín pueden ser útiles como los "focos cuánticos" de nuestro dispositivo de cálculo.

Al aplicar un campo magnético lo que hacemos es "pedirle" al foco cuántico que nos muestre una de las dos posibles alineaciones de su espín, es decir, ¡estamos midiendo el estado de espín! Antes de la medición, el espín puede estar no sólo en uno u otro valor, sino en una combinación

de ambos. En otras palabras, antes de que verifiquemos si nuestro foco cuántico está encendido o apagado, éste se encontrará en un estado $|\psi\rangle$ que representa a un foco que está al mismo tiempo encendido y apagado (recordemos lo rebeldes que son estos bichos). Decimos entonces que el estado de espín ½ está en una combinación lineal de los estados $|0\rangle$ y $|1\rangle$. Matemáticamente representamos esta propiedad como una suma:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle. \tag{1}$$

Esta superposición lineal obedece a la dualidad (onda-partícula) de los sistemas cuánticos y es indispensable para explicar sus manifestaciones ondulatorias. En la ecuación (1), a y b son números complejos. A diferencia de las variables booleanas x, y, z (que pueden tomar sólo uno de dos posibles valores), la variable $|\psi\rangle$ (que llamaremos *vector* ψ) puede tomar cualquiera de los valores que resulten de las combinaciones de a y b en (1). Es decir, con lo caprichosos que son los sistemas cuánticos, no podemos decir con certidumbre (antes de medirlos) cuánto valen a y b en cualquier momento. Sólo podemos jugar a las probabilidades. Diremos que el vector $|\psi\rangle$ tiene la probabilidad $|a|^2$ de estar en el estado $|0\rangle$ y la probabilidad $|b|^2$ de estar en el estado $|1\rangle$. Asumiendo que la partícula en cuestión existe, la probabilidad de encontrarla en cualquiera de tales estados debe ser $|a|^2+|b|^2=1$. Por ejemplo, el sistema puede estar en el estado

$$|\psi\rangle = \sqrt{\frac{1}{2}}|0\rangle + \sqrt{\frac{1}{2}}|1\rangle \tag{2}$$

entonces, como resultado de una medición, se tendrá igual probabilidad (50 por ciento) de encontrarlo en el estado $|0\rangle$ que en el estado $|1\rangle$. Para verificar esta predicción se requiere hacer estadística, es decir, correr varias veces el mismo experimento de medición, mientras más veces se efectúe el experimento mucho mejor.

En análoga con las variables booleanas llamaremos al vector ψ un *qubit* (por el acrónimo en inglés *quantum bit*). Así, un qubit no es más que un vector en un espacio complejo bidimensional que denotaremos por H. A los vectores especiales $|0\rangle$ y $|1\rangle$ se les conoce como *base de estados computacional* por que con ellos se puede construir cualquiera de los $|\psi\rangle$ en H. Como los vectores ψ son tales que $|a|^2+|b|^2=1$, diremos que tienen norma 1 (i.e., son de longitud 1) y, geométricamente, podemos representarlos como los puntos sobre la superficie de una esfera de radio 1, conocida como la *esfera de Bloch* (ver Figura 1). En esta perspectiva geométrica, el vector $|0\rangle$ corresponde al Polo Norte de la esfera mientras que $|1\rangle$ es su "antípoda": el Polo Sur (en cada caso, también se puede asumir la representación por medio de *flechas* cuya cola está en el centro de la esfera y cuya punta localiza el punto en cuestión. Cualquier otro vector $|\psi\rangle$ admite esta representación de flechas). Aprovechando la geometría involucrada podemos parametrizar a nuestros vectores ψ en términos de los ángulos θ y φ de las coordenadas esféricas (r=1):

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) \tag{3}$$

donde γ es un número real arbitrario que se ha introducido por mera formalidad (en la práctica uno puede ignorar el factor $e^{i\gamma}$). Obsérvese que cualquier punto sobre la esfera de Bloch podrá entonces describirse como una combinación del Polo Norte y del Polo Sur en términos de lo que valgan los parámetros θ y φ.

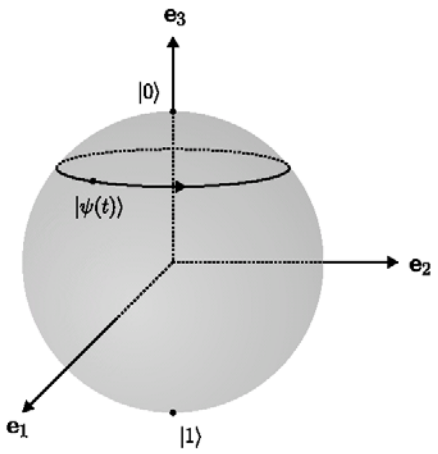

Figura 1: Representación de un qubit en la esfera de Bloch. El vector |0⟩ localiza al Polo Norte y |1⟩ al Polo Sur. Para un qubit arbitrario $|\psi(t)\rangle$, la presencia de un campo magnético **B**, apuntando en la dirección *z*, lo obliga a danzar alrededor del vector $\mathbf{e}_3$. La figura es una versión modificada de las publicadas en [12], por cortesía de su autor (S.G. Cruz y Cruz).

La habilidad de los qubits para estar, antes de la medición, en un continuo de estados (superposición) entre |0⟩ y |1⟩ violenta nuestro sentido común. Son entes 'multi-rostro' que siempre se nos ocultan para no identificarlos completamente. Pero, a pesar de sus 'extravagancias', son decididamente reales. Su existencia y comportamiento están validados por experimentos como los que mencionamos en la *historia de espectros*. Además, existe una enorme variedad de sistemas físicos que pueden ser usados para construirlos. Si escogemos fotones, por ejemplo, los vectores |0⟩ y |1⟩ podrían estar representados por alguna de dos posibles polarizaciones. Las compuertas lógicas correspondientes estarían representadas por polarizadores ópticos que reorienten a |0⟩ y |1⟩ en la forma apropiada. Podemos también escoger átomos con un único electrón exterior. Este último deberá tener sólo uno de dos posibles valores de la energía: su estado base (la energía más baja posible) y un único estado excitado (cualquier otro valor fijo de la energía). Las compuertas lógicas, en este caso, pueden implementarse por medio de baños de luz de determinados *colores* para excitar al electrón y arrancarlo de su estado base o, incluso, para 'enfriarlo' y hacer que descienda de su único estado excitado al estado fundamental por medio de la emisión de un fotón.

Si trabajamos con espines 1/2, lo apropiado sería usar campos magnéticos para realizar operaciones lógicas. En la *historia de espectros* comentamos que esta clase de espín es, en cierto sentido, un imán diminuto (ante campos magnéticos se comporta como la aguja de una brújula). Supongamos que tenemos un campo magnético homogéneo apuntando en la dirección *z* del plano cartesiano, es decir $\mathbf{B}=B_z\mathbf{e}_z$, donde $\mathbf{e}_z \equiv \mathbf{e}_3$ es un vector de longitud 1, sobre la vertical, apuntando hacia arriba. Ahora coloquemos nuestro qubit $|\psi\rangle$ en la región del campo. Si nuestro vector ψ apunta originalmente en la misma dirección que **B**, es decir $|\psi\rangle=|0\rangle$, entonces se mantendrá así, localizando por siempre al Polo Norte. Si, por el contrario, apunta en cualquier otra dirección (digamos que localiza un punto en el casquete superior de la esfera), entonces empezará a danzar al rededor del vector $\mathbf{e}_3$, describiendo un círculo centrado en el origen de coordenadas y paralelo al plano *xy* (ver Figura 1). Denotemos por **Z** a esta operación. Una forma

económica de representarla matemáticamente es usando la notación de Hubbard (consúltese [13]), tenemos $\mathbf{Z}=|0\rangle\langle 0|-|1\rangle\langle 1|$. Para aplicarla sobre nuestros qubits fundamentales usaremos la siguiente regla de símbolos:

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 0|1\rangle = \langle 1|0\rangle = 0.$$

Así, $\mathbf{Z}|0\rangle$ significa lo siguiente

$$\mathbf{Z}|0\rangle \equiv (|0\rangle \langle 0|-|1\rangle \langle 1|) |0\rangle = |0\rangle (\langle 0|0\rangle) - |1\rangle (\langle 1|0\rangle) = |0\rangle \cdot 1 - |1\rangle \cdot 0 = |0\rangle.$$

Tal como mencionamos líneas arriba, **Z** deja intacto al vector $|0\rangle$. El lector puede ahora verificar el resultado $\mathbf{Z}|1\rangle = -|1\rangle$; esto significa que la operación **Z** *cambia* el signo de $|1\rangle$. Para un vector arbitrario (3), la acción de **Z** sólo produce $\varphi \to \varphi + \pi$, es decir, agrega la fase $e^{i\pi}$. Por esta razón a **Z** se le conoce como la *compuerta de cambio de fase*. Para la operación negación, que en el caso cuántico denotaremos por **X**, necesitamos aplicar, por ejemplo, un campo magnético homogéneo dirigido en la dirección *x* del plano cartesiano: $\mathbf{B}=B_x\mathbf{e}_1$. En la notación de Hubbard: $\mathbf{X}=|1\rangle\langle 0|+|0\rangle\langle 1|$. Usando nuestra regla de símbolos es fácil verificar que **X** cambia $|0\rangle$ por $|1\rangle$ y viceversa. Durante su transformación, el punto que originalmente está en el Polo Norte deja una 'estela' sobre la esfera, que corresponde a las posiciones intermedias que va ocupando hasta colocarse en el Polo Sur (compárese con Figura 2). Este proceso se conoce como *rotación de Rabi* y es la 'piedra angular' de la resonancia magnética que se usa en los hospitales para obtener imágenes de, digamos, el cerebro. El lector puede imaginar que el tejido de nuestros órganos es, en una primera aproximación, una red de espines. Todos ellos orientados de forma independiente pero con la 'cola' atada en algún punto. Al aplicar campos magnéticos intensos, los espines danzan alrededor de la dirección del campo, intentando alinearse con el. Un segundo campo, ortogonal al primero y variando sinusoidalmente con el tiempo, es aplicado. Este último provoca que la danza de los espines se altere, algunos de ellos empiezan a cambiar bruscamente de $|0\rangle$ a $|1\rangle$ y viceversa, absorbiendo energía del campo y emitiéndola en forma de fotones. Los fotones emitidos son capturados por un sensor que manda esta información a un amplificador y, después, a un proyector.

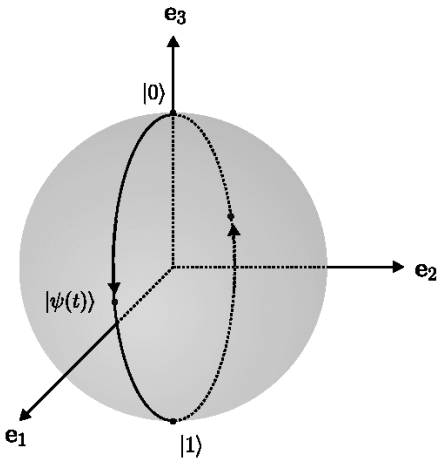

Figura 2: Rotación de Rabi del qubit $|0\rangle$. Durante su transformación, este vector pasa localizando los puntos $\psi(t)$ sobre el círculo paralelo al plano *xz*. La figura es una versión modificada de las publicadas en [12], por cortesía de su autor (S.G. Cruz y Cruz).

Asociado con los qubits de espín 1/2 tenemos también la operación identidad $\mathbf{I}=|0\rangle\langle 0|+|1\rangle\langle 1|$ y la operación generada por campos magnéticos homogéneos en la dirección *y* (ver Figura 2) $\mathbf{Y}=i(|1\rangle\langle 0|-|0\rangle\langle 1|)$. Así, hasta este momento contamos con cuatro *compuertas cuánticas* independientes: **I**, **X**, **Y** y **Z**; todas ellas pueden implementarse por la acción de campos magnéticos sobre estados de espín 1/2. Una compuerta más interesante es $\mathbf{H}=(\mathbf{X}+\mathbf{Y})/\sqrt{2}$, que recibe el nombre de *compuerta de Hadamard*. Esta satisface $\mathbf{H}^2=\mathbf{I}$ y es tal que cambia $|0\rangle$ por una mezcla de $|0\rangle$ y $|1\rangle$: $(|0\rangle+|1\rangle)/\sqrt{2}$ (ver ecuación 2). En forma similar, **H** transforma $|1\rangle$ en $(|0\rangle-|1\rangle)/\sqrt{2}$. En la esfera de Bloch, estos dos últimos vectores corresponden, respectivamente, a los puntos antipodales (1,0,0) y (-1,0,0). Geométricamente, la compuerta de Hadamard induce una rotación $\frac{\pi}{2}$ de la esfera de Bloch alrededor del eje $\mathbf{e}_2$, seguida de una reflexión del plano *xy*. Recientemente se ha reportado la *compuerta* χ*–Hadamard* $\mathbf{H}_\chi$. Esta es tal que $\mathbf{H}_\chi^2=\mathbf{I}$, y se define como $\mathbf{H}_\chi := \mathbf{X}\sin\chi+\mathbf{Z}\cos\chi$ [13]. Su acción sobre los vectores base es como sigue:

$$\mathbf{H}_\chi|0\rangle=\cos\chi|0\rangle+\sin\chi|1\rangle, \qquad \mathbf{H}_\chi|1\rangle=\sin\chi|0\rangle-\cos\chi|1\rangle$$

y para un vector general de la forma (1), tendremos

$$\mathbf{H}_\chi|\psi\rangle=(a\cos\chi+b\sin\chi)|0\rangle+(a\cos\chi-b\sin\chi)|1\rangle.$$

En la esfera de Bloch, los vectores $\mathbf{H}_\chi|0\rangle$ y $\mathbf{H}_\chi|1\rangle$ también están representados por puntos antipodales ($\pm\sin 2\chi,0,\pm\cos 2\chi$). La compuerta χ–Hadamard induce una rotación π-2χ sobre la esfera de Bloch al rededor del eje $\mathbf{e}_2$ más una reflexión del plano *xy*. El lector puede verificar que $\mathbf{H}_{\chi=\pi/4}\equiv\mathbf{H}$. Finalmente, para producir estas operaciones se requiere de campos magnéticos más sofisticados

$$\mu\mathbf{B}(\chi,t)=\dot{\alpha}(t)\sin\chi[\cos\beta(t)\mathbf{e}_1+\sin\beta(t)\mathbf{e}_2]+[\dot{\alpha}(t)\cos\chi-\dot{\beta}(t)]\mathbf{e}_3 \qquad (4)$$

donde $\dot{f}$ denota derivada de *f* con respecto a *t* y la forma específica de las funciones $\alpha(t)$ y $\beta(t)$ depende de las trayectorias que nuestro sistema describa sobre la esfera de Bloch. En general, para $\alpha(0)=\beta(0)=0$, los campos (4) inducirán rotaciones simultáneas de la esfera de Bloch alrededor de las direcciones definidas por $\mathbf{e}_3$ y $\mathbf{e}_\chi$, con rapidez angular dependiente del tiempo $\beta(t)$ y $\alpha(t)$, respectivamente [14, 15].

Como vemos, la versatilidad de los qubits es mayor que la de los bits: para un sólo bit tenemos una única operación $y=\bar{x}$, $\bar{\bar{x}}=x$, mientras que para un sólo qubit tenemos al menos cuatro **X**, **Y**, **X** y $\mathbf{H}_\chi$, ya que $\mathbf{H}_\chi^2=\mathbf{I}$ y $\mathbf{H}_{\chi=\pi/4}=\mathbf{H}$. En la sección anterior aprendimos que a mayor cantidad de focos (bits), más sofisticadas podrían ser las compuertas lógicas involucradas. En eso radica la enorme utilidad de las computadoras convencionales: a mayor capacidad de almacenar y procesar bits, mayor será la sofisticación de las operaciones que nuestro equipo puede hacer. Lo mismo vale para las computadoras cuánticas. Sin embargo, aunque una computadora cuántica con sólo un qubit de información admite cuatro compuertas, este resultado todavía no parece muy apasionante. La riqueza surge cuando pensamos en un *bonche* de qubits, mientras más de éstos tengamos mejor. Si disponemos de una cantidad ilimitada de qubits podríamos ir combinando operaciones para formar cadenas que desarrollen una tarea específica (e.g., calcular una integral).

A cada una de las cadenas les llamaremos *algoritmos cuánticos*, éstos serán cada vez más sofisticados y permitirán, a su vez, realizar tareas cada vez más complejas.

¡La moneda está en el aire! ... ¿Será posible comprar los 'focos cuánticos' que nos hacen falta en la tienda de la esquina?

El lector interesado en los algoritmos de la computación cuántica puede consultar el libro basado en el curso introductorio de Richard P. Feynman [16]; un curso intermedio está dado en el libro de Josef Gruska [17], mientras que los cursos avanzados pueden encontrarse en los libros de Michael A. Nielsen e Isaac L. Chuang [18] y de John Preskill [19]. Un material más formal desde el punto de vista matemático puede encontrarse en el curso de verano dictado por Guillermo Morales-Luna [20]. Las posibilidades de implementar compuertas cuánticas por medio de *pozos cuánticos* se discuten en el curso de verano dictado por Tatiana Rappoport [21].

La aventura continúa

Y será también muy grato y hermoso conocer la contextura sustancial de las estrellas, que un astrónomo llamó nebulosas, y yo con el dedo he demostrado que esta naturaleza es muy diferente de lo que hasta el día de hoy se ha creído
Galileo Galilei: Mensajero sideral

A estas alturas de nuestra discusión todo parece miel sobre hojuelas. Desafortunadamente no es así. Como hemos mencionado iteradamente, los entes cuánticos son 'caprichosos'. En el *canto de las sirenas cuánticas* usamos sólo la segunda de las propiedades dictadas en la *historia de espectros*. Hablemos ahora de las otras dos. En particular, si consiguiéramos 'atrapar' algún ente cuántico en un recipiente, éste podría *tunelear* las 'paredes' que lo contienen. ¡Tenemos el problema de que nuestros adolescentes cuánticos quieren salir de *antros* y, aunque le pasemos llave a su habitación, éstos terminan escapándose por las ventanas! La pregunta natural es ¿para qué queremos atrapar cuantos? Además, ¿cómo lo haríamos?

En la actualidad podemos frenar partículas hasta velocidades muy por debajo de las velocidades térmicas (las moléculas y los átomos se mueven, a temperatura ambiente, con una rapidez cercana a la del sonido: trescientos metros por segundo). Esta situación permite enfriar gases a temperaturas cercanas al cero absoluto, diseñar relojes atómicos y manipular moléculas de ADN. Aún más, al moverse tan lentamente, las partículas pueden ser atrapadas en un *recipiente láser* [22] o en una *botella electromagnética* [23, 24], según sean éstas cargadas o eléctricamente neutras. Incluso la luz puede frenarse y atraparse [25]. El problema sigue siendo el tiempo que podemos mantenerlas atrapadas. A pesar de esto, la importancia de atrapar moléculas, átomos, electrones, fotones y demás entes subatómicos radica en que ellos serán los 'focos cuánticos' con los que construiremos nuestro dispositivo de cálculo. Así que uno de los problemas a resolver es cómo mantenerlos atrapados por el mayor tiempo posible.

Por otro lado, el principio de incertidumbre y la dualidad cuántica representan una limitante muy fuerte para nuestros propósitos. Los cuantos interactúan siempre con todo aquello que les rodea, incluyendo el recipiente que pudiese contenerlos, por lo que ininterrumpidamente están intercambiando *información* con su entorno. El lector ya sabe que "interactuar" con los entes cuánticos significa, de algún modo, medirlos. Cuando los medimos pierden toda su belleza y su

misterio; en cierta forma *los destruimos* por que cambiamos su estado de una combinación lineal arbitraria $a|0\rangle+b|1\rangle$ a una superposición muy específica, digamos que a la descrita por la ecuación (2) o simplemente al estado $|1\rangle$ (que corresponde a $a = 0$ y $b = 1$). Al estar atrapados, el recipiente que los contiene mide constantemente sus diversas variables y termina por destruirlos. A este fenómeno se le conoce como *decoherencia*. El problema al que nos enfrentamos es al de inventar recipientes que interactúen poco con los cuantos. Necesitamos que el tiempo de decoherencia sea, al menos, ligeramente mayor que el tiempo que requerimos para que los cuantos efectúen las operaciones que necesitamos.

Otro conflicto se presenta cuando consideramos que los algoritmos exigen que hagamos operaciones selectivas sobre los focos cuánticos. Si pensamos en una red de espines, por ejemplo, requeriremos que el espín número 10 cambie su orientación de $|0\rangle$ a $|1\rangle$, mientras que el espín 134 obedezca a una transformación de Hadamard y el espín 4 una χ–Hadamard, al tiempo que los demás se sujetan a otras operaciones. El planteamiento teórico de todas estas operaciones se conoce como *manipulación dinámica* (ver por ejemplo [26, 27]). Pero todavía queda mucho camino por recorrer.

Como podemos notar, la serie de dificultades que debemos resolver antes de construir una computadora cuántica se presenta interminable. Consideremos, para continuar, que las computadoras convencionales necesitan un "arranque", es decir, se requiere poner a cero toda la información que se va a manejar antes de empezar cualquier cálculo. Esto significa, por ejemplo, poner a la red de espines en una determinada configuración, lo cual representa una combinación de los tres problemas anteriores. Una dificultad más radica en el manejo de errores. Si no se tiene cuidado, los algoritmos pueden incluir errores recursivos, lo que produciría un resultado erróneo después de algún tiempo de cálculo.

Todos estos problemas parecen cosa de niños si consideramos que para elaborar algoritmos complejos necesitamos más y más focos cuánticos. Sabemos que un ratón, por ejemplo, está compuesto de piel, carne y huesos, entre otras cosas. Cada uno de estos tejidos, a su vez, está compuesto por células y éstas por moléculas, y éstas por átomos, y éstos por otras partículas más fundamentales. Es claro que los últimos miembros de esta lista son entes cuánticos, pero si contamos la historia al revés notaremos que el ratón, a pesar de estar integrado por cuantos, no puede *tunelear* las paredes (¿o si?). Con esto queremos resaltar el hecho de que, al aglutinar una enorme cantidad de focos cuánticos, eventualmente tendremos un ente que deja de obedecer las leyes del mundo cuántico y empieza a obedecer las del mundo macroscópico, al que estamos habituados. Esta situación, al parecer, impone una limitante muy fuerte a la clase de computadoras cuánticas que podríamos construir... y lo que éstas podrían hacer.

Queda entonces la pregunta abierta: ¿Computación Cuántica?

Para terminar debemos mencionar que el panorama no es tan desolador. Por muchas razones hay cientos, sino es que miles, de investigadores alrededor del mundo trabajando en el asunto. En general, cualquier computadora cuántica comercial podría efectuar miles de millones de cálculos en un par de horas. Una tarea que a la mejor de las computadoras convencionales le costaría años e incluso siglos de tiempo-máquina, sin mencionar la cantidad de energía necesaria para alimentarla (ver por ejemplo [28]). Por otro lado, el potencial de una computadora cuántica sería la delicia de los ladrones cibernéticos ya que nuestros códigos de seguridad electrónicos podrían violentarse fácilmente. Los bancos más importantes del mundo están invirtiendo mucho en las investigaciones de esta índole por que el cifrado (criptografía) de las cuentas que manejan

quedaría expuesto una vez que se cuente con una de estas computadoras. Así, los banqueros pretenden ser de los primeros en obtener un dispositivo cuántico de cálculo para inventar nuevas claves y, de esta forma, asegurar las cuentas de sus clientes (y su propio negocio). Sin embargo, como sabemos, los ladrones están siempre a la vanguardia y suelen actualizarse antes que las instituciones. ¿Quién ganará en esta carrera? En otro matiz, los míticos viajes a las estrellas y la teleportación *Sci-fi*, que hasta el momento solo contemplamos en las salas de cine, se antojan cada vez mas viables si la construcción de las computadoras cuánticas se hace una realidad. Recientes investigaciones, por ejemplo, han hecho posible teleportar fotones por distancias de hasta un kilómetro. Pero eso es otra historia.

El lector interesado en el aspecto formal de la manipulación dinámica puede consultar los trabajos de Bogdan Mielnik [29-32]. En el artículo de revisión [26], David Fernández presenta un panorama general de la manipulación dinámica de sistemas cuánticos. Algunas aplicaciones de este formalismo pueden encontrarse en los trabajos [33-36] y [13-15]. En la referencia [27] se relata parte de la historia relacionada con las trampas de partículas. Para los temas paralelos a la Computación Cuántica como son teleportación y criptografía cuántica, además de los libros de Nielsen-Chuang, Gruska y Preskill, el lector puede consultar la referencia [37]. Finalmente, para buscar computadoras cuánticas no hay nada mejor que usar una computadora convencional, la *red de redes* ofrece una infinidad de salidas usando `quantum computing or quantum computation` como palabras de búsqueda. El lector encontrará excelentes páginas web y lo dejamos en libertad de escoger las que más le acomoden.

Agradecimientos

El autor agradece al Prof. Moisés Santillán por su atenta invitación a participar en el proyecto que representa este libro y a la Dra. Sara G. Cruz y Cruz por las figuras que se incluyen. Se reconoce el apoyo secretarial de la Srita. Miriam Araceli Lomelí Cortés, así como el apoyo económico del CONACyT. Parte de este material ha sido presentado como charla para estudiantes en diversas instituciones: Benemérita Universidad Autónoma de Puebla, Universidad Autónoma del Estado de México, CECyT 7 del IPN, Departamento de Física del Cinvestav, Universidad de Burgos (España), y Universidad de Valladolid (España). A todos los asistentes mi agradecimiento.

Bibliografía

[1] Moore G., Cramming more components onto integrated circuits, *Electronics*, **38**, No 8 (April 19, 1965).

[2] Kuekes P.J., Snider G.S., and Williams R.S., Crossbar Nanocomputers, *Sci. Am.* **293**, No 5, 48-55 (November 2005)

[3] Keyes R.W., Miniaturization of Electronics and its Limits, *IBM Journal of Research and Development*, **32**, 24-28 (January, 1988)

[4] Coello C.A., Breve historia de la computación y sus pioneros, *Fondo de Cultura Económica*, México, 2003.

[5] Vallentin A. Leonardo Da Vinci, *Ediciones Vitae*, España, 2004.

[6] Gamow G., El breviario del señor Tompkins, *Fondo de Cultura Económica*, México, 1985.

[7] Gamow G., Thirty years that shook physics, *Dover*, New York, 1985.

[8] Gamow G., The Great Physicists from Galileo to Einstein, *Dover*, New York, 1988.

[9] Eisberg R. y Resnick R., Física Cuántica. Átomos, Moléculas, Sólidos, Núcleos y Partículas, *Limusa*, México, 1988.

[10] Cohen-Tannoudji C., Diu B. y Laloë F., Quantum Mechanics, Vol I., *Wiley*, New York, 1977.

[11] Lindig M., ¿Qué hay detrás de las computadoras?, *publicaciones del IPN*, México, 1994.

[12] Cruz y Cruz S.G., Esquemas cuánticos de Floquet: espectros y operaciones, Tesis Doctoral, *Cinvestav*, México, 2005.

[13] Rosas-Ortiz O., Quantum Control of Two-level Systems, en Moya-Cessa H, et. al. (Eds), Proceedings of the 8th International Conference on Squeezed States and Uncertainty Relations, *Rinton Press*, Princeton, 2003.

[14] Fernández D. y Rosas-Ortiz O., Inverse techniques and evolution of spin-1/2 systems, *Phys. Lett. A* **236**, 275 (1997)

[15] Fernández D. y Rosas-Ortiz O., Evolution loops and spin-1/2 systems, en Schlichenmaier M., et. al. (Eds), Coherent States, Quantization and Gravity, *Varsaw University Press*, Varsaw, 2001.

[16] Feynman R.P., Feynman Lectures on Computation, *Perseus Publishing*, EUA, 1999.

[17] Gruska, J., Quantum Computing, *Mc Graw Hill*, Cambridge, 1999.

[18] Nielsen M.A. y Chuang I.L., Quantum Computation and Quantum Information, Cambridge, 2000.

[19] Preskill J., Lecture Notes for Physics 229: Quantum Information and Computation, *California Institute of Technology*, EUA, 1998.

[20] Morales-Luna G., Basics for Algorithms in Quantum Computing, en Rosas-Ortiz O, et. al. (Eds), *AIP Conference Proceedings* **809**, New York, 2005.

[21] Rappoport T.G., Semiconductors: Nanostructures and Applications in Spintronics and Quantum Computation, en Rosas-Ortiz O, et. al. (Eds), *AIP Conference Proceedings* **809**, New York, 2005.

[22] Chu S., Laser Trapping of Neutral Particles, *Sci. Am.* **266**, Núm. 2, 48 (1992)

[23] Ekstrom P. y Wineland D., The isolated electron, *Sci. Am.* **243**, Núm. 2, 90 (1980)

[24] Fernández D. y García R., Física: Átomos sin núcleo como nuevos patrones de tiempo, *Avance y Perspectiva, Cinvestav* **8**, 30 (1989)

[25] Hau L.V., Frozen Light, *Sci. Am. Sp.* **13**, Núm. 1, 44 (2004)

[26] Fernández D., The manipulation problem in Quantum Mechanics, en Ballesteros A., et al (Eds), *Symmetries in Quantum Mechanics and Quantum Optics*, Universidad de Burgos, España, 1999 (visitar la página `http://www.fis.cinvestav.mx/~david`)

[27] Rosas-Ortiz O., Manipulando el mundo atómico: Ingeniera Cuántica, *Avance y Perspectiva,* **23**, 19 (2005) (visitar la página `http://www.fis.cinvestav.mx/~orosas`)

[28] Nielsen M.A., Simple rules for a complex quantum world, *Sci. Am. Sp.* **13**, 24 (2003)

[29] Mielnik B., Generalized Quantum Mechanics, *Comm. Math. Phys.* **37**, 221 (1973)

[30] Mielnik B., Global mobility of Schrödinger's particle, *Rep. Math. Phys.* **12**, 331 (1977)

[31] Mielnik B., Space Echo, *Lett. Math. Phys.* **12**, 49 (1986)

[32] Mielnik B., Evolution loops, *J. Math. Phys.* **27**, 2290 (1986)

[33] Mielnik B. y Fernández D.J., An electron trapped in a rotating magnetic field, J Math Phys **30**, 537 (1989)

[34] Fernández D.J. y Mielnik B., Nodal resonance in a strong standing wave, Phys Rev A **41**, 5788 (1990); Fernández D.J. y Mielnik B., Controlling quantum motion, J Math Phys **35**, 2083 (1994)

[35] Fernández D.J., Transformations of a wave packet in a Penning trap, Nuovo Cim. **107 B**, 885 (1992)

[36] Cruz y Cruz S. y Mielnik B., The parity phenomenon of the Floquet spectra, Phys. Lett. A **352**, 36 (2006)

[37] Bouwmeester D., Ekert A. y Zeilinger A (Eds), The Physics of Quantum Information, *Springer*, Alemania, 2001.