UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

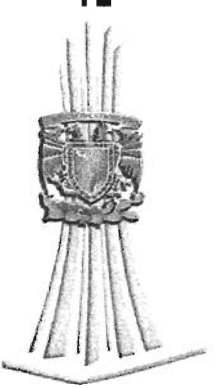
FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

"COMPUTACIÓN CUÁNTICA"

T E S I S
PARA OBTENER EL TITULO DE:
INGENIERA EN COMPUTACIÓN

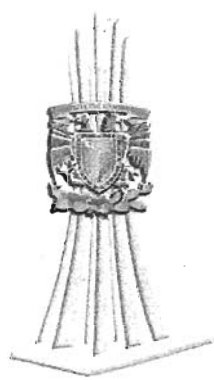
PRESENTA:
Nidia Cendejas Cervantes

ASESOR: **Mat. Luis Ramírez Flores**



MÉXICO 2005

Computación Cuántica



AGRADECIMIENTOS

A MIS PADRES:

A quienes me han heredado el tesoro más valioso que puede dársele a un hijo: Amor. A quienes sin escatimar esfuerzo alguno han sacrificado gran parte de su vida para formarme y educarme. A quienes la ilusión de su vida ha sido convertirme en persona de provecho. A quienes nunca podré pagar todos sus desvelos ni aún con las riquezas más grandes del mundo. Por esto y más GRACIAS.

A MIS HERMANOS:

(Adolfo, Toña, Lucía, Chayo, Juanito), A quienes con su ayuda y apoyo, he logrado llegar a una de mis metas, y ser quien ahora soy.

A CARLOS:

A quien con su amor, cariño, compresión, tiempo y sobre todo ayuda logre terminar de dar este paso tan importante para mí.

AL MTRO. LUIS:

A quien no sólo fue mi asesor, sino mi gran amigo, que me ha apoyado en las buenas y en las malas, por los consejos que me ha dado para saber dirigirme por el camino de la vida. No tengo palabras para agradecerle todo lo que ha hecho por mí, y solo puede decirle GRACIAS.

AL MTRO. EDGAR LIÑAN:

Por su apoyo y revisión en este trabajo.

A la UNAM:

Por haberme formado como Universitaria y en especial a la FES Aragón.

"... a nivel cuántico no es posible conocer de forma exacta el momento lineal y la posición de una partícula. O de forma más correcta, es imposible conocer dichos valores más allá de cierto grado de certidumbre. A nivel cuántico las partículas no son pequeñas esferas, sino borrones. Si es posible fijar la posición de la partícula con total precisión será imposible conocer su velocidad. Si por el contrario se conoce su velocidad, no se sabrá a ciencia cierta en qué punto se halla. Esto tiene un curioso colorario, que no se observa en el mundo macroscópico: la acción del observador altera el sistema observado".

Werner Heisenberg

ÍNDICE

INTRODUCCIÓN

La tecnología en computación avanza de manera constante; a la par, se requiere manejar una gran cantidad de información en diversas áreas del conocimiento y es aquí donde se prevee que, al cabo de poco tiempo, la informática convencional será incapaz de satisfacer los requerimientos tan apremiantes en esta época. Por tal razón, en la presente tesis se aborda dicha problemática. La investigación indaga hacia dónde se dirige la tecnología en computación así como los medios que existen para poder cubrir la demanda creciente de este servicio tan urgente e importante en la actualidad.

En primer lugar, se expondrá un panorama general de lo que constituye la computación cuántica, tecnología que se cree, podrá resolver de una manera eficiente el problema antes mencionado. Con esta tecnología se han hecho experimentos incipientes, uno de ellos es la velocidad de procesamiento para encontrar la solución a problemas relativamente complejos o realizar una búsqueda rápida en una base de datos con elementos considerablemente grandes. Al resolver esta cuestión se ha demostrado que una computadora convencional se ha tardado horas o hasta días en ofrecer el resultado; sin embargo, una computadora cuántica lo daría en lapsos mas breves, de esta manera habrá una alternativa más interesante y al parecer más económica.

Con el fin de poder comprender cuál es el funcionamiento de las computadoras cuánticas y qué tanto podemos lograr con ellas, proponemos la siguiente metodología:

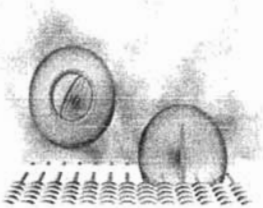
1. Como primer tema, se mencionará en términos generales, cómo ha evolucionado la computación hasta llegar a su versión cuántica y posteriormente algunos elementos básicos que se utilizan en esta nueva tecnología.

2. En seguida, se verán cuáles son los elementos necesarios para crear una computadora cuántica. Aunque no se ha concretado mucho, ya se tiene una serie de condiciones que se deben cumplir para considerársele así.

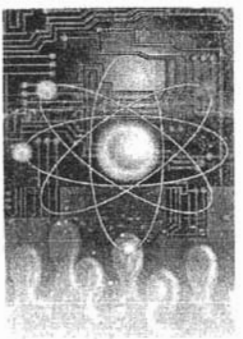
3. Con base en lo anterior, se señalará cuáles son los algoritmos que hacen que la computación cuántica sea funcional, entre ellos veremos el Algoritmo de Shor y el de Grover, que demuestran, de una manera sencilla, todo lo que se puede realizar con ellos, así como, la criptografía y la búsqueda en las bases de datos.

4. Por consiguiente, se estudiarán las tendencias que existen en la computación, no sólo es computación cuántica, sino también en la computación celular y molecular, cuyas aplicaciones están básicamente en la medicina; con esta tecnología se podrán encontrar soluciones mediante simulaciones en enfermedades que hasta la fecha se consideran incurables.

5. Finalmente, se hablará de algunas aplicaciones que permitirán esclarecer qué es la computación cuántica así como sus adaptaciones en la tele transportación y la criptografía. Esta última es de sumo interés pues en la actualidad la información puede ser utilizada con fines contrarios a los intereses de los usuarios.



Capítulo 1



Conceptos generales

¿Por qué las cosas son como son y no de otra manera?
(Johannes Kepler)

A través de la historia el ser humano ha usado diversos materiales y utilizado múltiples mecanismos en el diseño, construcción y operación de máquinas que agilicen y automaticen la realización de cálculos y el procesamiento de información. La computadora para llegar a ser tal como la conocemos actualmente, ha pasado por un proceso de evolución iniciado hace aproximadamente 2500 años, algunos consideran que las computadoras no tiene más que unos cientos de años de evolución, y otros sostienen que es un fenómeno iniciado recientemente en el siglo pasado. Algunos hechos que han marcado hitos importantes en este proceso son descritos a continuación.

Antiguamente, los primeros modelos fueron manuales, estos se remontan aproximadamente hasta 500 A.C., cuando los egipcios inventaron un artefacto que consistía en una serie de esferas atravesadas por varillas; este artefacto fue cambiado y perfeccionado por los chinos; y posteriormente en el siglo XIII D.C. es cuando toma la forma clásica que conocemos; el ÁBACO está compuesto por 10 líneas con 7 esferas cada una, una línea corta todas las líneas en dos partes una más grande que la otra, ubicándose 2 esferas en la parte superior y cinco en la parte inferior.

Mucho tiempo después, se desarrollaron modelos mecánicos y eléctricos, es así que, Blaise Pascal, en 1649, fabricó la PASCALINA, una máquina que hacía operaciones de 8 dígitos. En 1820, Charles Babbage con la ayuda de la Condesa Ada Byron, construyó dos equipos totalmente mecánicos, usaban ejes, engranajes y poleas para

realizar cálculos; Byron fue la primera persona que programó una computadora, tiempo después un lenguaje de programación fue nombrado como Ada en su honor. Herman Hollerith desarrolló unas máquinas que clasificaban, ordenaban y enumeraban tarjetas perforadas. Estas se usaron en el censo realizado en 1890 por el gobierno de los Estados Unidos de Norte América. Konraz Suze, ingeniero alemán, en 1942, construyó la primera computadora digital (electromecánica binaria) programable.

Entre 1937 y 1942 Atanasoff y Berry, construyeron un prototipo compuesto de tubos al vacío, capacitores y un tambor de rotatorio para el manejo de los elementos de la memoria, fue usada para resolver ecuaciones matemáticas complejas. En 1941 Turing construyó la COLLOSUS, una computadora que usaba miles de válvulas, 2400 bombas de vidrio al vacío, y un escáner con capacidad de leer 5000 caracteres por cinta de papel.

En 1944 IBM (International Business Machines) construye la MARK I en cooperación con la Universidad de Harvard, media 15 metros de largo, 2.40 metros de altura y pesaba cinco toneladas. La ENIAC contaba con 17,468 tubos de vidrio al vacío similares a los tubos de radio, fue construida en 1946 en la Universidad de Pensylvania.

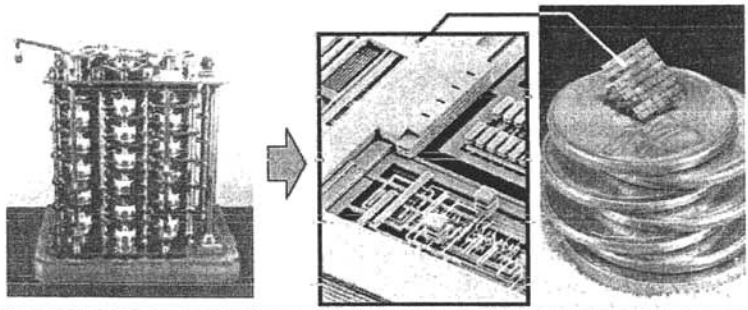


Figura 1.- Desde el principio hasta el presente: A la izquierda una máquina de engranajes, a la derecha un chip de la IBM de 0.25 micras. La versión producida por la IBM contiene 6 millones de transistores.

Finalmente se inició la era digital, con modelos electrónicos basados inicialmente en tubos de vacío y luego en transistores. La EDVAC fue la primera computadora electrónica digital, su memoria consistía en líneas de mercurio dentro de un tubo de vidrio al vacío, donde se podía almacenar ceros y unos. El transistor, es el invento que más ha influenciado en la evolución de las computadoras, este fue concebido en 1948, por tres científicos en los laboratorios de Bell, este contiene un material semiconductor que funciona como un interruptor. En 1958 Kilby y Noycea, de la Texas Instrument, inventaron los circuitos integrados, haciendo que las computadoras fuesen cada vez más pequeñas. En Intel, en 1971, Hoff desarrollo un microprocesador de 4 bits que contenía 23,000 transistores que procesaban 108 kHz o 0.06 MIPS[1], tenía 46 instrucciones y 4 kilobytes de espacio de almacenamiento. En 1974 Intel presentó una CPU compuesto por el microchip 8080, este contenía 4500 transistores y podía almacenar 64 kilobytes de memoria RAM, tenía un bus de datos de 8 bits. Wozniak y Jobs, en 1976, empiezan con Apple, revolucionando el mundo de las computadoras al introducir la interfaz gráfica y el ratón. El microprocesador

[1] MIPS: Millones de instrucciones por segundo

Intel 8086, se lanzó en 1978, e inició una nueva era en la producción de computadoras personales. A comienzos de la década de los 80 IBM empezó a desarrollar las computadoras personales con PC-DOS como sistema operativo, empezando así una nueva era, donde las computadoras estaban al alcance de todos. Las computadoras portátiles, las computadoras de escritorio, y los modelos no comerciales que son tan pequeños como una moneda de un centavo.

La constante miniaturización de los componentes de hardware ha logrado la realización de nano-circuitos. Pronto no será posible reducir más los circuitos, debido a que proximamente la miniaturización será tal que las leyes de la física clásica ya no sean validas, entonces se entrará en los dominios del mundo subatómico, donde las leyes de la física de la mecánica cuántica tienen validez. El cambio en los componentes fundamentales de las computadoras, hace necesario redefinir muchos elementos de la computación actual, la arquitectura, los algoritmos, y los componentes de hardware. Es así como nace la computación cuántica y con ella los algoritmos cuánticos.

La aplicabilidad de la computación cuántica depende de la posibilidad de desarrollar una computadora cuántica. Un ejemplo del inmenso poder de las computadoras cuánticas es el algoritmo cuántico para determinar si un número es primo. Una computadora actual se tardaría miles y hasta millones de años (dependiendo de cuan grande sea el número a factorizar) en ejecutar tal algoritmo; a diferencia de una

computadora cuántica le tomaría tan solo unos cuantos segundos el completar la tarea.

El incremento del poder de las computadoras se debe esencialmente a la miniaturización incesante del componente más elemental de la computadora, el transistor. Cuando los transistores se reducen de tamaño y se logran integrar en un solo microchip se incrementa el poder computacional. Sin embargo, las técnicas de integración de microcircuitos están empezando a tropezar con sus límites.

Mediante técnicas litográficas avanzadas podrían producirse elementos cien veces menores que los hoy disponibles. Pero a tal escala, en la que la materia se presenta como una muchedumbre de átomos disgregados, los circuitos integrados apenas consiguen funcionar. Al reducir la escala diez veces más, los átomos manifiestan ya su identidad individual, y basta un solo defecto para provocar una catástrofe. Por consiguiente, si se pretende que las computadoras del futuro reduzcan su tamaño, será preciso que la técnica de uso se reemplacé o complemente con otras nuevas.

La ciencia de la computación en busca de una alternativa más allá de la tecnología del transistor, ha iniciado el estudio de la mecánica cuántica y su aporte para la creación de nuevas computadoras. Es así como han surgido las disciplinas: Nano-Computación y Computación Mecánico-Cuántica.

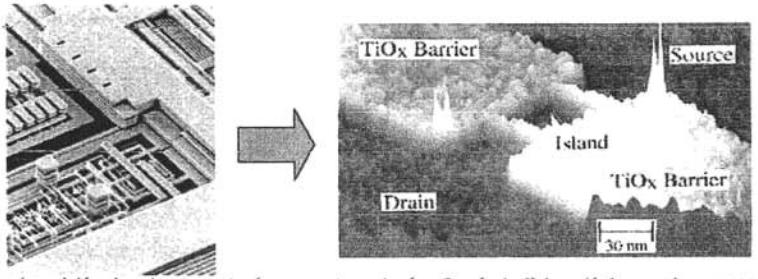


Figura 2.- La transición de microtecnología a nanotencología. Según la física clásica, no hay manera de que los electrones puedan llegar desde el "Source" al "Drain" debido a las dos barreras que se encuentran al lado del "Island" pero la estructura es tan pequeña que los efectos de la cuántica ocurren, y los electrones pueden bajo ciertas circunstancias romper la barrera del túnel.

Como se muestra en la Figura 2, hay formas de rediseñar los transistores para que trabajen usando efectos cuánticos. Pero podría ser mejor dejar la idea de transistores y usar una nueva arquitectura completamente nueva que sea más adecuada al utilizar los principios de la mecánica cuántica. En la Figura 3, se presenta una idea de esta arquitectura.

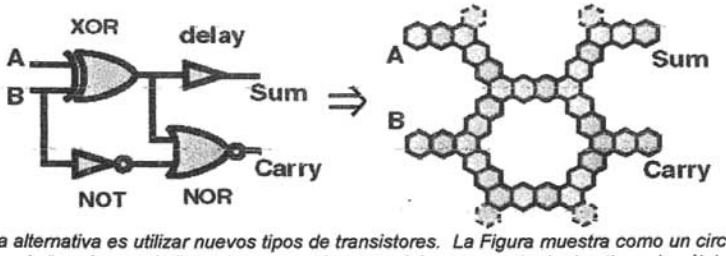


Figura 3.- Una alternativa es utilizar nuevos tipos de transistores. La Figura muestra como un circuito particular llamado "semi-sumador" puede crearse de un modelo compuesto de dos tipos de células.

Las nano-computadoras tendrán componentes cuyo funcionamiento se rigen por los principios de la mecánica cuántica, pero los algoritmos que ellas ejecuten probablemente no involucren un comportamiento cuántico; mientras que las computadoras cuánticas buscan una posibilidad más excitante, usar la mecánica

cuántica en un nuevo tipo de algoritmo que sería fundamentalmente más poderoso que cualquier otro esquema clásico. Una computadora que puede ejecutar este tipo de algoritmo será una verdadera computadora cuántica.

Una computadora cuántica es un nuevo dispositivo fantástico que puede resolver ciertos problemas importantes muy eficazmente. Una computadora cuántica proporciona paralelismo masivo aprovechando la naturaleza exponencial de la mecánica cuántica. Una computadora cuántica puede almacenar una cantidad exponencial de datos, y realizar un número exponencial de operaciones usando recursos polinomiales. Este paralelismo cuántico no es fácil de aprovechar. Sin embargo, unos algoritmos cuánticos descubiertos en 1993 (Algoritmo de Shor) han creado un interés en el potencial de las computadoras cuánticas.

La construcción de una computadora cuántica funcional a opuesto una resistencia fuera de lo común. El problema estriba en que cualquier interacción que un sistema cuántico tenga con su entorno, piénsese en el choque de un átomo contra otro o contra un fotón errante, constituye una medición. La superposición de estados mecánicos cuánticos se resuelve en un solo estado bien definido; y éste es el que el observador detecta.

Dicho fenómeno de decoherencia[2], así se llama, imposibilita cualquier cálculo cuántico. Al objeto de mantener, pues, la coherencia, las operaciones internas de una computadora cuántica deben separarse de su entorno. Más, a la vez, han de ser accesibles para que puedan cargarse, ejecutarse y leerse los cálculos.

Pese a todo, no será fácil conseguir una computadora cuántica cuyas proporciones le permitan competir con los más rápidos de los clásicos. Pero el reto merece la pena. Las computadoras cuánticas, por modestas que sean, se convertirán en soberbios laboratorios naturales donde poder estudiar la mecánica cuántica. Con semejantes dispositivos y la ejecución de un programa adecuado, podrán abordarse otros sistemas cuánticos que revisten interés fundamental.

Por ironía de las cosas, las computadoras cuánticas podrían ayudar a científicos e ingenieros en la resolución de los problemas que se les plantean en la creación de microcircuitos mínimos con transistores mínimos; muestran éstos un comportamiento mecánico cuántico cuando la reducción de su tamaño llega al límite de las posibilidades.

Cuando teóricos tales como Richard Feynmann, del California Institute of Technology, de Pasadena (California); Paul Benioff, de Argonne National Laboratory,

[2] La decoherencia es la consecuencia inevitable del enredo incontrolable que tienen todos los sistemas físicos con su ambiente. El enredo quiere decir que la realidad no puede estar localizada en el espacio y en el tiempo. Este enredo ha sido confirmado experimentalmente por Aspect y otros como "el no lugar cuántico". Este "no lugar cuántico" es el que permite hablar de teletransportación cuántica, de computadoras cuánticas y de otras consecuencias predichas por la teoría cuántica. En este enredo incontrolable, los estados coherentes típicos de la teoría cuántica son no locales, por lo que no pueden ser observados por un observador. A esta falta de coherencia de los estados cuánticos se llama decoherencia.

en Illinois; David Deutsch, de la Universidad de Oxford, en Inglaterra, y Charles Bennett, del T.J. Watson Research Center de IBM en Yorktown Heights (Nueva York), propusieron por primera vez el concepto de las computadoras cuánticas en las décadas de 1970 y 1980, muchos científicos dudaron que alguna vez ese tipo de computadora pudiera resultar práctica. Pero en 1994, Peter Shor, de AT&T Research, describió un algoritmo cuántico específicamente diseñado para factorizar números grandes y exponencialmente más rápido que las computadoras convencionales, lo suficientemente rápido como para quitar la seguridad de muchos criptosistemas de clave pública. El potencial del algoritmo de Shor alentó a muchos científicos a tratar de explotar las capacidades de las computadoras cuánticas. En los últimos años, varios grupos de investigación de todo el mundo han alcanzado progresos significativos en este campo.

Mientras estuvo en IBM, Chuang amplió su reputación como uno de los experimentalistas en computación cuántica más importantes del mundo. Dirigió el grupo que demostró la primera computadora cuántica de 1 qubit (en 1998 en la Universidad de California en Berkeley). En IBM Almaden, Chuang y sus colegas fueron los primeros en demostrar los importantes algoritmos cuánticos, el algoritmo de Grover concebido en 1999 para hacer búsquedas en bases de datos con ayuda de una computadora cuántica de 3 qubits, y la búsqueda de pedidos ideada en agosto del 2000, con una computadora cuántica de 5 qubits. La factorización con el algoritmo de Shor anunciada hoy es el algoritmo más complejo que se haya demostrado hasta ahora usando una computadora cuántica.

Además de su ambicioso programa experimental, la División de Investigación de IBM Research es conocida también por sus muchas contribuciones teóricas en el emergente campo de la información cuántica. Los científicos de IBM fueron pioneros en criptografía cuántica, en comunicaciones cuánticas (incluso el concepto de teleporte cuántico) y en metodologías eficientes para corregir errores. David DiVincenzo, miembro del cuerpo de investigadores del laboratorio Watson de IBM, ha promulgado los cinco criterios necesarios para construir una computadora cuántica práctica:

1. Un sistema físico de escala flexible con qubits bien caracterizados;
2. Capacidad de inicializar el estado de un qubit;
3. Tiempos de decoherencia más largos que el tiempo de operación de la puerta cuántica;
4. Un conjunto universal de puertas cuánticas; y
5. La capacidad de medir qubits específicos.

La comunidad científica dedicada a investigar tópicos en el ámbito de la computación cuántica, ha logrado enormes avances teóricos, al demostrar que es posible reducir drásticamente los recursos computacionales requeridos en la ejecución de algoritmos. Algunos de esos algoritmos requieren un inmenso poder de cómputo aún en las computadoras más avanzadas de la actualidad. Algunos algoritmos matemáticos como la búsqueda de los números primos enteros, algoritmos de manejo de información como la búsqueda en bases de datos no ordenadas; han

sido teóricamente desarrollados con mucho éxito, utilizando los fundamentos de la computación cuántica.

La teoría de la computación cuántica esta basada en las interacciones del mundo atómico y en futuras implementaciones de las computadoras cuánticas. Estas aún están en los laboratorios de investigación pero ya se tienen resultados alentadores, como el desarrollo de la computadora cuántica de cinco qubits desarrollado por Steffen.

La computación cuántica esta basada en las propiedades de la interacción cuántica entre las partículas subatómicas, como la superposición simultanea de dos estados en una sola partícula subatómica. La superposición cuántica, propiedad fundamental de la interacción cuántica, es ampliamente aprovechada para el desarrollo teórico de los algoritmos cuánticos, logrando una capacidad de procesamiento exponencial.

La superposición cuántica permite mantener simultáneamente múltiples estados en un bit cuántico, es decir "0" y "1" a la vez; a diferencia del bit – elemento fundamental en la computación actual – que únicamente es capaz de mantener un estado discreto, alternativo, a la vez, el "0" o "1" lógico. La computación cuántica, aprovecha la superposición cuántica, para lograr el paralelismo cuántico y el paralelismo cuántico masivo.

Cualquier interacción con el mundo subatómico, producirá un cambio en este, es decir, cualquier medición o lectura traerá indefectiblemente un cambio. Este fenómeno cuántico es aprovechado en la tele-transportación cuántica para la transmisión de qubits, y asimismo es utilizada como mecanismo de seguridad en la criptografía cuántica.

Sin embargo la progresiva miniaturización de los chips de las computadoras se está acercando al límite de las leyes físicas clásicas. La computación actual busca nuevos caminos, y la computación cuántica se presenta como una alternativa diferente y revolucionaria.

Desde su programación hasta sus soportes, pasando por su arquitectura, sus algoritmos y sus unidades de información, este incipiente campo científico comienza a vislumbrar el futuro de la informática, faltando para ello mucho tiempo y trabajo.

La potencia de las computadoras cuánticas es una buena razón para seguir investigando: una computadora de este tipo podría realizar algunas tareas millones de veces más rápido que las "supercomputadoras" actuales.

En 1965, Gordon Moore, cofundador de Intel y uno de los gurús de la tecnología de la información, hizo una predicción que se vio confirmada con bastante precisión: en las décadas siguientes la potencia de las computadoras se duplicaría cada 18 meses. Este incremento se ha debido sobre todo a la miniaturización progresiva de

los componentes electrónicos, pero las leyes físicas clásicas tienen una frontera: el mundo subatómico.

En unos años, los nanocircuitos actuales no podrán continuar disminuyendo de tamaño porque entrarían en los dominios de las partículas subatómicas, donde rigen las leyes de la física de la mecánica cuántica. Entonces podría comenzar la era de la computación cuántica, pero es mucho más complejo de lo que parece, porque para ello habrá que redefinir muchos elementos de la computación actual, como su arquitectura, sus algoritmos o los elementos de hardware, por citar algunos ejemplos. Puede ser cuestión de años, de décadas o de siglos.

CONCEPTO DE COMPUTACIÓN CUÁNTICA

La computación cuántica se desarrolla en la física cuántica obteniendo partido de algunas propiedades físicas de los átomos o de los núcleos que permiten trabjar conjuntamente con bits cuánticos (en el procesador y en la memoría de la computadora). Interactuando unos con otros estando aislados de un ambiente externo los bits cuánticos pueden ejecutar cálculos exponenciales mucho más rápido que las computadoras convencionales.

Mientras que las computadoras tradicionales codifican información usando números binarios (0, 1) y pueden hacer solo cálculos de un conjunto de números de una sola vez cada uno, las computadoras cuánticas codifcan información como serie de

estados mecánicos cuánticos tales como direcciones de los electrones o las orientaciones de la polarización de un fotón representando un número que expresaba que el estado del bit cuántico está en alguna parte entre 1 y 0, o una superposición de muchos diversos números de forma que se realizan diversos cálculos simultáneamente.

En las computadoras cuánticas su comportamiento es determinado de forma importante por leyes de la mecánica cuántica. El sistema descrito está formado por bits cuánticos (quantum bits) o qubits, y pueden ser por ejemplo: núcleos, puntos cuánticos semiconductores y similares.

FUNDAMENTOS DE LA COMPUTACIÓN CUÁNTICA

Este, es un los puntos que ofrecen una gama de prestaciones enormes; imaginarse que los dispositivos de almacenamiento más avanzados hasta ahora se duplicaran, suena bastante interesante, pues los qubits pueden representar cuatro números a la vez, siendo que la lógica binaria sólo permite un 1 ó un 0 para un solo bit. Esto definitivamente implica una duplicación por así decirlo de la capacidad de procesamiento no sólo de las memorias o dispositivos de almacenamiento secundario; sino además en todos los demás componentes de un sistema informático como pueden ser: microprocesadores, tarjetas de video, de sonido, etc.

Además, lógicamente estos descubrimientos aumentarían notablemente la velocidad de los micros y de todos sus demás componentes.

En la computación tradicional, un bit es la mínima unidad de información pero, para representarlo, se utiliza la ausencia o la presencia de miles de millones de electrones en un diminuto transistor de silicio

La computación cuántica pretende utilizar un principio básico de la mecánica cuántica por el cual todas las partículas subatómicas (protones, neutrones, electrones, etc.) tienen una propiedad asociada llamada spin[3]. El spin se asocia con el movimiento de rotación de la partícula alrededor de un eje. Esta rotación puede ser realizada en un sentido, o el opuesto. Si por ejemplo tomamos como bit al spin de un protón, podemos usar una dirección como 1 y otra como 0. Estos bits, tomados a partir del spin de las partículas han recibido el nombre de qubits.

Sin embargo, en mecánica cuántica el estado de una partícula se determina a través de la asignación de una probabilidad, no podemos hablar de un estado 1 ó 0 claramente determinado. Esta aparente ambigüedad tiene una ventaja que convierte a la computación cuántica en un desarrollo revolucionario: La lógica de un bit es uno u otro, mientras que un qubit (nombre dado al bit cuántico) entraña el concepto ambos a la vez. Si tomamos por ejemplo dos bits, sus estados posibles son cuatro:

[3] El spin es el momento angular intrínseco de una partícula subatómica. El spin es una propiedad fundamental de todas las partículas elementales, y existe incluso aunque la partícula no se mueva; el momento angular orbital se debe al movimiento de la partícula.

00, 01, 10, 11. Son necesarios cuatro pares de bits para representar la misma información que un solo par de qubits con comportamiento ambiguo.

Los qubits pueden representar en este caso cuatro números a la vez, cuatro respuestas posibles a la vez. Procesamiento paralelo real, algo no tan importante de la computación. Sus aplicaciones principales entran en el campo de la criptografía y teoría de numeros, y en el análisis de gigantescos volúmenes de información.

No todos los problemas pueden ser resueltos por este tipo de lógica. Sin embargo, una computadora cuántica podría resolver los que sí pueden, a una velocidad varias veces superior a la de los microprocesadores conocidos hasta hoy, esta también se considera una tecnología hipotética, pues aún sólo se ha quedado en la investigación sin llegar a desarrollar un sistema completo utilizando esta lógica, pero aún así, si se logra implantar algún día será definitivamente demasiado cara debido a las características necesarias para su buen funcionamiento.

Señalan en la Universidad de Michigan que se esta a punto de entrar a la nueva era de la computación puesto que se elevará la velocidad en el procesamiento de la información de manera sorprendente ¿cómo?, bueno indican que mediante la utilización de circuitos que combinan la mecánica cuántica con los principios de la computación.

Señalan los investigadores que las nuevas computadoras realizaran los cálculos más complejos en mucho menor tiempo. En un artículo publicado en Physical Review Letters, se realiza una propuesta de un circuito realizable de forma experimental contemplando de esta manera una forma de implementar una computación cuántica escalable.

Se cree que esta tecnología proporcionará sistemas en los que participarán muchos qubits, lo que hará posible construir una computadora cuántica. Bajo esta linea se ha escrito en la Universidad de Michigan el artículo titulado "Scalable quantum computing with Josephson charge qubits". La información se procesará mediante átomos individuales o partículas subatómicas llamadas qubits. Pero la tarea no resulta nada sencilla puesto que para poder utilizar esta tecnología será estrictamente necesario manipular, preparar y medir el frágil estado cuántico de un sistema. Asimismo dentro de las mayores dificultades que se presentan son que es necesario manejar muchos qubits, y controlar la conectividad entre ellos.

La computación cuántica esta basada en las propiedades de la interacción cuántica entre las partículas subatómicas, como la superposición simultanea de dos estados en una sola partícula subatómica. La superposición cuántica, propiedad fundamental de la interacción cuántica, es ampliamente aprovechada para el desarrollo teórico de los algoritmos cuánticos, logrando una capacidad de procesamiento exponencial.

La superposición cuántica permite mantener simultáneamente múltiples estados en un bit cuántico, es decir "0" y "1" a la vez; a diferencia del bit – elemento fundamental en la computación actual – que únicamente es capaz de mantener un estado discreto, alternativo, a la vez, el "0" o "1" lógico. La computación cuántica, aprovecha la superposición cuántica, para lograr el paralelismo cuántico y el paralelismo cuántico masivo.

Cualquier interacción con el mundo subatómico, producirá un cambio en este, es decir, cualquier medición o lectura traerá indefectiblemente un cambio. Este fenómeno cuántico es aprovechado en la tele transportación cuántica para la transmisión de qubits, y asimismo es utilizada como mecanismo de seguridad en la criptografía cuántica.

ELEMENTOS BÁSICOS DE LA COMPUTACIÓN CUÁNTICA

- **Bit cuántico**

El elemento básico de la computación cuántica es el bit cuántico o qubit [4] (quantum bit por sus siglas en inglés), un qubit representa ambos estados simultáneamente, un "0" y un "1" lógico, dos estados ortogonales de una sub partícula atómica, como es representada en la figura 4. El estado de un qubit se puede escribir como $\{|0\rangle, |1\rangle\}$, describiendo su múltiple estado simultaneo.

[4] "qubit" término acuñado por Schumacher en 1995.

Un vector de dos qubits, representa simultáneamente, los estados 00, 01, 10 y 11; un vector de tres qubits, representa simultáneamente, los estados 000, 001, 010, 011, 100, 101, 110, y 111; y así sucesivamente. Es decir un vector de n qubits, representa a la vez 2^n estados.

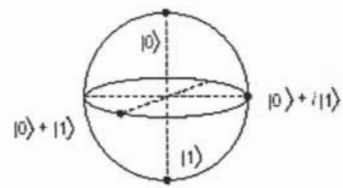


Figura 4. *Representación de cuatro estados diferentes de un qubit.*

Cualquier sistema cuántico con dos estados discretos distintos puede servir como qubit, un espín de electrón que apunta arriba o abajo, o un espín de fotón con polarización horizontal o vertical. En la figura 4 se tiene una representación pictórica de cuatro diferentes estados basado en el espín de un núcleo atómico, por lo que puede ser usado como un qubit. Un qubit no puede ser clonado, no puede ser copiado, y no puede ser enviado de un lugar a otro.

Resumiendo el bit (Binary Digit) es la unidad de información más pequeña manipulada por los computadoras actuales. Adquiere el valor de un 0 o un 1 para el procesamiento y almacenamiento de datos, y puede materializarse en algo tan simple como que un condensador esté cargado o descargado.

Una agrupación de ocho bits (byte) ya permite representar todo tipo de información, como las letras del alfabeto y los dígitos del 0 al 9. Extrapolar este sistema a la computación cuántica presenta las primeras dificultades. "Un átomo simple no se comporta como un bit clásico. Puede estar tanto en 0 como en 1 como en los dos estados a la vez: es el qubit (Quantum Bit)".

"En un solo qubit - continúa el físico - se podría almacenar una cantidad ilimitada de información, jugando con los coeficientes de la superposición cuántica de los estados 0 y 1". Esta manifestación del principio de superposición cuántica potenciaría la capacidad de computación hasta límites abrumadores. Y es más, teóricamente sería posible preparar las partículas para registrar los infinitos estados existentes entre el 0 y el 1. Las desorbitadas posibilidades que ofrecería una computadora de este tipo se potenciarían aún más por un extraño fenómeno cuántico: el entrelazamiento.

La intuición humana, acostumbrada al mundo clásico, conduce a confusiones en el mundo cuántico, y el entrelazamiento (entanglement, en inglés) es un claro ejemplo de ello. Esta propiedad implica correlaciones entre sistemas cuánticos que no tienen un análogo clásico y que dificultan su comprensión. "Si tu y yo compartimos un par de partículas - o qubits - que hemos manipulado para dejarlas en un estado entrelazado, y cada uno nos llevamos una separándolas tanto cuanto queramos, cuando las observemos encontraremos que están todavía relacionadas de alguna manera".

Es como si acuñamos dos monedas y las llevamos a distintos países: estén a la distancia que estén, si las tiramos al aire las dos darán siempre el mismo resultado, ya sea sol o aguila. Esta propiedad permite poner a trabajar a los qubits como un enorme conjunto de computadoras en paralelo, aumentando su capacidad de almacenamiento y procesamiento de información a niveles extraordinarios. "Una computadora cuántica que actuase sobre unos cientos de átomos podría realizar simultáneamente más computaciones que el número de átomos presentes en el universo visible".

- **Compuertas lógicas**

Las compuertas lógicas son operaciones unarias sobre qubits. La compuerta puede ser escrita como $P(\theta)=|0\rangle\langle 0| + \exp(i\theta) + |1\rangle\langle 1|$, donde $\theta = \omega t$. Aquí algunas compuertas cuánticas elementales:

$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ = identidad

$X \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$ = NOT

$Z \equiv P(\pi)$

$Y \equiv XZ$

$H \equiv \frac{1}{\sqrt{2}}\left[(|0\rangle+|1\rangle)\langle 0| + (|0\rangle-|1\rangle)\langle 1|\right]$

Donde I es la identidad, X es el análogo al clásico NOT, Z cambia el signo a la amplitud, y H es la transformación de Hadamard.

Estas compuertas forman uno de los más pequeños grupos de la computación cuántica. La tecnología de la física cuántica puede implementar esas compuertas eficientemente. Todos excepto el CNOT operan en un simple qubit; la compuerta CNOT opera en dos qubits.

Una compuerta de dos qubits en especial interesante, es la conocida como "U controlada",

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

Son operadores actuando sobre dos qubits, donde I es la operación de identidad sobre un qubit, y U es cualquier otra compuerta sobre un qubit. El estado del qubit U es controlado mediante el estado del qubit I. Por ejemplo el NOT controlado (CNOT) es: $|00\rangle \rightarrow |00\rangle$; $|01\rangle \rightarrow |01\rangle$; $|10\rangle \rightarrow |11\rangle$; $|11\rangle \rightarrow |10\rangle$

- **"Entanglement"**

La capacidad computacional de procesamiento paralelo de la computación cuántica, es enormemente incrementada por el procesamiento masivamente en paralelo,

debido a una interacción que ocurre durante algunas millonésimas de segundo. Este fenómeno de la mecánica cuántica es llamado "entanglement".

Debido al "entanglement", dos partículas subatómicas, permanecen indefectiblemente relacionadas entre si, si han sido generadas en un mismo proceso. Por ejemplo la desintegración en un protón y un electrón. Estas partículas forman subsistemas que no pueden describirse separadamente. Cuando una de las dos partículas sufre un cambio de estado, repercute en la otra. Esta característica se desencadena cuando se realiza una medición sobre una de las partículas.

- **Tele transportación cuántica**

La tele transportación cuántica es descrita por Stean como la posibilidad de "transmitir qubits sin enviar qubits". En la computación tradicional para transmitir bits, estos son clonados o copiados y luego enviados a través de diferentes medios como el cobre, fibra óptica, ondas de radio y otros. En la computación cuántica no es posible clonar, tampoco copiar, y mucho menos enviar qubits de un lugar a otro como se hacen con los bits.

Si enviamos un qubit $|\varnothing\rangle$ donde $\varnothing$ es un estado desconocido, el receptor no podrá leer su estado con certidumbre, cualquier intento de medida podría modificar el estado del qubit, por lo tanto se perdería su estado, imposibilitando su recuperación. La tele transportación cuántica, resuelve este problema, esta se basa en el

"entanglement" para poder transmitir un qubit sin necesidad de enviarlo. El emisor y el receptor poseen un par de qubits "enredados" (entangled). Entonces el qubit es transmitido desde el emisor, desaparece del emisor y el receptor tiene el qubit tele transportado.

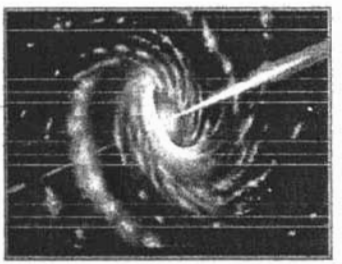


Figura 5. Fenómeno de teletransportación.

Este fenómeno es posible debido a un mecanismo conocido como el efecto EPR[5]. En la tele transportación cuántica primero dos qubits E y R son "enredados" y luego separados (entangled), el qubit R es ubicado en el receptor y el qubit E es ubicado en el emisor junto al qubit original Q a ser transmitido, al realizar la lectura del estado de los dos qubits Q y E, estos cambian su estado a uno aleatorio debido a la interacción. La información leída es enviada al receptor, donde esta información es utilizada para un tratamiento que es aplicado al qubit R, siendo ahora R una réplica exacta del qubit Q.

[5] La "correlación de Einstein-Podolsky-Rosen (EPR)" o "entanglement", ha sido al menos en parte conocido desde los 1930s cuando fue discutido en un famoso paper por Albert Einsten, Boris Podolsky, y Nathan Rosen.

- **Paralelismo cuántico**

La superposición cuántica permite un paralelismo exponencial o paralelismo cuántico en el cálculo, mediante el uso de las compuertas lógicas de qubits. Los qubits, a diferencia de los bits, pueden existir en un estado de superposición, representado por $a|0\rangle + b|1\rangle$, donde a y b son números complejos que satisfacen la relación $|a|^2 + |b|^2 = 1$

Dado a una compuerta lógica de un qubit f, transforma el estado $|a|$ en el estado $|f(x)|$, cuando el qubit de entrada tiene en el estado

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

una superposición igual de $|0\rangle$ y $|1\rangle$.

Por linealidad[6] de la mecánica cuántica, la compuerta lógica f transforma el estado del qubit a

$$\frac{1}{\sqrt{2}}|f(0)\rangle + \frac{1}{\sqrt{2}}|f(1)\rangle$$

[6] La linealidad de la mecánica cuántica, se refiere al principio de correspondencia, donde a cada observable de la mecanica clásica le corresponde un operador lineal en mecánica cuántica. Ademas, este deber ser hermético, es decir: $F(a\varphi_1 + b\varphi_2) = aF\varphi_1 + bF\varphi_2$

El estado resultante es la superposición de los 2 valores de salida, siendo f evaluado para los 2 valores de entrada en paralelo. Para una compuerta lógica g de 2 qubits, que tienen dos qubits de entrada en superposición de $|0\rangle$ y $|1\rangle$, tendríamos una superposición de 4 estados

$$c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

La compuerta lógica g transforma el estado de entrada a

$$c_0|g(00)\rangle + c_1|g(01)\rangle + c_2|g(10)\rangle + c_3|g(11)\rangle$$

así g es evaluado en un solo paso para 4 valores de entrada.

En una compuerta lógica h de 3 qubits, se tienen 3 qubits de entrada en superposición de $|0\rangle$ y $|1\rangle$, juntos hacen una superposición de 8 estados, que son evaluados en paralelo. Por cada qubits adicional la cantidad de estados se duplica.

- **Criptografía cuántica**

Criptografía, es la ciencia matemática de las comunicaciones secretas, tiene una larga y distinguida historia de uso militar y diplomático que se remonta a los antiguos Griegos. Fue un elemento importante y decisivo durante la segunda guerra mundial. Hoy en día su uso es muy común y necesario, para brindar seguridad en las

transacciones comerciales, comunicaciones, y privacidad; que se llevan a cabo mediante Internet.

Dado M y f, donde M es un mensaje y f una función de encriptación, tenemos C = f(M), C entonces es el mensaje encriptado. C es enviado al receptor mediante un canal público, este obtiene el mensaje original con f^{-1}, haciendo M = $f^{-1}(C)$. Si f^{-1} es conocido y C es interceptado en el canal público, entonces se puede obtener M. La seguridad de f depende de la dificultad con que pueda obtenerse f^{-1}.

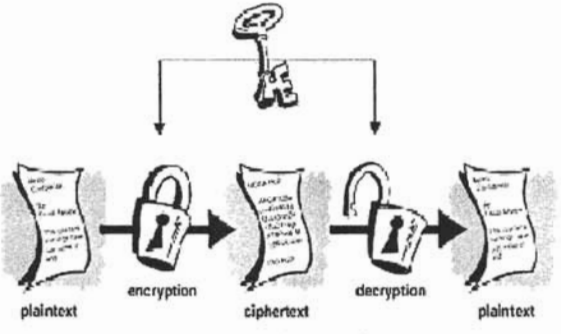


Figura 6. Criptografía

El factorizar es un aspecto muy importante en la criptografía moderna, debido a que, la seguridad del mecanismo de criptografía RSA de clave pública, se basa en la dificultad de factorizar número grandes. El mejor algoritmo para hallar los factores aún sigue siendo el de las divisiones sucesivas.

Dado M, R_1 y R_2, mediante el mecanismo de RSA se define una función p, tal que $C_1 = p(Q_1, P_1, M_1)$ y $C_2 = p(Q_2, P_2, M_2)$, donde P_1 y P_2 son claves públicas generadas en base a Q_1 y Q_2 que son claves privadas pertenecientes a A y B respectivamente.

A y B comparten sus respectivas claves públicas P_1 y P_2, y ambos pueden obtener y descifrar sus mensajes mediante p^{-1}, de tal modo que:

$$M_1 = p^{-1}(Q_1, P_1, M^1) \text{ y } M_2 = p^{-1}(Q_2, P_2, M_2)$$

El tiempo que requeriría el realizar la factorización se estima en aproximadamente $4x10^{16}$ años. Sin embargo en 1994 se logró desarrollar un algoritmo, usando recursos en redes, donde la factorización únicamente tomo 8 meses, el equivalente a 4,000 MIPS-años. Los algoritmos cuánticos de factorización, se estima que realizarían este cálculo en apenas unos segundos. El algoritmo cuántico de Peter Shor para factorizar números grandes, muestra el gran poder de las computadoras cuánticas.

Utilizando claves privadas, es posible – al menos en teoría – tener un algoritmo de encriptación imposible de romper. El emisor cada vez que envía un mensaje M, genera aleatoriamente una diferente clave privada P, mediante una función de encriptación E se codifica el mensaje de tal modo que C = E(P, M). El receptor necesita la clave privada P para poder realizar el proceso inverso $M = E^{-1}(P, C)$. Actualmente este mecanismo es utópico, debido a la gran dificultad que surge en la distribución de la clave privada P, debido a que necesita un canal muy seguro para su entrega.

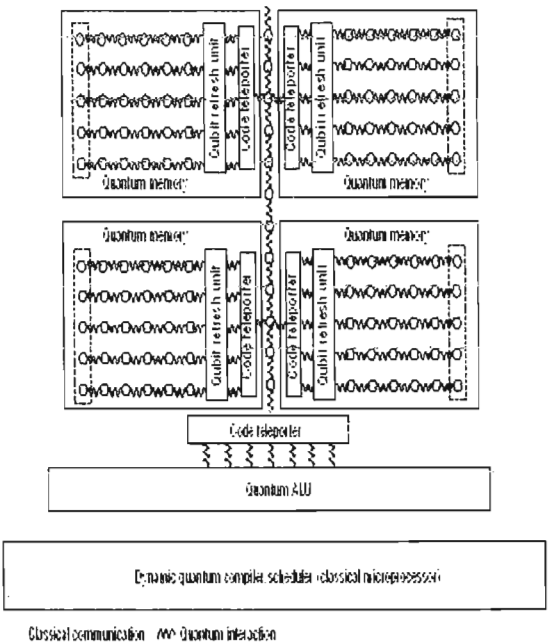
La criptografía cuántica hace posible la distribución de la clave privada P. P es transmitida mediante un canal cuántico. Cualquier intento de medir P será notado, debido a que es imposible observar un qubit sin dejar rastro.

RSA

Uno de los primeros esquemas de clave pública fue desarrollado por R. Rivest, A. Shamir y L. Adleman en el MIT. El esquema Rivest-Shamir-Adleman (RSA) ha sido desde la fecha de su publicación el único sistema ampliamente aceptado para la implementación de encriptación mediante clave pública. El principal inconveniente de este sistema es la existencia de una patente sobre este algoritmo, lo cual dificulta su uso fuera de los EE.UU. si no se ha obtenido la correspondiente licencia de exportación. El algoritmo estrella de encriptación asimetrica hoy es el RSA (por sus inventores Rivest, Shamir, Adleman) es a la vez el más sencillo, fácil de implementar y hasta el momento ha soportado todos los ataques conocidos cuando se usan claves lo suficientemente largas (por ejemplo 1024 bits o más). La mayor vulnerabilidad conocida del algoritmo RSA tiene que ver con el largo de las claves, el propio Shamir presentó en 1999 un método que ponía en peligro al RSA con claves de 512 bits o menos, hoy se considera "muy seguro" al RSA con claves de 1024 bits.

RSA es un cifrador de bloque, es decir crea bloques de longitud fija, si faltan datos para completar un bloque usualmente el faltante se rellena con ceros.

Capítulo 2



Principio Funcional (Estructura)

La ciencia será siempre una búsqueda, jamás un descubrimiento real. Es un viaje, nunca una llegada.
(Karl R. Popper)

Aún no se ha resuelto el problema de qué hardware sería el ideal para la computación cuántica. Se ha definido una serie de condiciones que debe cumplir, conocida como la *lista de Di Vinzenzo*, y hay varios candidatos actualmente, y para ello deben cumplir con las siguientes condiciones:

- El sistema ha de poder inicializarse, esto es, llevarse a un estado de partida conocido y controlado.

- Ha de ser posible hacer manipulaciones a los qubits de forma controlada, con un conjunto de operaciones que forme un conjunto universal de puertas lógicas (para poder reproducir a cualquier otra puerta lógica posible).

- El sistema ha de mantener su coherencia cuántica a lo largo del experimento.

- Ha de poder leerse el estado final del sistema, tras el cálculo.

- El sistema ha de ser escalable: tiene que haber una forma definida de aumentar el número de qubits, para tratar con problemas de mayor coste computacional.

Aunque no se conoce en su totalidad el hardware que pudiese utilizar una computadora cuántica, se tiene una idea de la arquitectura de una computadora

cuántica la cual es similar a la de las computadoras tradicionales, con ciertos elementos propios de la computación cuántica.

Oskin propone una arquitectura de una computadora cuántica que esta conformada por una ALU cuántica, memoria cuántica, y un planificador dinámico, tal como puede observarse en la figura 7.

La corrección de errores es un aspecto que debe ser tomado muy en cuenta en el diseño de una arquitectura cuántica.

ALU CUÁNTICA

La ALU cuántica tiene como funciones fundamentales la ejecución de operaciones cuánticas y la corrección de errores.

La ALU prepara los datos cuánticos, antes de ejecutar cualquier compuerta lógica, aplicando una secuencia de transformaciones cuánticas básicas, que incluyen:

- Hadamard (raiz cuadrada, transformada de Fourier de 1 qubit),
- I, Identidad (I, NOP cuántico),
- X, NOT cuántico,
- Z, (cambia los signos de las amplitudes),
- Y = XZ,

- rotación por $\pi/4$ (S),
- rotación por $\pi/8$ (T), y
- NOT controlado (CNOT).

La ALU aplica esta secuencia de operaciones elementales para la corrección de errores, indispensable en la computación cuántica. Este procedimiento consume estados auxiliares adicionales, para la verificación de paridad. La ALU hace uso de hardware especializado estándar, que provee estados elementales estándares, para producir los estados auxiliares adicionales.

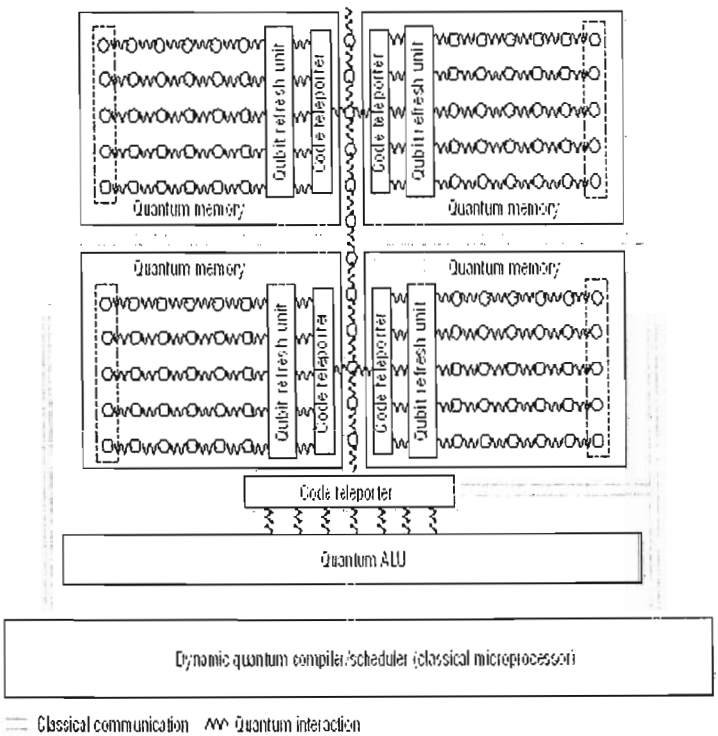


Figura 7. *Arquitectura cuántica.*

MEMORIA CUÁNTICA

Al igual que en las arquitecturas actuales en la arquitectura cuántica, la memoria cuántica es un elemento arquitectural muy importante. La memoria cuántica debe ser confiable, con el propósito de dotarla de tal característica Oskin incluye una unidad especializada de "actualización" en cada banco de memoria, cuya representación pictórica se puede apreciar en la figura 7. Una unidad especializada actualiza periódicamente los qubits lógicos individuales, ejecutando algoritmos de detección y corrección de errores.

TELE TRANSPORTADORA DE CÓDIGO

La tele transportadora de código desde la memoria cuántica a la ALU, añade alguna funcionalidad adicional a la tele transportación cuántica convencional, proveyendo un mecanismo general para simultáneamente ejecutar operaciones mientras transporta los datos cuánticos.

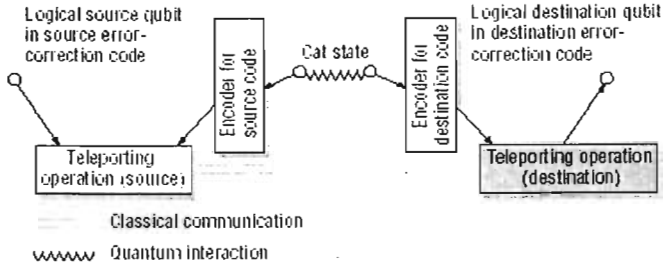


Figura 8. *Tele transportadora de código.*

Este mecanismo se usa para la corrección de errores en el codificador de código origen y en el codificador de código destino, como puede observarse en la figura 8. El emisor y el receptor entonces ejecutan qubits lógicos equivalentes en la operación de tele transportación en cada terminal del par "enredado" (entangled).

PLANIFICADOR DINÁMICO

Oskin proponen un procesador clásico de alto desempeño como parte principal del planificador dinámico. Este procesador ejecuta un algoritmo de planificación dinámico que toma operaciones cuánticas lógicas, intercaladas con construcciones clásicas de control de flujo, y dinámicamente las traduce en operaciones individuales de qubits físicos.

PROCESADOR

En 2004, científicos del Instituto de Física aplicada de la Universidad de Bonn publicaron resultados sobre un registro cuántico experimental. Para ello utilizaron átomos neutros que almacenan información cuántica, por lo que son llamados *qubits* por analogía con los bits. Su objetivo actual es construir una puerta cuántica, con lo cual se tendrían los elementos básicos que constituyen los procesadores, que son el corazón de los computadores actuales. Cabe destacar que un chip de tecnología

VLSI[7] contiene actualmente más de 100,000 puertas, de manera que su uso práctico todavía se presenta en un horizonte lejano.

TRANSMISIÓN DE DATOS

Científicos de los laboratorios Max Planck y Niels Bohr publicaron, en noviembre de 2004, en la revista Nature, resultados sobre la transmisión de información cuántica, usando la luz como vehículo, a distancias de 100 km. Los resultados dan niveles de éxito en las transmisiones de 70%, lo que representa un nivel de calidad que permite utilizar protocolos de transmisión con autocorrección.

Actualmente se trabaja en el diseño de repetidores, que permitirían transmitir información a distancias mayores a las ya alcanzadas.

En general una definición acerca de las computadoras cuánticas ampliamente aceptada por los investigadores, es la expuesta por Beth. El la concibe como un sistema de circuitos cuánticos, actuando en un espacio de estados, que es un espacio complejo 2n-dimensional de Hilbert. El circuito es una secuencia de transformaciones unitarias $U_t \in SU(2^n)$ seguido por una medición. Esas transformaciones, son llamadas compuertas cuánticas, y son controladas por una computadora clásica. El espacio de estados de una computadora cuántica tiene la

[7] Acrónimo inglés de Very Large Scale Integration, integración en escala muy grande. Se suele considerar que, a raíz de la VLSI, entramos en la cuarte generación de computadoras, en las que el corazón de una computadora (el microprocesador) está empaquetado en una sola pastilla

estructura de un espacio de un vector Hermitiano. Así esto permite la superposición simultanea de estados básicos ortogonales (correspondientes a estados clásicos "0" y "1") con la posibilidad de interferencia constructiva y destructiva entre las diferentes rutas de computación. Este principio permite el uso de los estados confusos (entangled states).

REQUERIMIENTOS DE IMPLEMENTACIÓN

Para la implementación de una computadora cuántica, se deben cumplir al menos cinco requisitos:

1. Se necesita un sistema de qubits.
2. Los qubits deben ser individualmente direccionables y deben interactuar con otros para conformar compuertas lógicas de propósito general.
3. Debe ser posible la inicialización de las compuertas.
4. Se debe tener la posibilidad de extraer los resultados computacionales.
5. Es la necesidad de un tiempo de coherencia duradero.

Las computadoras actuales están llegando al límite de la miniaturización y la frecuencia de pulsaciones de los relojes de cuarzo, pronto no podrán ser más rápidos. La computación cuántica es una gran promesa que podría permitirnos seguir construyendo computadoras más veloces. La arquitectura cuántica es muy similar a las arquitecturas actuales, sin embargo la computación cuántica introduce elementos

arquitecturales cuánticos que obedecen a los fenómenos causados por la interacción cuántica como la corrección de errores.

El avance de la computación cuántica esta limitada por sus principales ventajas. Con lo referente a la superposición cuántica, que permite el paralelismo masivo y mantener una gran cantidad de múltiples estados en un mismo instante, el mayor inconveniente esta en la imposibilidad de leer toda esa información sin desestabilizar el sistema.

Desde el punto de vista del hardware, en la parte física la meta es lograr diseñar dispositivos en sólidos, y no en gases como se da en la mayoría de los experimentos actualmente. En la parte lógica mantener la coherencia en un dispositivo cuántico es un desafío, principalmente debido a la gran cantidad de información adjunta que se necesita para garantizar la ausencia de errores, por lo que es necesario el desarrollo de mejores mecanismos de corrección de errores.

Prevenir la incoherencia y preservar los frágiles estados cuánticos. Esto es fácil en pequeños sistemas pero más complejo en grandes sistemas cuánticos.

En el futuro, se espera que las computadoras cuánticas, estén completamente desarrolladas aproximadamente el 2020. Otro sistema de encriptación cuántica es el desarrollado por Prem Kumar y Horace Yuen, profesores de la universidad

"Northwestern", capaz de codificar flujos de datos y enviarlos a velocidades de las troncales de Internet.

MODELO DEL CIRCUITO CUÁNTICO

El modelo de red es el más utilizado en computación convencional. Se basa, en la concatenación de etapas de puertas lógicas (no necesariamente binarias). Este modelo es fácilmente traducible a un mundo de puertas lógicas cuánticas, si bien no aporta nada nuevo sobre el modelo tradicional, y tropieza con muchas dificultades. La ventaja que tiene no es otra que el hecho de ser un modelo más maduro, y por tanto con más posibilidades de llevarse al laboratorio. El inconveniente consiste en que lo que hacemos es trasladar un diseño que surgió para sistemas clásicos al campo de los sistemas cuánticos, por lo que el modelo en sí no explota las particularidades de este dominio.

Aquí no debemos entender las puertas lógicas como en los circuitos electrónicos. En un circuito electrónico una puerta lógica era algún dispositivo físico que encuentra una señal eléctrica a su paso, y que es capaz de permitirle o no el paso en función de unas determinadas circunstancias.

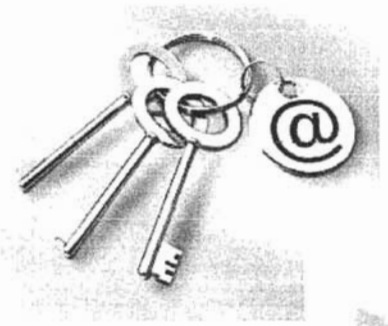
En una red cuántica, en cambio, las puertas lógicas no pueden realizarse de esta manera por varias razones. Entre otras cosas, no podemos clonar a voluntad un cierto estado, mientras que en un circuito electrónico esto es inmediato. Por otra

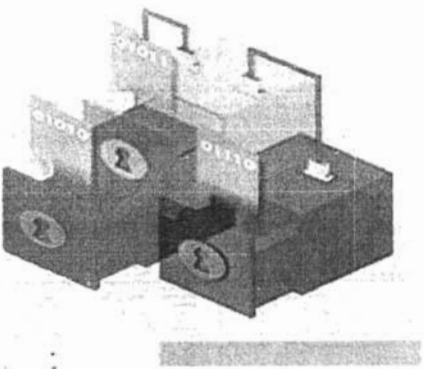
parte, la naturaleza de los qubits (habitualmente magnética) requiere que utilicemos por ejemplo campos magnéticos para manipularlos.

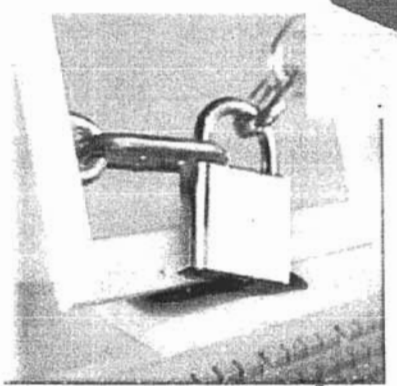
Podemos entonces preparar una especie de trayectoria que vaya recorriendo todo el sistema, esparcida de regiones donde producimos campos magnéticos durante tiempos tan cortos que podamos estar seguros de que sólo afectar a un qubit, y tan bien sincronizados que además sabremos a que qubit afectan. Deberíamos hacer tantos de estos dispositivos como etapas tenga la operación que hayamos previsto realizar.

Lo razonable es dejar fijos en el espacio, y operar sobre ellos con un único conjunto de actuadores que produzcan los respectivos campos magnéticos, o el efecto que queramos aprovechar para modificar el estado del arreglo. Si se tratará de campos magnéticos, obligando a los spinies a orientarse de determinada manera, no sería necesario que nos preocupáramos de si éstos están activos un poco más de tiempo de la cuenta, pues cada electrón acabaría en el mismo estado final. Así vemos que la idea de red en computación cuántica tiene muy poco que ver con la de la computación tradicional.

Capítulo 3







Algoritmos

La ciencia son hechos; de la misma manera que las casas están hechas de piedras, la ciencia está hecha de hechos; pero un montón de piedras no es una casa y una colección de hechos no es necesariamente ciencia.

(Henri Poincare)

Los físicos han comprobado el proceso que convierte en realidad los estados probabilísticos del mundo subatómico: la fricción con el entorno es lo que elimina las ondas de probabilidad, pero la conciencia del observador forma parte del proceso cuántico.

Fue el físico cuántico John Wheeler quien dijo que "son necesarios los observadores para dar existencia al mundo" porque vivimos en un "universo de participación", según escribió con Wojcieck Zurek. "Más allá de las partículas, de los campos de fuerza, de la geometría, del espacio y del tiempo, está el último elemento constitutivo de todo ello, el acto todavía más sutil del observador que participa".

Desde entonces la física no ha dejado de profundizar en el dilema que plantean las partículas elementales. El mundo cuántico describe objetos que se encuentran simultáneamente en varios lugares a la vez. Para describir estos objetos, la física recurre a superposición de estados cuánticos: es una manera de decir que las partículas elementales existen en varios estados superpuestos al mismo tiempo.

La duda surge a la hora de explicar el proceso que reduce esos estados superpuestos al estado concreto que nuestros sentidos perciben en el universo cotidiano. Porque es evidente que en el universo macrofísico los objetos se nos presentan en un estado concreto y no superpuesto.

Cuando se ha extrapolado el mundo cuántico al mundo macrofísico, como ha hecho Schrödinger[8] con su ejemplo del gato[9], se ha identificado al observador y sus instrumentos de medida como el factor de realidad, es decir, aquel elemento que permite a los estados cuánticos superpuestos devenir en estados reales de dimensión única.

Sin embargo, nuevas investigaciones han abierto otras interpretaciones al proceso físico conocido como "reducción del paquete de ondas", es decir, al proceso que reduce la superposición de estados de probabilidad y concreta uno de ellos en el universo macrofísico en el que desenvolvemos nuestra existencia cotidiana.

Para W.H. Zurek y Dieter Zeh, entre otros autores, los así llamados modelos de decoherencia permiten explicar la ausencia de superposiciones en los estados macroscópicos de la materia, sin necesidad de una intervención determinante del observador.

[8] **Erwin Rudolf Josef Alexander Schrödinger.** Físico austríaco famoso por sus contribuciones a la mecánica cuántica, especialmente la ecuación de Schrödinger por la que le fue otorgado el Premio Nobel de Física en 1933. Propuso el experimento mental del gato de Schrödinger.

[9] Supongamos un sistema formado por una caja cerrada y opaca que contiene un gato, una botella de gas venenoso, una partícula radiactiva con un 50% de posibilidades de desintegrarse y un dispositivo tal que, si la partícula se desintegra, se rompa la botella y el gato muere. Al depender todo el sistema del estado final de un único átomo que actúa según la mecánica cuántica, tanto la partícula como el gato forman parte de un sistema sometido a las leyes de la mecánica cuántica. Siguiendo la interpretación de Copenhague, mientras no abramos la caja, el gato está en un estado tal que está vivo y muerto a la vez. En el momento en que abramos la caja, la sola acción de observar al gato modifica el estado del gato, haciendo que pase a estar solamente vivo, o solamente muerto.

Para cada observación hay que hablar de tres subsistemas implicados: el objeto (átomo, gato), el aparato de medida (que permite localizar el objeto) y el entorno (o escenario) donde se desenvuelve el proceso.

La interacción de los sistemas macroscópicos con su entorno es lo que diluye la superposición de estados cuánticos, según los modelos de decoherencia. Es decir, si un pequeño sistema como es un átomo, puede ser aislado de su entorno para ser estudiado, en el mundo macroscópico ese aislamiento no es posible porque un gato (por seguir el ejemplo de Schrödinger) está demasiado adherido a su universo a través de unos intensos mecanismos de fricción, lo que impide observarlo sin su entorno inmediato.

Estas interacciones del gato con su universo inmediato son las que anulan los estados de superposición de los espacios cuánticos y dejan fuera al papel del observador que describía Wheeler como creador de realidad.

La desaparición progresiva de la superposición cuántica ha sido observada experimentalmente en 1996 en el laboratorio Kastler Brossel (LKB) y explica por qué una superposición cuántica no puede sobrevivir a una escala macroscópica.

La decoherencia es la consecuencia inevitable del enredo incontrolable que tienen todos los sistemas físicos con su ambiente. El enredo quiere decir que la realidad no puede estar localizada en el espacio y en el tiempo. Este enredo ha sido confirmado

experimentalmente por Aspect y otros como 'el no lugar cuántico'. Este "no lugar cuántico" es el que permite hablar de teletransportación cuántica, de computadoras cuánticas y de otras consecuencias predichas por la teoría cuántica. En este enredo incontrolable, los estados coherentes típicos de la teoría cuántica son no locales, por lo que no pueden ser observados por un observador. A esta falta de coherencia de los estados cuánticos se llama decoherencia.

En virtud de la decoherencia, el mundo parece clásico. Es decir, ciertos objetos aparecen localizados en el espacio ("partículas"), mientras otros tienen valores repartidos por el espacio ("campos"). De la misma forma, los saltos cuánticos parecen ocurrir debido al mismo proceso de decoherencia según la ecuación de Schrödinger, si el entorno es realmente tenido en cuenta. La realidad es en cambio coherentemente descrita según conceptos cuánticos (como funciones de onda en un espacio multidimensional). De esta forma podemos reestablecer una descripción racional de la naturaleza (aunque haya una cierta relación del observador con el mundo observado).

Por otro lado la decoherencia tiene un significado muy amplio dentro de la física cuántica (o más bien habría que llamarlo un logro) consiste en que el "verdadero mundo cuántico" debe ser mucho más rico que nuestro mundo observado. En términos clásicos hay que decir que existen "muchos mundos" que en total forman el único y verdadero mundo cuántico.

Desde los inicios de la mecánica cuántica se conoce la extraña interacción existente entre un estado cuántico y su entorno: cualquier modificación del mismo transforma el sistema cuántico. De esta forma, si pretendemos observar el estado de un qubit cambiaremos automáticamente su estado, porque no es posible realizar dicha observación sin alterar el entorno.

Se ha demostrado que la computación cuántica tolerante a fallos es viable por debajo de un determinado umbral de ruido, que en términos cuánticos se denomina decoherencia. Si se consigue que los cambios en el sistema cuántico sean mínimos, es decir, que la decoherencia permita realizar operaciones con una fidelidad razonable, no hay ninguna ley física que impida la construcción de una computadora de este tipo.

"El principal obstáculo para hacer actualmente una computadora cuántica es la decoherencia", uno de los pioneros de este emergente campo científico, David Deutsch, físico de la Universidad de Oxford, Inglaterra.

"Una vez superado esto, aunque todavía estamos a décadas de conseguir uno". La mayoría de los científicos involucrados en las investigaciones coinciden en señalar que todavía habrá que esperar bastante tiempo para ver de la potencia de cálculo de estos "supercomputadores", que, sin duda, reportaría beneficios enormes a la sociedad. "Los avances en su comprensión son avances en nuevos materiales, nuevos fármacos, nuevos procesos de síntesis química, nuevos dispositivos

electrónicos: circuitos, sensores, displays...". Cuanto menos, esta tecnología ha generado una gran expectación en el ámbito científico, habiendo sido citada como una de las "10 tecnologías emergentes que cambiarán el mundo"

La computación cuántica, además de su enorme potencial operativo, vemos una nueva forma de calcular basada en principios cuánticos. En 1994, Peter Shor, de los laboratorios AT&T, inventó un algoritmo para computadoras cuánticas (como lo veremos adelante) capaz de factorizar grandes números en sus factores primos en un tiempo insignificante frente a las computadoras actuales.

Este descubrimiento tan solo sería una curiosidad si el problema que resuelve no fuese el pilar sobre el que está construido uno de los sistemas de protección de datos más usado en el mundo: el RSA (Rivest Shamir Adleman). Utilizando el algoritmo de Shor, una computadora cuántica podría descifrar información militar oculta tras una clave de 1024 bits (la habitual para estos asuntos) en cuestión de horas, cuando utilizando unas 8000 computadoras tardaríamos más de 800 millones de años actualmente.

De esta forma, el nacimiento de la computadora cuántica significaría la destrucción de la criptografía actual, pero también el nacimiento de la criptografía cuántica, mucho más segura e inviolable.

Otro de los algoritmos cuánticos más conocidos es el creado por Lov Grover (que veremos más adelante), también de AT&T, capaz de buscar a una velocidad increíble en bases de datos. De momento, los clientes más interesados en esta tecnología son las agencias gubernamentales y de seguridad, así como bancos e institutos de investigación, pero hace falta crear más algoritmos cuánticos, algo extremadamente difícil por la complejidad que exige recrear un sistema así.

"Computadoras cuánticas de algunas decenas de qubits serían ya útiles para simular los propios sistemas cuánticos, que requieren enormes esfuerzos computacionales en las computadoras clásicas actuales". Si se consiguen crear más algoritmos, es posible que se llegue a configurar algún día una computadora cuántica de carácter general, pero en caso contrario se limitaría a explotar su enorme potencia en determinadas operaciones complejas.

El campo de la computación e informática cuántica no ha hecho más que comenzar y ya ha obtenido resultados fundamentales. Hasta ahora el contexto en el que se han realizado la mayoría de las implementaciones de algoritmos completos o núcleos básicos de los mismos es la Resonancia Magnética Nuclear (RMN) sobre moléculas en estado líquido.

Las trampas de iones (conjuntos de iones atrapados en una trampa electromagnética) también han sido empleadas para realizar pequeños sistemas cuánticos, pero el futuro parece encontrarse en otros soportes. "Los dispositivos de

estado sólido son posiblemente los más prometedores hacia la construcción de una computadora cuántica escalable (ampliable). Ya estén basados en nanotecnología o en microelectrónica, se beneficiarían de todo el conocimiento y saber hacer de la industria de semiconductores", opinan los investigadores del tema de la UPM. "De momento hay muchas propuestas, pero ninguna realización completa, a pesar de que ha habido avances muy importantes".

Los algoritmos cuánticos se basan en un margen de error conocido en las operaciones de base y trabajan reduciendo el margen de error a niveles exponencialmente pequeños, comparables al nivel de error de las máquinas actuales.

La clase de complejidad BQP estudia el costo de los algoritmos cuánticos con bajo margen de error.

En Teoría de la complejidad computacional, **BQP** representa la clase de algoritmos que pueden ser resueltos en una computadora cuántica en tiempo polinómico con un margen de error promedio inferior a ¼.

Dicho de otra forma, existe un algoritmo de computación cuántica cuya cota superior en tiempo es polinómica para resolver ese problema, tal que la probabilidad de obtener una respuesta equivocada es menor de 25%.

El nivel de error de ¼ es arbitrario, cualquier valor real k tal que $0 < k < ½$ podría ser utilizado sin cambiar el conjunto **BQP**. La idea es que con una pequeña probabilidad de error se corre el algoritmo un número suficiente de veces se llega a una probabilidad exponencialmente pequeña de que la mayoría de las corridas sean erróneas.

El número de qubits en la computadora depende del tamaño del problema. Por ejemplo, ya se conocen algoritmos para factorizar un entero de n bits utilizando solo $2n$ qubits.

La computación cuántica ha despertado interés debido a que problemas que se supone no pertenecen a P pertenecen a la clase BQP.

Veamos a que se refiere que los problemas pertenecen a P:

En computación, cuando el tiempo de ejecución de un algoritmo (mediante el cual se obtiene una solución al problema) es menor que un cierto valor calculado a partir del número de variables implicadas (generalmente variables de entrada) usando una formula polinómica, se dice que dicho problema se puede resolver en un "Tiempo polinómico".

Por ejemplo, si determinar el camino óptimo que debe recorrer un cartero que pasa por N casas necesita menos de $50*N^2+N$ segundos, entonces el problema es resoluble en un "tiempo polinómico".

De esa manera, tiempos de $2n^2+5n$, o $4n^6+7n^4-2n^2$ son polinómicos; pero 2^n no lo es.

Dentro de los tiempos polinómicos, podemos distinguir los lineales (n), los cuadráticos (n^2), cúbicos (n^3), etc.

En teoría de la complejidad, la clase de complejidad de los problemas de decisión que pueden ser resueltos en tiempo polinómico calculado a partir de la entrada por una máquina de Turing determinista es llamada **P**. Cuando se trata de una máquina de Turing no-determinista, la clase se llama NP.

*Si **P** = **NP**, **P** contendría las zonas **NP** y **NP**-completo.*
Figura 9.

En este problema la clase de los problemas NP-completos que pueden ser descritos como los problemas en **NP** que tienen menos posibilidades de estar en **P**. Actualmente los investigadores piensan que las clases cumplen con el diagrama mostrado por lo que P y NP-completo tendrían intersección vacía.

La importancia de la pregunta **P** = **NP** radica en que de encontrarse un algoritmo en P para un problema NP-completo, todos los problemas NP-completos (y por ende, todos los problemas de NP) tendrían soluciones en tiempo polinómico.

Actualmente solo se han clasificado tres de esos problemas:

- Factorización entera (algoritmo de Shor)
- Logaritmo discreto
- Simulación de sistemas cuánticos

La clase QBP está definida en base a un computador cuántico. La clase correspondiente para una máquina de Turing se llama **BPP.**

ALGORITMO DE SHOR

Es un algoritmo cuántico para descomponer en factores un número *N* en tiempo $O((\log N)^3)$ y espacio $O(\log N)$, así nombrado por Peter Shor.

Muchas Criptografías de clave pública, tales como RSA, llegarían a ser obsoletas si el algoritmo de Shor es implementado alguna vez en una computadora cuántica práctica. Un mensaje cifrado con RSA puede ser descifrado descomponiendo en factores la llave pública *N*, que es el producto de dos números primos. Los algoritmos clásicos conocidos no pueden hacer esto en tiempo $O((\log N)^k)$ para ningún *k*, así que llegan a ser rápidamente imprácticos a medida que se aumenta *N*. Por el contrario, el algoritmo de Shor puede romper RSA en tiempo polinómico. También se ha ampliado para atacar muchas otras criptografías públicas.

Como todos los algoritmos de computación cuántica, el algoritmo de Shor es probabilístico: da la respuesta correcta con alta probabilidad, y la probabilidad de fallo puede ser disminuida repitiendo el algoritmo.

El algoritmo de Shor fue demostrado en 2001 por un grupo en IBM, que descompuso 15 en sus factores 3 y 5, usando una computadora cuántica con 7 qubits.

Procedimiento

El problema que estamos intentando solucionar es que, dado un número entero *N*, intentamos encontrar otro número entero *p* entre *1* y *N* que divida *N*.

El algoritmo de Shor consiste en dos partes:

1. Una reducción del problema de descomponer en factores al problema de encontrar el orden, que se puede hacer en una computadora clásica.

2. Un algoritmo cuántico para solucionar el problema de encontrar el orden.

Parte clásica

1. Escoja un número pseudo-aleatorio $a < N$

2. Compute el mcd(a, N). Esto se puede hacer usando el algoritmo de Euclides. (ver anexo)

3. Si el mcd(a, N) $\neq 1$, entonces es un factor no trivial de N, así que terminamos.

4. Si no, utilice el subprograma para encontrar el período para encontrar r, el período de la función siguiente:

$f(x) = a^x \bmod N$, es decir el número entero más pequeño *r* para el cual $f(x+r) = f(x)$.

5. Si *r* es impar, vaya de nuevo al paso 1.

6. Si $a^{r/n} \equiv -1 (\bmod N)$, vaya de nuevo al paso 1.

7. Los factores de *N* son el $mcd(a^{r/2} \pm 1, N)$. Terminamos.

Parte cuántica: subprograma para encontrar el período:

1. Comience con un par de registros qubits de entrada y salida con $\log_2 N$ qubits cada uno, e inicialícelos a $N^{-1/2} \sum_x |x\rangle |0\rangle$ donde *x* va de 0 a *N-1*.

2. Construya *f(x)* como función cuántica y aplíquela al estado anterior, para obtener $N^{-1/2} \sum_x |x\rangle |f(x)\rangle$

3. Aplique la transformada de Fourier cuántica al registro de entrada. La transformada de Fourier cuántica en *N* puntos se define como:

$$U_{QFT} |x\rangle = N^{-1/2} \sum_y e^{2\pi i xy/N} |y\rangle$$

Lo que nos deja en el estado siguiente: $N^{-1}\sum_x\sum_y e^{2\pi ixy/N}|\,y\rangle|\,f(x)\rangle$

4. Realice una medición. Obtenemos un cierto resultado *y* en el registro de entrada y $f(x_0)$ en el registro de salida. Puesto que *f* es periódica, la probabilidad de medir cierto *y* viene dada por

$$N^{-1}\left|\sum_{x:f(x)=f(x_0)} e^{\frac{2\pi ixy}{N}}\right|^2 = N^{-1}\left|\sum_b e^{\frac{2\pi i(x_0+rb)y}{N}}\right|^2$$

El análisis muestra ahora que tanto más alta es esta probabilidad, tanto más el yr/N es cercano a un número entero.

5. Convierta a y/N en una fracción irreducible, y extraiga el denominador *r* ', que es un candidato a *r*.

6. Compruebe si $f(x)=f(x+r')$. Si es así terminamos.

7. Si no, obtenga más candidatos a *r* usando valores cercanos a *y*, o múltiplos de *r* '. Si cualquier candidato trabaja, terminamos. Si no, vaya de nuevo al paso 1 del subprograma.

8. Si no, vaya de nuevo al paso 1 del subprograma.

Explicación del algoritmo

El algoritmo se compone de dos partes. La primera parte del algoritmo convierte el problema de descomponer en factores se reduce a encontrar el período de una función, y se puede implementar clásicamente. La segunda parte encuentra el período usando la transformada de Fourier cuántica, y es responsable de la aceleración cuántica.

I. Obtención de factores a partir del período

Los números enteros menores que *N* y coprimos con *N* forman un grupo finito bajo multiplicación módulo *N*, que se denota típicamente $(Z/NZ)^{x}$. Para el final del paso 3, tenemos un número entero a en este grupo. Puesto que el grupo es finito, a debe tener un orden finito *r*, el número entero positivo más pequeño tal que $a^r \equiv 1 \bmod N$.

Por lo tanto $N \mid (a^r - 1)$. Suponga que podemos obtener *r*, y es par. Entonces

$$a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \bmod N$$
$$\Rightarrow N \mid (a^{r/2} - 1)(a^{r/2} + 1)$$

r es el número entero positivo *más pequeño* tal que $a^r \equiv 1$, así que *N* no puede dividir a $(a^{r/2}-1)$. Si *N* tampoco divide $(a^{r/2}+1)$, entonces *N* debe tener un factor común no trivial con $(a^{r/2}-1)$ y $(a^{r/2}+1)$.

Prueba:

Por simplicidad, consideremos $(a^{r/2}-1)$ y $(a^{r/2}+1)$ *u* y *v* respectivamente. $N \mid uv$, luego $kN = uv$ para un cierto número entero *k*. Suponga que el $mcd(u,N)=1$; entonces $mu + nN = 1$ para ciertos números enteros *m* y *n* (ésta es una propiedad del máximo común divisor.) Multiplicando ambos lados por *v*, encontramos que $mkN + nvN + nvN = v$, luego $N \mid v$. Por contradicción $mcd(u,N) \neq 1$. Por un argumento similar $mcd(v,N) \neq 1$.

Esto nos provee de una factorización de *N*. Si *N* es el producto de dos primos, esta es la *única* factorización posible.

II. Encontrar el período

El algoritmo para encontrar el período de Shor se basa radicalmente en la capacidad de una computadora cuántica de estar en muchos estados simultáneamente. Los físicos llaman a este comportamiento una "superposición" de estados. Para computar

el período de una función *f*, evaluamos la función en todos los puntos simultáneamente.

Sin embargo, La física cuántica no permite que tengamos acceso a toda esta información directamente. Una medición cuántica dará solamente uno de todos los valores posibles, destruyendo todos los otros. Por lo tanto tenemos que transformar cuidadosamente la superposición a otro estado que devuelva la respuesta correcta con alta probabilidad. Esto es alcanzado y usando la transformada de Fourier cuántica.

Shor tuvo que solucionar así tres "problemas de implementación". Todos tuvieron que ser implantados "rápidos", que significa ejecutar con un número de puertas cuánticas que es polinómico en $\log N$.

1. Crear una superposición de estados. Esto puede ser hecho aplicando las puertas de Hadamard a todos los qubits en el registro de entrada. Otro enfoque sería utilizar transformada de Fourier cuántica.

2. Implementar la función *f* como una transformada cuántica. Para alcanzar esto, Shor utilizó exponenciación por cuadrados para su transformación modular de la exponenciación.

3. Realizar una transformada de Fourier cuántica. Usando puertas controladas NOT y puertas de una sola rotación de qubit, Shor diseñó un circuito para la transformada de Fourier cuántica que usa exactamente $((\log N)^2)$ puertas.

Después de todas estas transformaciones una medición dará una aproximación al período *r*. Por simplicidad asuma que hay una *y* tal que yr/N es un número entero. Entonces la probabilidad de medir *y* es 1. Para ver esto notemos que

$$e^{2\pi ibyr/N} = 1$$

para todos los números enteros *b*. Por lo tanto la suma que nos da la probabilidad de la medición y será N/r puesto que b toma aproximadamente N/r valores y así la probabilidad es *1/r*. Hay *r*, y tales que yr/N es un número entero, luego la suma de las probabilidades es 1. Nota: otra manera de explicar el algoritmo de Shor es observando que es precisamente el algoritmo de valoración de fase cuántica disfrazado.

ALGORITMO DE DEUTSCH-JOZSA

Sea $v=\{0,1\}$ el conjunto de valores de verdad clásicos. De las $2^2=4$ funciones booleanas $f: v \to v$ dos son constantes y las otras dos son equilibradas. Al nombrarlas

$$f_0: \begin{matrix} 0 \mapsto 0 \\ 1 \mapsto 0 \end{matrix}, \quad f_1: \begin{matrix} 0 \mapsto 0 \\ 1 \mapsto 1 \end{matrix},$$
$$f_2: \begin{matrix} 0 \mapsto 1 \\ 1 \mapsto 0 \end{matrix}, \quad f_3: \begin{matrix} 0 \mapsto 1 \\ 1 \mapsto 1 \end{matrix}$$

se tiene que las funciones constantes son f_0 y f_3, y las equilibradas son f_1 y f_2.

El propósito del algoritmo de Deutsch-Jozsa es decidir, para una f dada, si acaso es constante o equilibrada "utilizando un solo paso de cómputo".

Sea U_f una matriz permutación de orden $2^2 \times 2^2$ tal que $U_f(e_x \otimes e_z) = (e_x \otimes e_{(z+f(x)) \bmod 2})$. U_f es pues unitaria. De hecho es muy similar al funcionamiento de la compuerta "negación controlada", salvo que en aquella, la función f es propiamente la identidad. En la siguiente tabla ilustramos la acción de U_f refiriéndonos solamente a los índices de vectores básicos.

Tabla: Acción de la matriz unitaria U_f en el algoritmo de Deutsch-Jozsa.

(x,z)	$(x,(z+f(x)) \bmod 2)$
(0,0)	$(0,f(0))$
(0,1)	$(0,\overline{f(0)})$
(1,0)	$(1,f(1))$
(1,1)	$(1,f(1))$

Considerando el operador de Hadamard H, hagamos $H_2 = H \otimes H$. Primero se tiene,

$H(e_0) = x_0 = (1/\sqrt{2})(e_0 + e_1)$ y $H(e_0) = x_1 = (1/\sqrt{2})(e_0 - e_1) \in H_1$ y luego

$H_2(e_0 \otimes e_1) = H(e_0) \otimes H(e_1) = x_0 \otimes x_1$. Claramente, $x_0 \otimes x_1 = \frac{1}{2}(e_{00} - e_{01} + e_{10} - e_{11}) \in H_2$

Por tanto,

$$U_f(x_0 \otimes x_1) = \tfrac{1}{2}(e_{0,f(0)} - e_{0,\overline{f(0)}} + e_{1,f(1)} - e_{1,\overline{f(1)}})$$

$$= \frac{1}{\sqrt{2}} e_0 \otimes \left[\frac{1}{\sqrt{2}}(e_{f(0)} - e_{\overline{f(0)}})\right] + \frac{1}{\sqrt{2}} e_1 \otimes \left[\frac{1}{\sqrt{2}}(e_{f(1)} - e_{\overline{f(1)}}\right]$$

$$= \begin{cases} \frac{1}{\sqrt{2}} e_0 \otimes x_1 + \frac{1}{\sqrt{2}} e_1 \otimes x_1 & si \quad f = f_0 \\ \frac{1}{\sqrt{2}} e_0 \otimes x_1 - \frac{1}{\sqrt{2}} e_1 \otimes x_1 & si \quad f = f_1 \\ -\frac{1}{\sqrt{2}} e_0 \otimes x_1 + \frac{1}{\sqrt{2}} e_1 \otimes x_1 & si \quad f = f_2 \\ -\frac{1}{\sqrt{2}} e_0 \otimes x_1 - \frac{1}{\sqrt{2}} e_1 \otimes x_1 & si \quad f = f_3 \end{cases}$$

$$= \begin{cases} x_0 \otimes x_1 & si \quad f = f_0 \\ x_1 \otimes x_1 & si \quad f = f_1 \\ -x_1 \otimes x_1 & si \quad f = f_2 \\ -x_0 \otimes x_1 & si \quad f = f_3 \end{cases}$$

En consecuencia,

$$H_2 U_f H_2(e_0 \otimes e_1) = H_2 U_f(x_0 \otimes x_1) = \begin{cases} Hx_0 \otimes Hx_1 & si \quad f = f_0 \\ Hx_1 \otimes Hx_1 & si \quad f = f_1 \\ -Hx_1 \otimes Hx_1 & si \quad f = f_2 \\ -Hx_0 \otimes Hx_1 & si \quad f = f_3 \end{cases}$$

$$= \begin{cases} e_0 \otimes e_1 & si \quad f = f_0 \\ e_1 \otimes e_1 & si \quad f = f_1 \\ -e_1 \otimes e_1 & si \quad f = f_2 \\ -e_0 \otimes e_1 & si \quad f = f_3 \end{cases}$$

vale decir, al aplicar el algoritmo cuántico $H_2 U_f H_2$ (nótese que utilizamos notación algebraica: los operadores se aplican de derecha a izquierda), partiendo del vector básico $e_0 \otimes e_1$ se obtiene un vector de la forma $\varepsilon e_S \otimes e_1$ donde $\varepsilon \in \{-1,1\}$ es un signo y

S es una señal que indica si acaso f es o no equilibrada. En otras palabras, la respuesta S coincide con $f(0) \oplus f(1)$, donde $\oplus$ es la *disyunción excluyente*, XOR. La exploración del valor S se realiza siguiendo el postulado de medición, y su valor está apareciendo leyendo sólo el primer qubit. Al efectuar la medición se elige al vector básico $e_S \otimes e_1$ con probabilidad $\varepsilon^2 = 1$.

ALGORITMO DE BÚSQUEDA DE GROVER

Muchos problemas, que se pueden denominar problemas de búsqueda, se pueden plantear de la siguiente forma: "Hallar x en un conjunto de posibles soluciones tal que la sentencia $P(x)$ sea cierta".

Por ejemplo, el problema de buscar un factor para un número entero q se puede tratar con un algoritmo de búsqueda en una lista que contenga a todos los enteros ente 2 y $\sqrt{q}$, buscando uno que verifique la propiedad $P(x) : q \bmod x = 0$.

Un problema de búsqueda no estructurada es aquel para cuya resolución no puede usar ninguna hipótesis relativa a la estructura del espacio de soluciones o a la sentencia P.

Por ejemplo, una búsqueda en una lista alfabetizada, como la búsqueda del número de un usuario en el directorio telefónico, es un problema de búsqueda estructurada,

mientras que la búsqueda en el mismo directorio del titular de un número concreto sería una búsqueda no estructurada. En una búsqueda estructurada, se puede usar la estructura ordenada de la lista para construir algoritmos eficientes, pero en una búsqueda no estructurada lo habitual es probar aleatoriamente la veracidad de la sentencia. En el modelo de computación clásico, para un espacio de búsqueda de tamaño N, sería necesario evaluar P un promedio de $N/2$ veces y N veces en el peor de los casos. Los algoritmos clásicos de búsqueda no estructurada requieren $O(N)$ evaluaciones de P.

Grover probó en 1996 que, en computación cuántica, un problema de búsqueda no estructurada, con solución única, se puede resolver, con probabilidad acotada, con $O(\sqrt{N})$ evaluaciones de P. Posteriormente, Boyer y otros generalizaron el algoritmo para problemas con solución múltiple (obviamente, el caso interesante es cuando el número de soluciones es pequeño en relación al tamaño de la lista).

Veamos como funciona el algoritmo de búsqueda de Grover.

Partimos de una lista de tamaño N. Supondremos, incrementando la lista si es preciso, que $N = 2^n$ para algún n. Trabajaremos con los índices de los elementos de la lista, es decir con $x = 0 \ldots 2^n - 1$ y queremos localizar aquellos x tales que $P(x) = 1$, para una cierta propiedad P.

La computación cuántica permite evaluar P simultáneamente sobre todas las posibles entradas, sin más que construir el estado:

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{x=0}^{N-1} |x\rangle$$

que se obtiene, a partir de $|00\ldots0\rangle$, con la transformación de Walsh-Hadamard. El problema es que no se puede leer el resultado obtenido sin destruir el estado.

La idea que aplicaremos es la siguiente: Partimos del estado $|\psi\rangle$ y lo iremos modificando de modo que se vaya incrementando la amplitud de los x tales que $P(x)=1$ y disminuyendo la de aquellos que no verifican la propiedad. Así conseguiremos, al medir el registro resultante, tener un acierto con probabilidad alta. Para conseguir tal efecto, en un estado cuántico

$$\sum_{j=0}^{N-1} a_j |x_j\rangle$$

primero invertimos la amplitud, es decir cambiaremos a_j por $-a_j$ para los x_j tales que $P(x_j)=1$ y después realizamos la operación denominada inversión sobre el promedio, que transforma:

$$\sum_{j=0}^{N-1} a_j |x_j\rangle \quad \text{en} \quad \sum_{j=0}^{N-1} (2A - a_j) |x_j\rangle$$

donde A es el promedio de los a_j.

Notemos que si los a_j son números reales, después de realizar estas operaciones se tendrá un estado cuyas amplitudes serán también números reales.

Veamos cómo llevar a cabo cada una de estas operaciones:

1. Cambio de signo de la amplitud, es decir, tendremos que implementar la siguiente transformación:

$$U:|x\rangle \to (-1)^{P(x)}|x\rangle$$

que no modifica los $|x\rangle$ tales que $P(x)=0$ y pone un coeficiente -1 a los que verifican $P(x)=1$.

La puerta cuántica U_p implementa la evaluación de la función P del siguiente modo:

$$U_p:|x,b\rangle \to |x,b\oplus P(x)\rangle$$

donde $\oplus$ es la suma módulo 2. Cuando sólo se quiere evaluar P sobre un estado $|x\rangle$ se aplica U_p con $b=0$, pero nosotros vamos a considerar el estado $b=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$.

Notemos que si $P(x)=0$ entonces $b \oplus P(x) = b$, mientras que si $P(x)=1$ es $b \oplus P(x) = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -b$. Luego:

$$U_p(|x,b\rangle) = (-1)^{P(x)}|x,b\rangle$$

Con esta transformación se realiza simultáneamente la evaluación de P y la inversión de amplitudes de los $|x_j\rangle$ que satisfacen la propiedad.

Vamos a detallar la actuación de U_p sobre un estado cualquiera $\phi = \sum_{j=0}^{N-1} a_j |x_j\rangle$.

Sean $X_0 = \{x : P(x) = 0\}$ y $X_1 = \{x : P(x) = 1\}$. Entonces:

$$U_p(|\phi,b\rangle) = U_p\left(\sum_{x_j \in X_0} a_j |x_j,b\rangle + \sum_{x_j \in X_2} a_j |x_j,b\rangle\right)$$

$$= \left(\sum_{x_j \in X_0} a_j |x_j,b\rangle - \sum_{x_j \in X_2} a_j |x_j,b\rangle\right) = \left(\sum_{x_j \in X_0} a_j |x_j\rangle - \sum_{x_j \in X_2} a_j |x_j\rangle\right) \otimes |b\rangle$$

Por tanto, el efecto de U_p es el cambio de signo de las amplitudes.

Notemos que en la salida de U_p no se modifica el estado b, por tanto podemos omitirlo al escribir y en lo que sigue nos referiremos a esta trasformación como:

$$U : |x\rangle \rightarrow (-1)^{P(x)}|x\rangle$$

2. Inversión sobre el promedio.

Dado $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$, es fácil ver que la transformación $G = 2|\psi\rangle \langle\psi| - I$ cuya matriz asociada es:

$$G = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix}$$

transforma $\sum_{j=0}^{N} a_j |x_j\rangle$ en $\sum_{j=0}^{N} (2A - a_j)|x_j\rangle$, donde A es el promedio de los a_j.

Grover propuso una implementación eficiente de esta transformación con $O(\log(N))$ puertas elementales. Para ello basta probar que $G = W_n R W_n$ donde W_n es la transformación de Walsh-Hadamard $(W_n = H \otimes \ldots (n \otimes H)$ y $R = (r_{ij})$ es una matriz diagonal tal que $r_{11} = 1$ y $r_{ii} = -1$ para $i = 2 \ldots N$.

La matriz R se puede escribir como $R = R' - I$ donde $R' = 2|0\rangle \langle 0|$ es una matriz con todos sus elementos iguales a 0 menos el de la primera fila y primera columna que es $r'_{11} = 2$. Entonces

$$W_n R W_n = W_n (2|0\rangle \langle 0| - I) W_n = W_n 2|0\rangle \langle 0| W_n - I$$

y como $W_n|0\rangle = |\psi\rangle$, se concluye que:

$$W_n R W_n = 2|\psi\rangle\langle\psi| - I = G$$

La transformación R se puede implementar con $n = \log(N)$ puertas de Toffoly y el costo de W_n también es $\log(N)$.

El algoritmo de Grover consiste en aplicar sucesiva y reiteradamente las trasformaciones U y G. Debemos determinar cuántas veces hacerlo para maximizar la probabilidad de acierto.

Ejemplo:

Supongamos que se tiene una lista de 64 elementos de los que sólo uno, que denominamos x_0, verifica la propiedad P.

En primer lugar se construye el estado $|\psi\rangle = \frac{1}{8}\sum_{x=0}^{63}|x\rangle$. Inicialmente todos los coeficientes son iguales a $1/8$. Cambiamos el signo de la amplitud de x_0 y hacemos el promedio, que será $A = (63\frac{1}{8} - \frac{1}{8})/64 \approx 0.12109$. Hacemos la operación de inversión en el promedio y la nueva amplitud para x_0 es 0.367818, mientras que para el resto es 0.117187. Si repetimos el proceso, después de 6 iteraciones, el coeficiente de $|x_0\rangle$ es 0.998291, mientras que el

resto de los coeficientes son iguales a -0.00736174. Si en este momento medimos el estado, tendremos una probabilidad de acierto de 0.998291^2, pero si seguimos iterando las cosas empiezan a cambiar. Por ejemplo después de 10 iteraciones la amplitud de x_0 es aproximadamente 0.487922. Por esto es importante determinar el número adecuado de veces que hay que aplicar al algoritmo.

Ahora veamos el algoritmo de búsqueda de Grover desde una visión geométrica.

Supongamos que tenemos una lista de $N = 2^n$ elementos de los cuales s verifican la propiedad P. Construimos el siguiente estado :

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

y consideramos los siguientes estados:

$$|\alpha\rangle = \frac{1}{\sqrt{N-s}} \sum_{x \in X_0} |x\rangle, \qquad |\beta\rangle = \frac{1}{\sqrt{s}} \sum_{x \in X_1} |x\rangle$$

con X_0 y X_1 definidos anteriormente.

Evidentemente $|\alpha\rangle$ y $|\beta\rangle$ son ortonormales y podemos considerar el subespacio de Hilbert real.

$$L_R(|\alpha\rangle,|\beta\rangle) = \{a|\alpha\rangle + b|\beta\rangle, a,b \in R\}$$

que tiene como base $\{|\alpha\rangle,|\beta\rangle\}$.

En este espacio podemos escribir

$$|\psi\rangle = \sqrt{\frac{N-s}{N}}|\alpha\rangle + \sqrt{\frac{s}{N}}|\beta\rangle$$

y las trasformaciones U y G verifican que:

$$U(L_R(|\alpha\rangle,|\beta\rangle)) = L_R(|\alpha\rangle,|\beta\rangle), \qquad G(L_R(|\alpha\rangle,|\beta\rangle)) = L_R(|\alpha\rangle,|\beta\rangle)$$

Trabajando con este plano euclídeo, la trasformación U es una simetría respecto a $|\alpha\rangle$ ya que transforma el vector $a|\alpha\rangle + b|\beta\rangle$ en $a|\alpha\rangle - b|\beta\rangle$, mientras que $G = 2|\psi\rangle\langle\psi| - I$ es una simetría respecto de $|\psi\rangle$, pues su matriz asociada es:

$$G = 2\begin{pmatrix}\sqrt{\frac{N-s}{N}}\\ \sqrt{\frac{s}{N}}\end{pmatrix}\begin{pmatrix}\sqrt{\frac{N-s}{N}} & \sqrt{\frac{s}{N}}\end{pmatrix} - I = \begin{pmatrix}1-\frac{2s}{N} & 2\frac{\sqrt{(N-s)s}}{N}\\ 2\frac{\sqrt{(N-s)s}}{N} & \frac{2s}{N}-1\end{pmatrix}$$

que es la matriz de una simetría respecto a $|\psi\rangle$.

La composición de dos simetrías es un giro de ángulo doble del que forman los dos vectores. Por lo tanto, trabajando en el plano $L_R(|\alpha\rangle,|\beta\rangle)$ el algoritmo de Grover consiste en hacer un giro de ángulo θ donde $\theta \in [0, \frac{\pi}{2}]$ y $\cos(\frac{\pi}{2})$ es el producto escalar de los vectores unitarios $|\alpha\rangle$ y $|\psi\rangle$:

$$\cos\left(\frac{\theta}{2}\right) = \langle\alpha|\psi\rangle = \sqrt{\frac{N-s}{N}}$$

Obviamente $\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{s}{N}}$

Sea $\gamma = \frac{\theta}{2}$. En la base $\{|\alpha\rangle,|\beta\rangle\}$, el estado inicial es: $|\psi\rangle = \cos(\gamma)|\alpha\rangle + \sin(\gamma)|\beta\rangle$.

La aplicación del algoritmo supone un giro de ángulo $\theta = 2\gamma$ y el estado se trasnforma en:

$$\cos(3\gamma)|\alpha\rangle + \sin(3\gamma)|\beta\rangle.$$

El número óptimo de iteraciones será el número de veces que hace falta hacer un giro de ángulo θ para llevar $|\psi\rangle$ a $|\beta\rangle$ y cabe esperar que sea próximo a

$$\frac{\frac{\pi}{2}-\gamma}{2\gamma}=\frac{\pi}{4\gamma}-\frac{1}{2}.$$

Después de k iteraciones tendremos:

$$\cos((2k+1)\gamma)|\alpha\rangle+\sin((2k+1)\gamma)|\beta\rangle$$

La expresión de este estado en el espacio N-dimensional es:

$$\cos((2k+1)\gamma)\frac{1}{\sqrt{N-s}}\sum_{x\in X_0}|x\rangle+\sin((2k+1)\gamma)\frac{1}{\sqrt{s}}\sum_{x\in X_1}|x\rangle$$

Sin embargo también tendremos que considerar cual será el número óptimo de iteraciones y para ello partimos de una lista de $N=2^n$ elementos de los cuales s verifican la propiedad P. Construimos el siguiente estado:

$$|\psi\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

y aplicamos reiteradamente el algoritmo de Grover. Después de k iteraciones, los elementos que verifican la propiedad tendrán todos la misma amplitud, que

denominamos b_k, y los que no la verifican tendrán una amplitud, que denominamos m_k. Podemos escribir el estado de la siguiente forma:

$$m_k \sum_{x \in X_0} |x\rangle + b_k \sum_{x \in X_1} |x\rangle$$

En cada iteración del algoritmo, las amplitudes b_k cambian de signo (es el efecto de la aplicación U) y después se aplica G, cuyo efecto es la inversión en el promedio de las amplitudes, luego se verifican las siguientes ecuaciones recursivas:

$$m_0 = b_0 = \frac{1}{\sqrt{N}}$$

$$m_{k+1} = 2A_k - m_k \qquad b_{k+1} = 2A_k + b_k$$

donde:

$$A_k = \frac{(N-s)m_k - sb_k}{N}$$

Es decir:

$$\begin{pmatrix} m_{k+1} \\ b_{k+1} \end{pmatrix} = \begin{pmatrix} \frac{N-2s}{N} & -\frac{2s}{N} \\ \frac{2N-2s}{N} & \frac{N-2s}{N} \end{pmatrix} \begin{pmatrix} m_k \\ b_k \end{pmatrix}$$

Se puede demostrar por inducción que la solución de este sistema de ecuaciones en diferencias es precisamente el resultado obtenido geométricamente. Es decir:

$$m_k = \frac{1}{\sqrt{N-s}}\cos((2k+1)\gamma) \qquad b_k = \frac{1}{\sqrt{s}}\sin((2k+1)\gamma)$$

donde

$$\cos(\gamma) = \sqrt{\frac{N-s}{N}} \qquad \sin(\gamma) = \sqrt{\frac{s}{N}}$$

Para conseguir la máxima probabilidad de acierto, habría que minimizar $|m_k|$. Se tendría $m_k = 0$ si $(2k+1)\gamma = \frac{\pi}{2}$. Es decir si $k = \frac{\pi}{4\gamma} - \frac{1}{2}$, como habíamos visto con anterioridad. Pero esto no es posible porque el número de iteraciones debe ser entero.

Vamos a tomar $\tilde{k} = \left\lfloor \pi/(4\gamma) \right\rfloor$ y así $\left|k - \tilde{k}\right| \le 1/2$, con lo que:

$$\left|\frac{\pi}{2} - \left(2\tilde{k}+1\right)\gamma\right| = \left|(2k+1)\gamma - \left(2\tilde{k}+1\right)\gamma\right| = \left|2\gamma\left(k-\tilde{k}\right) \le \gamma\right|$$

Después de $\tilde{k}$ iteraciones la probabilidad de fallo es:

$$(N-s)\left(m_{\tilde{k}}\right)^2 = \cos^2\left(\left(2\tilde{k}+1\right)\gamma\right) = \sin^2\left(\frac{\pi}{2} - \left(2\tilde{k}+1\right)\gamma\right) \le \sin^2(\gamma) = \frac{s}{N}$$

En consecuencia, la probabilidad de fallo después de $\left\lfloor \pi/(4\gamma) \right\rfloor$ iteraciones es menor que s/N.

Ahora veamos el algoritmo de búsqueda de Grover cuando se conoce el número de soluciones.

Se dispone de una lista de $N = 2^n$ elementos de los cuales se sabe que hay s que verifican la propiedad P. Se numeran los elementos de la lista y se trabaja con los índices correspondientes.

El siguiente algoritmo proporciona solución con probabilidad de fallo menor que s/N:

1. Estado inicial: $|0\ldots0\rangle$.
2. Aplicar la transformación de Hadamard con la que se obtiene $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
3. Aplicar $U : |x\rangle \rightarrow (-1)^{P(x)} |x\rangle$.
4. Aplicar $G = 2|\psi\rangle\langle\psi| - I$.
5. Repetir $\left\lfloor \pi/(4\gamma) \right\rfloor$ veces los pasos 3 y 4.
6. Leer el resultado.

Este algoritmo es apropiado cuando s es pequeño en relación a N.

El número de iteraciones es $O(\sqrt{N})$ ya que:

$$\left\lfloor \frac{\pi}{4\gamma} \right\rfloor \leq \frac{\pi}{4\sin(\gamma)} = \frac{\pi}{4\sqrt{s/N}} = \frac{\pi}{4}\sqrt{\frac{N}{s}}$$

Si tenemos en cuenta que el coste de la transformación G es $O(\log(N))$, la complejidad total es $O(\sqrt{N}\log(N))$.

Veamos un ejemplo de aplicación del algoritmo de búsqueda de Grover.

Supongamos que partimos de una lista de 8 elementos $[0,1,\ldots,7]$ y buscamos un múltiplo de 5 distinto de 0, sabiendo que existe una única solución. En este caso la propiedad P podría ser $P(x) = 1 - (x+1) \bmod 5$, de modo que si $P(x) = 1$, entonces $x+1$ es la solución.

La transformación unitaria U correspondiente a esta propiedad tiene como matriz:

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Pero esta matriz no es conocida, si no se conoce la solución del problema. La transformación U actúa como caja negra. Por ello, muchos autores la denominan "oráculo".

La matriz de la aplicación G sólo depende del tamaño de la lista y en este ejemplo es:

$$G = \frac{1}{4}\begin{pmatrix} -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -3 \end{pmatrix}$$

A continuación aplicamos el algoritmo:

1. Partimos del estado $|00\ldots0\rangle$.
2. Transformación de Walsh-Hadamard y resulta $\frac{1}{\sqrt{8}}\sum_{x=0}^{7}|x\rangle$.
3. a 5. El número de iteraciones es $\lfloor \pi\sqrt{N}/4 \rfloor = 2$.

Tras la primera aplicación de U y G las amplitudes resultantes son:

$$\frac{1}{4\sqrt{2}}[1,1,1,1,5,1,1,1]$$

Notemos que este resultado es desconocido, ya que si medimos el estado se destruye. Después de la segunda iteración resulta:

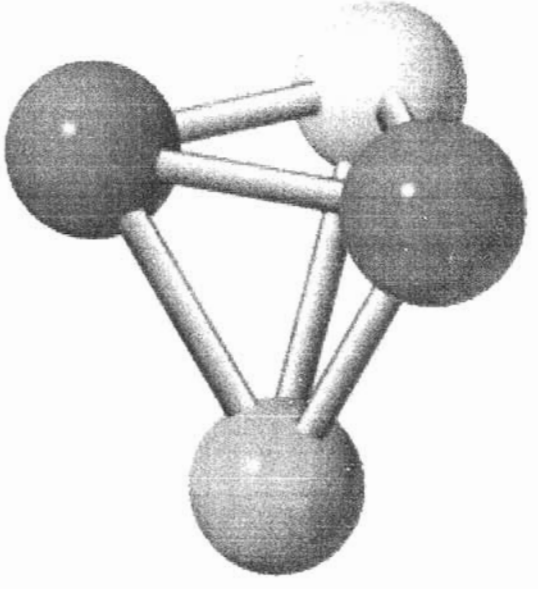
$$\frac{1}{8\sqrt{2}}[-1,-1,-1,-1,11,-1,-1,-1]$$

6. Leer el resultado.

La probabilidad real de éxito es $121/128 \approx 0.9453125$. El método garantiza una probabilidad de éxito mayor o igual que $7/8 \approx 0.875$.

Cuando no se conoce el número de soluciones una alternativa es usar una aplicación de la trasformada cuántica de Fourier para determinar dicho número y después encontrar una solución con el algoritmo de Grover básico.

Capítulo 4



Nuevas Tendencias

La ciencia será siempre una búsqueda,
jamás un descubrimiento real.
Es un viaje, nunca una llegada.
(Karl R. Popper)

AUTÓMATA CELULAR CUÁNTICO (QCA)

A diferencia de los modelos de computadoras, el autómata celular cuántico está diseñado de modo que aprovecha el comportamiento de los sistemas a escala cuántica. El modelo de red o circuito cuántico, por ejemplo, no trata de ser más que una adaptación del modelo de circuito tradicional, aunque como tal tropieza con dificultades, como la imposibilidad de clonar los estados y el hecho de que debemos pensar en las operaciones como operadores actuando sobre registros cuánticos, y no necesariamente como etapas en la propagación de señales.

Básicamente, un autómata celular consiste en un arreglo de puntos cuánticos, acoplados mediante interacción coulombiana. En cada celda, los electrones tienen un estado bien definido, y determinado por la interacción con las celdas vecinas. La probabilidad de efecto túnel será despreciable. Más adelante veremos que no es complicado en principio conseguir que un sistema de este tipo realice diferentes tipos de operaciones. De hecho, si hay algo difícil en el autómata celular es la conexión con el exterior, en mucho mayor medida que la implementación de las operaciones.

En la definición de computadora cuántica[10] vemos que es necesario proveer un método para inicializar los qubits en un estado conocido. Esto lo haremos por medio

[10] Colección de n qubits sobre los que es posible:

1. Cada qubit puede prepararse en un estado conocido $|0\rangle$.
2. Los qubits pueden medirse en la base $\{|0\rangle,|1\rangle\}$.

de unos electrodos de control. El estado de todo el sistema viene dado por unas condiciones de contorno que son precisamente las que producen los canales de entrada, y es ahí donde los electrodos de control irán situados. Sin entrar aún en la descripción de cada celda, un autómata celular en dos dimensiones es el sistema representado en la siguiente figura:

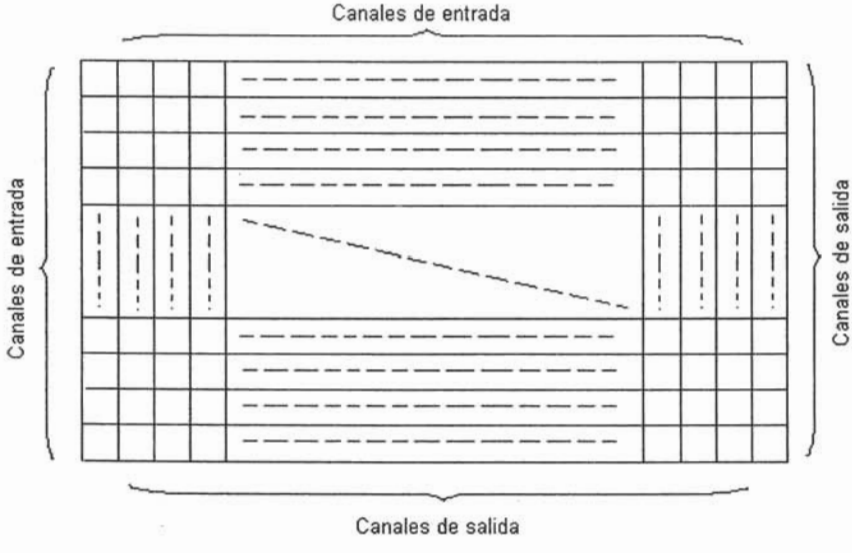


Figura 10. *Autómata celular cuántico*

Existe un problema, asociado a la interconexión de dispositivos cuando el tamaño disminuye, que resuelve el esquema propuesto. Como sólo suministramos entradas desde los bordes del arreglo, a medida que este se hace más pequeño las energías características asociadas se hacen cada vez más importantes, y con ello se hace

3. Sobre cualquier subconjunto de qubits de tamaño fijo podemos aplicar una (o un conjunto de) puertas universales.
4. Los qubits sólo evolucionarán de la manera prevista en las puertas.

factible realizar computaciones a mayores temperaturas. Se considera posible llevar de esta manera la computación cuántica a escala molecular.

Primero nos aproximaremos al autómata celular desde su comportamiento independiente del tiempo, para luego ver cómo evoluciona con el paso de este.

Para el caso independiente del tiempo, lo que debemos hacer es buscar el estado fundamental de los arreglos de puntos cuánticos. Recordando algo sobre el modelo de Ising, lo primero que observamos es que no importa cómo evolucione el arreglo, sino hacia dónde evoluciona. Esto hace aún más interesante el modelo QCA, dado que podemos obviar una serie de operaciones que sería inabordable a poco que el arreglo aumentará de tamaño. La computación puede llevarse a cabo correctamente sin necesidad de controlar todos los detalles de la evolución del sistema, ésta se realiza preparando el sistema en un estado tal que la solución de su evolución corresponda a la de problema propuesto.

La necesidad de estudiar la dinámica del autómata celular no está asociada tanto a la realización de las operaciones como a la de averiguar la velocidad con que éstas serán llevadas a cabo. Por otra parte, existe la posibilidad de que bajo ciertas condiciones iniciales el sistema no alcance la solución, sino algún estado meta estable a medio camino entre ella y el estado inicial, y queremos saber si el estado final será alcanzado o no. Veamos como decidir cuándo una señal ha alcanzado el extremo del arreglo, o cuándo podemos decir que la operación ha sido finalizada.

ACOPLAMIENTO CON EL EXTERIOR

Nos centraremos en dos límites para el acoplamiento con el exterior:

1. La evolución (elástica) del sistema tiene lugar en una escala de tiempo mucho más larga que el acoplamiento (inelástico) entre el autómata y el medio exterior. Si el acoplamiento con el exterior es lo bastante alto como para forzar el tránsito al estado fundamental entonces la dinámica del sistema puede describirse mediante la tasa dada por la regla de oro pasa el **scattering** a partir del estado inicial, sin necesidad de saber qué ocurre en las etapas intermedias.

2. El otro límite, el acoplamiento (inelástico) con el exterior tiene lugar en escalas de tiempo mucho más largas que el acoplamiento (elástico) entre puntos. Esta situación hace aceptable la aproximación del sistema aislado, y el estudio de la evolución mediante la ecuación de Schrödinger:

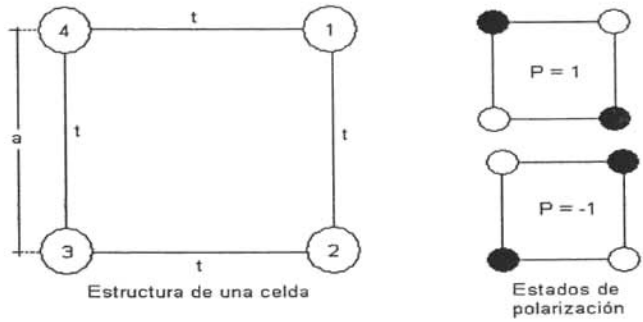
$$i\hbar \frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle$$

Una vez establecido que nuestro autómata evoluciona como n sistema aislado, resta decir que se sabe que es posible detectar el estado de carga de una celda de modo

no invasivo, desde el punto de vista clásico. Una medida siempre provocará la caída del estado cuántico sobre el subespacio asociado al valor encontrado, de modo que no podrá ser no invasiva desde el punto de vista cuántico. Aún así, en el QCA lo que se hace es medir el estado de las celdas de los bordes una vez que se ha alcanzado el estado de equilibrio, y esto se hace a lo largo de un intervalo de tiempo largo comparado con el de incertidumbre de los estados de cada celda, obteniéndose así un valor esperado.

DESCRIPCIÓN DEL AUTÓMATA CELULAR

En un autómata celular no asociaremos cada celda a un único punto cuántico, sino que haremos construcciones como la de la siguiente figura:



Celdas del autómata celular

Figura 11

En este caso el esquema para cada celda consiste en cuatro puntos cuánticos por cada celda. Hay otros modelos, como el que incluye un punto cuántico adicional en el

centro. En el interior de la celda hay dos electrones. No hay efecto túnel. A medida que las celdas se hacen más pequeñas, la separación entre niveles energéticos se hace mayor, lo que acelera la respuesta temporal de los sistemas.

Veamos los resultados obtenidos por Douglas y Lent, para lo que se hace necesario referirnos a su celda estándar. Esta celda parece mostrar un buen comportamiento. Para este caso, la distancia entre puntos (t, en la figura anterior) del interior de una celda es de 20nm, mientras que los centros de las celdas distan 60nm entre sí. Para esta construcción, la energía de efecto túnel es de 0.3MeV, mientras que el resto de parámetros fueron escogidos de acuerdo a los del GaAs.

El hamiltoniano empleado para el análisis de la evolución de tales sistemas fue el de Hubbard extendido:

$$H^{cell} = \sum_{i,\sigma}(E_0 + V_i)\bar{n}_{i,\sigma} + \sum_{i>j,\sigma} t_{ij}\left(\bar{a}^{t}{}_{i,\sigma}\bar{a}_{j,\sigma} + \bar{a}^{t}{}_{j,\sigma}\bar{a}_{i,\sigma}\right) + \sum_{i} E_Q \bar{n}_{i,\uparrow}\bar{n}_{i,\downarrow} + \sum_{i>j,\sigma,\sigma'} V_Q \frac{\bar{n}_{i,\sigma}\bar{n}_{i,\sigma'}}{\left|\bar{R}_i - \bar{R}_j\right|}$$

En este hamiltoniano no entran en juego los grados internos de libertad de la celda. Veamos lo que significa cada término:

1. Los operadores $\bar{a}_{i\sigma}$ y $\bar{a}^{t}{}_{i\sigma}$ destruyen y son electrones con spin σ en la posición i (son operadores de creación y aniquilación). Esto hace que el término $\bar{n}_{i,\sigma} = \bar{a}^{t}_{i,\sigma}\bar{a}_{j,\sigma}$ sea el operador número, que da el número de electrones con sipin σ que ocupan la i-ésima celda, y, por tanto $(E_0 + V_i)$ es la

energía de cada electrón. Así, el primer término de la ecuación es la energía de cada punto cuántico aislado. El potencial V_i es generado por las distribuciones de carga exteriores a la celda, de modo que es aproximadamente una constante dentro de ella.

2. El segundo término da cuenta del efecto túnel, con $t_{i,j} = 0.3MeV$, la energía de efecto túnel, y el término entre paréntesis el operador responsable de que el electrón j pase a la posición i o al contrario (destrucción de uno, creación del otro). Para salto en diagonal tomamos $t_{i,j} = 0$.

3. El tercer término expresa la energía necesaria para poner dos electrones con spines contrarios en el mismo punto cuántico, E_Q cada vez que esto ocurra.

4. El último término de la ecuación es puramente colombiano, y se refiere a la interacción entre electrones del interior de la misma celda.

La ecuación de Schrödinger independiente del tiempo:

$$\hat{H}^{cell}|\psi_i\rangle = E_i|\psi_i\rangle$$

Es la que nos permitirá encontrar el estado estacionario de la celda, Ahora nos queda elegir la base adecuada para tratar el problema. Los auto estados de $\hat{H}^{cell}$

serán en principio los de la base para dos electrones de spin contrario y cuatro posiciones:

$$\left\{ |\phi_1\rangle = \begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix} ; |\phi_2\rangle = \begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{vmatrix} \ldots |\phi_{16}\rangle = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{vmatrix} \right\}$$

En la fila superior de cada vector aparecen las posiciones ocupadas por electrones con spin up con un uno, y las no ocupadas de esta forma con un cero. Hacemos exactamente lo mismo para los electrones con spin down en la fila de abajo. Los números de columna corresponden a las posiciones con que numeré los puntos cuánticos en la figura anterior. Un electrón apuntando hacia arriba en la primera posición y otro apuntando hacia abajo en la tercera vendrían representados como:

$$|\phi\rangle = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{vmatrix}$$

En esta base el hamiltoniano es una matriz de 16×16, de la forma $\langle \phi_i | \hat{H} | \phi_j \rangle$, mientras que el estado fundamental de la celda viene expresado como:

$$|\psi_0\rangle = \sum_j \psi_j^0 |\phi_j\rangle$$

donde $|\phi_j\rangle$ son los distintos elementos de la base.

La base anterior puede sin embargo reducirse, teniendo en cuenta una serie de consideraciones. Al tomar efecto túnel despreciable, el número de electrones está restringido a dos por celdas. Dado que el término $t_{i,j}$ valía cero para posiciones enfrentadas por una diagonal, el estado fundamental esperamos que sea precisamente este para la celda. Estos son los dos estados de polarización contemplados a la derecha en la figura. Si la energía de efecto túnel se hace comparable a las energías de interacción culombianas del problema los electrones perderán rápidamente su estado de localización, y los estados de polarización dejarán de estar bien definidos. Así pues, para nosotros los términos de efecto túnel del hamiltoniano serán pequeños frente a los demás, y el estado del sistema muy próximo a los de la figura.

Definiremos la *polarización de la celda* como:

$$P = \frac{(p_1 + p_3) - (p_2 + p_4)}{p_1 + p_2 + p_3 + p_4}$$

donde $p_i = \langle \psi_0 | \bar{n}_i | \psi_0 \rangle$ es el valor esperado del operador número para la posición i en el estado fundamental $|\psi_0\rangle$, es precisamente esta función la que toma valores ± 1 para los estados de la figura. De ahora en adelante $P = 1$ equivale a un qubit "1", mientras que $P = -1$ equivale a un qubit "0".

Ahora veamos qué efecto tiene una celda sobre sus celdas vecinas. Los resultados de Douglas y Lent, para una serie de simulaciones, fueron los siguientes:

Partiendo de fijar el estado de una de las celdas (denominada celda de control, o de entrada), procedieron a buscar el estado fundamental de la celda adyacente directamente, por medio de la diagonalización de la descripción del autómata celular. El efecto resultó ser muy próximo a una función escalón, en la que P_2 toma valor 1 por pequeño que sea el valor de P_1, mientras este sea positivo, y toma valor -1 con cualquier valor negativo de P_1. Vemos que un valor muy pequeño de polarización se convierte inmediatamente en un valor extremo. Esto permite evitar que una señal se pierda por el camino cuando es transmitida por un hilo de celdas.

El siguiente paso fue precisamente simular el hilo de celdas, para lo que debíamos hacer algunas aproximaciones más si queríamos que el problema fuese tratable. Lo más simple fue la *aproximación entre células de Hartree*. En esta aproximación se incluyen los efectos de correlación e intercambio dentro de cada celda, pero se desprecia la posibilidad de que se produzcan entre celdas diferentes. Todo el efecto de las celdas vecinas se recoge en el potencial V_i del primer término de la ecuación de Schrödinger. Así podemos encontrar el estado fundamental de una celda examinando sólo el hamiltoniano local. El procedimiento escogido para conocer el estado de todas las celdas fue fijar la polarización de todas menos de la que se analiza, para a continuación hacer lo mismo con cada una de las demás. Esto se realiza iterativamente hasta el momento en que el estado de todas las celdas

permanezca sin cambios de una etapa a la siguiente. El inconveniente es que proceder así nos lleva al estado de equilibrio, pero no nos informa sobre la dinámica.

La evolución de un sistema como el anterior obedece a lo que puede verse a continuación:

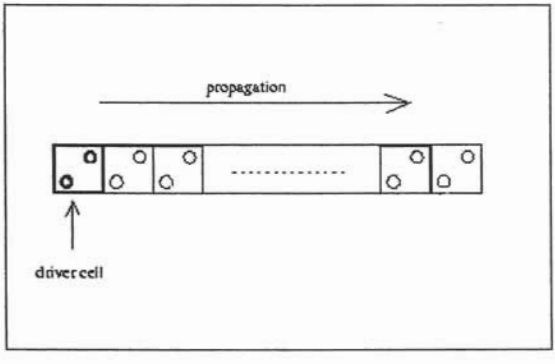


Figura 12. *Equilibrio en un array de celdas controlado.*

Lo que llama la atención es que el estado no se pierde, sino que avanza de una celda a otra. La celda sombreada es la de control, que mantuvimos en el estado $P=1$. La hipotética pérdida de polarización debida a cualquier efecto no será importante a menos que ésta se invierta, dado que cada celda amplifica P hasta su valor de saturación.

Si quisiéramos realizar una operación sencilla, tal como una inversión, podríamos recurrir a la siguiente estrategia:

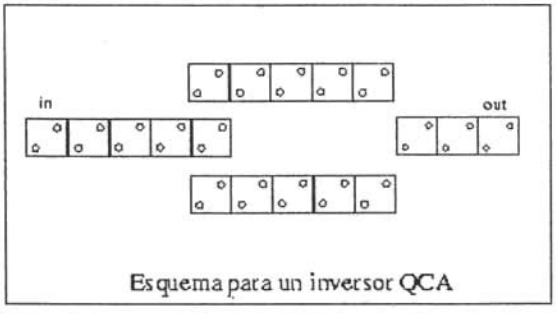


Figura 13. Esquema para inversión de una señal.

Pero no sólo necesitamos realizar operaciones sobre un único qubit, como sabemos. Aquí vemos una puerta generalizada en funcionamiento:

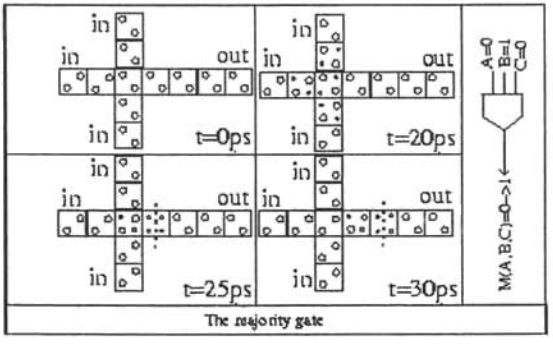


Figura 14. Puerta generalizada en QCA.

Con estas operaciones es claro que podríamos, en principio realizar cualquier operación más complicada. Por otra parte, vemos que lo único que debemos hacer es introducir las entradas adecuadas desde las líneas conectadas a los bordes del autómata.

Una limitación básica para la construcción del QCA es la puramente tecnológica. En primer lugar, nos enfrentamos a la necesidad de crear un arreglo de puntos cuánticos, que son de por sí nanométricos, en el que las distancias entre unos y otros lo deben ser también. Este problema, a pesar de todo, no parece excesivamente importante, dado que se trata de simple miniaturización, la búsqueda de una técnica que haga posible reproducir a escala muy pequeña un patrón sencillo. Dado que la construcción de puntos cuánticos es factible en la práctica, es razonable pensar que este tipo de construcciones lo llegarán a ser también.

El otro problema surge cuando nos proponemos por un lado controlar todas las entradas, cada una de las cuales tiene escala nanométrica, pero necesita un dispositivo capaz de polarizarla adecuadamente para preparar el estado inicial y cada salida, donde necesitamos realizar medidas sobre todos las celdas de un lado del arreglo. Si tratamos de realizar operaciones en el sentido descrito antes debemos enfrentarnos a saber que filas interactúan con que columnas, y necesitamos controlar exactamente las entradas y salidas correspondientes, lo que significa ser capaces de manipular y leer las entradas y salidas de una en una, al tiempo que sincronizarlas. Esto es técnicamente más complicado, y está relacionado con el problema de la interconexión.

COMPUTACIÓN MOLECULAR

Las cosas han cambiado mucho desde las primeras computadoras electrónicas. El ENIAC I fue desarrollado en la Universidad de Pennsylvania en 1945. Estaba compuesto por más de 70,000 resistencias, 18,000 válvulas y 10,000 condensadores; pesaba 30,000 Kilos y ocupaba 1.300 metros cuadrados.

Pero el descubrimiento del chip, a mediados de los años setenta, ha reducido, por suerte para todos, el tamaño de las computadoras. El primer 486 utilizaba tecnología de una micra (millonésima parte de un metro). Hasta hace poco tiempo, los Pentium tradicionales utilizaban tecnología de 0.35 y 0.25 micras. Los modelos más modernos han reducido este valor hasta 0.13 micras. El nanómetro marcará el límite de reducción a que podemos llegar cuando hablamos de objetos materiales, en este caso dispositivos computacionales.

La velocidad de las computadoras y su capacidad de almacenamiento han sido las principales barreras en el desarrollo de la inteligencia artificial. Con la nanotecnología aparece la posibilidad de compactar la información hasta límites inimaginables y crear chips con memorias de un terabit por centímetro cuadrado. Un Terabit es la capacidad de la memoria humana, lo que quiere decir que las computadoras del futuro podrán llegar a tener inteligencia propia, es decir, serán capaces de aprender, tomar decisiones y resolver problemas y situaciones "imprevistas", ya que con esta memoria se les podrá dotar de códigos extremadamente complejos. Según los

expertos, esto se puede conseguir en un plazo de no más de cinco años. Lógicamente, con computadoras tan pequeñas, los dispositivos de uso también cambiarán. Al tiempo que evoluciona la tecnología de reconocimiento de voz y de escritura, se irán desarrollando otro tipo de "computadoras personales" en miniatura, casi invisibles, insertados en objetos de uso común como un anillo, por ejemplo, o implantados en nuestro propio organismo en forma de lentillas o chips subcutáneos.

También es necesario fabricar otros conductores, porque los existentes no sirven. Los experimentos con nanotubos de carbón (milmillonésima parte de un metro) para la conducción de información entre las moléculas ya han dado resultados. IBM anunció que ha conseguido crear un circuito lógico de ordenador con una sola molécula de carbono, una estructura con forma de cilindro 100,000 veces más fino que un cabello. Este proyecto permite introducir 10,000 transistores en el espacio que ocupa uno de silicio.

La posibilidad de desarrollar miniordenadores de cien a mil veces más potentes que los actuales podría suponer que éstos tuvieran inteligencia propia, lo que cambiaría los sistemas de comunicaciones. Por ejemplo, los datos podrían transmitirse con imágenes visuales mediante "displays" incorporados en forma de lentillas. La comunicación telefónica se realizaría por audioconferencias en 8 o 10 idiomas.

En un futuro no muy lejano, las PCs estarán compuestas, en lugar de transistores, por otros componentes como las moléculas, neuronas, bacterias u otros métodos de

transmisión de información. Entre estos proyectos se encuentra la futura computadora "química", desarrollada por científicos de Hewlett-Packard y de la Universidad de California (Los Ángeles). Los circuitos de este nuevo modelo son moléculas, lo que supone transistores con un tamaño millones de veces más pequeños que los actuales.

Esto es uno de los aspectos más interesantes ya que no sólo se podrán desarrollar máquinas mucho más pequeñas que una bacteria o una célula humana. Además, se puede empezar a tomar elementos del mundo biológico –por ejemplo, trocitos de ADN para procesadores de computadoras–. Así, científicos del grupo de investigación Montemagno de la Universidad de Cornell han logrado unir ya elementos biológicos y mecánicos creando pequeños motores del tamaño de un virus. Aunque aún faltan muchas cosas por afinar, estos motores podrían trabajar en el interior de una célula humana.

Dispositivos nanoinformáticos

Usando nanotubos semiconductores, investigadores de varias empresas y laboratorios han desarrollado circuitos de computación de funcionamiento lógico y transistores, las puertas electrónicas lógicas de que están compuestos los chips.

En lo que es considerado un paso fundamental hacia la computadora molecular, IBM mostró el primer circuito de ordenamiento lógico formado por nanotubos de carbono.

Las computadoras moleculares basadas en estos circuitos tienen el potencial de ser mucho más pequeñas y rápidas que las actuales, además de consumir una cantidad considerablemente menor de energía.

El transistor se enciende y se apaga -recordemos el 1 y el 0 del sistema binario, que forma la base de la informática- más de mil millones de veces por segundo, un 25% más veloz que los transistores más recientes. Para el 2007, Intel espera estar fabricando chips conteniendo mil millones de estos transistores, lo que le permitiría llegar a una velocidad de 20 Ghz. con la energía de un voltio.

En cuanto a memorias, IBM pretende crear capacidades mayores a las existentes, se basa en procesos de escala nanométrica. Este dispositivo de almacenamiento regrabable, de alta capacidad y densidad, trabaja en base a mil pequeñas agujas similares a las del microscopio AFM, con puntas capaces de tocar átomos individuales y escribir, leer y borrar así grandes cantidades de información en un espacio mínimo. De apenas nueve milímetros cuadrados, los investigadores de IBM estiman que en los próximos años, la tecnología Millipede puede superar la capacidad de la tecnología de memoria Flash en cinco veces o más.

Este tipo de desarrollos -tanto los nanotransistores, como las nanomemorias- pueden ser cruciales para absorber las crecientes e inmensas capacidades de procesamiento y memoria que demandan los desarrollos multimedia, más aún

cuando se observa que de aquí a máximo diez años la tecnología actual de semiconductores habrá agotado sus posibilidades de crecimiento.

En cuanto a alimentación, la corporación japonesa NEC, junto a otros institutos de investigación; ha anunciado el desarrollo de una célula de carburante con una capacidad diez veces mayor que una batería de litio, pero de tamaño diminuto, en lo que constituye otra aplicación de los nanotubos de carbono, esta vez como electrodos. En el futuro próximo, esta batería le podría permitir a dispositivos portátiles, como las notebooks, funcionar varios días seguidos sin conectarse a la corriente.

Los desarrollos en Nanotecnología se están aplicando también a los sistemas de seguridad. Los cuales pueden utilizarse para probar la autenticidad de pasaportes y otros documentos y tarjetas, con el fin de evitar el pirateo.

Este chip podrá utilizarse también en tarjetas de débito, carnés, matrículas de automóviles, permisos de conducir, discos compactos, DVD, programas informáticos, títulos y valores, bonos, libretas bancarias, antigüedades, pinturas, y otras aplicaciones en las que se necesite comprobar la autenticidad.

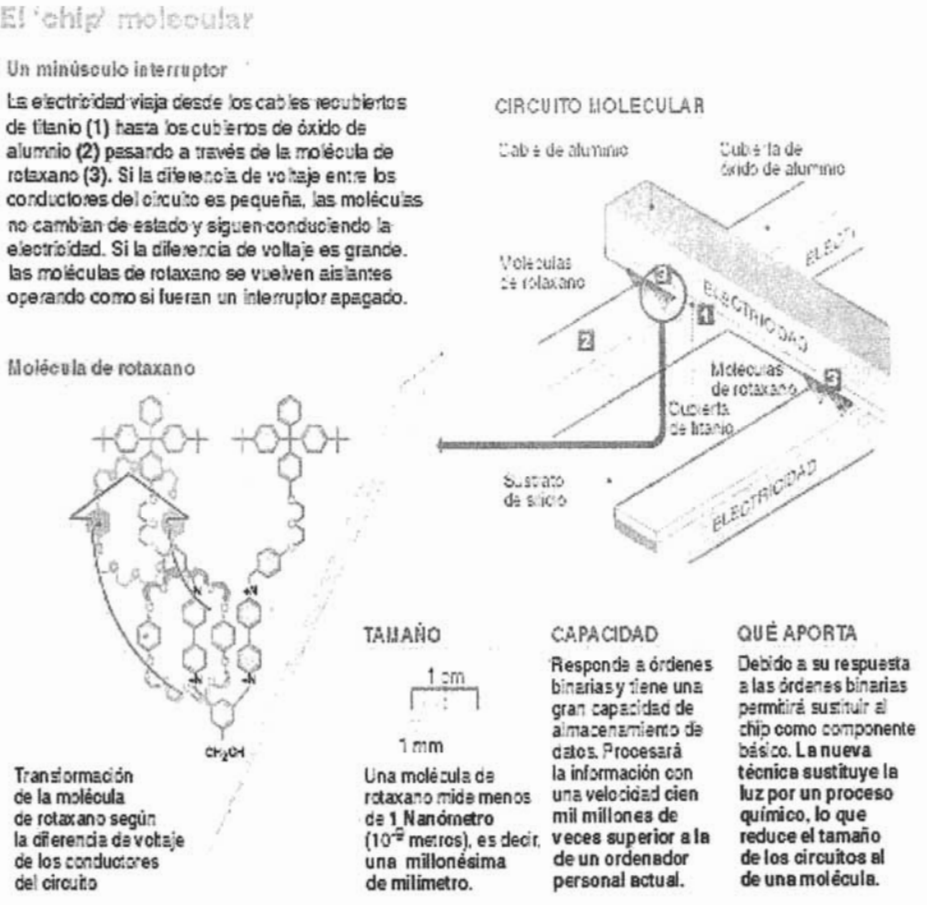


Figura 15.

Las aplicaciones más inmediatas de la Nanotecnología se dirigen al sector de la exploración espacial. Entre éstas, podemos hablar de bases de lanzamiento de gran altitud, estaciones espaciales, vehículos ligeros y muy resitentes, naves personales para viajar por el espacio o los conocidos nanosatélites, como el NANOSAT, un proyecto de desarrollo de un nanosatélite español, iniciado en 1995.

El NANOSAT parte de un concepto ideado en el INTA y cuya gestión y construcción se realiza totalmente en España, partiendo de una nueva filosofía de diseño: más pequeño, más potente, más rápido, con una aplicación específica concreta, con mayores prestaciones y menor consumo.

Por otro lado aunque todavía no se han fabricado nanorobots, existen múltiples diseños de éstos, incluso no pueden ser del todo robots es decir pueden hasta ser modificaciones de células normales llamadas también células artificiales. Las características que éstos deben de cumplir, entre las que se pueden mencionar:

Tamaño.- Como el nombre lo indica, los nanorobots deben de tener un tamaño sumamente pequeño, alrededor de 0.3 micras ($1micra=1x10^{-6}$).

Componentes.- El tamaño de los engranes o los componentes que podría tener el nanorobot seria de 1 a 100 nanómetros ($1nm=1x10^{-9)}$ y los materiales variaría de diamante como cubierta protectora, hasta elementos como nitrógeno, hidrógeno, oxigeno, fluoruro, silicón utilizados quizás para los engranes.

Velocidad de procesamiento.- El procesador central del nanorobot solo poseerá una velocidad de 106-109 operaciones por segundo, por lo tanto una mayor inteligencia de procesamiento no será requerida.

El ensamblador.- Se le ha dado el término de "ensamblador" a aquella pieza del nanorobot que es semejante a un brazo submicroscopico, cuyas características principales son las de construir a discreción la materia, reaccionar con compuestos, construir secuencias de moléculas y quizás la de copiarse a sí mismo, teniendo con esto la capacidad de autoreplicarse. Se le puede comparar con los ribosomas, las organelas encargadas de la trascripción y traducción de proteínas. Según los recientes diseños el brazo del ensamblador seria de diamante, de 100 nm de largo por 30 nm de diámetro. Todo esto suena muy complejo, pero cuando se llegue a la tecnología para fabricarlo será relativamente económico.

La clave para la manufactura con estos ensambladores a gran escala es la auto-reproducción. Un robot de tamaño nano haciendo trabajos en madera en tamaño nano puede ser dolorosamente lento. Pero si estos ensambladores se pueden reproducir así mismos, podemos tener trillones de ensambladores trabajando al unísono. Entonces no tendríamos límites para el tipo de cosas que quisiéramos crear. "No solo el proceso de fabricación se transformará, sino todo el concepto del trabajo..

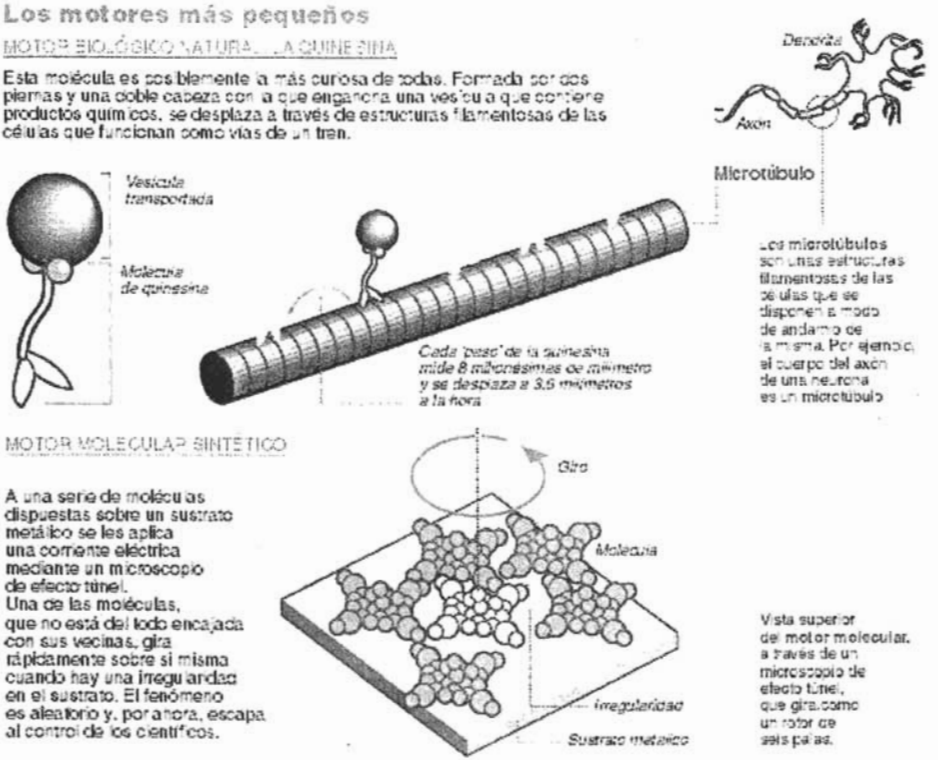


Figura 16.

La nanotecnologia al aplicarse a la medicina se le conoce como nanomedicina. Con la descripción de los nanorobots, se puede intuir que la utilidad de éstos en las ramas medicas será muy importante. Para empezar los nanorobot medirán de alrededor de 0.5-3 micras, por lo cual podrán flotar libremente por los vasos sanguíneos. Las principales aplicaciones de estos será la interacción de los nanorobots con las células sanguíneas (eritrocitos y leucocitos) en la reparación de los tejidos, la cura del cáncer o SIDA y la posible terapia de enfermedades genéticas.

Sin lugar a dudas la nanotecnologia cambiara en gran medida a la medicina, ya que aunque la medicina de hoy comprende que la mayoría de las enfermedades se deben a cambios estructurares en las moléculas de las células, dista mucho ahora de corregirlas. Esto es el caso con el cáncer ya que se sabe que se debe a una reproducción anormal de un tejido, pero la solución sigue siendo extirpar el tejido afectado, seguimos dando soluciones macroscópicas, sin resolver las microscópicas y este tipo de problemas es de lo que sé encarga de resolver la nanomedicina.

Por lo tanto, la nanotecnología puede significar el final de las enfermedades como la conocemos ahora. Si pesca un resfrío o se contagia de SIDA, sólo tendrá que tomar una cucharada de un líquido que contenga un ejército de nanorobots de tamaño molecular programados para entrar a las células de su cuerpo o combatir los virus. Si sufre una enfermedad genética que azota a su famila, al ingerir algunos nanorobots que se introducirán en su ADN, repararán el gen defectuoso. Inclusive la cirugía plástica tradicional será eliminada, ya que nanorobots médicos podrán cambiar el color de sus ojos, alterar la forma de su nariz, y más aún, podrán hacerle un cambio total de sexo sin el uso de cirugía.

Por otro lado el sistema inmune de nuestro cuerpo es el encargado de proporcionar defensas contra agentes extraños o nocivos para nuestro cuerpo, pero como todos los sistemas éste siempre no puede con todo. Entre estas deficiencias se encuentra que muchas veces no responde (como es el caso con el SIDA) otras veces sobreresponde (en el caso de enfermedades autoinmunitarias). Cabe decir que los

nanorobots estarán diseñados para no provocar una respuesta inmune, quizás las medidas que tienen estos bastaran para no ser detectados por el sistema inmune. La solución que ofrece la nanomedicina es proporcionar dosis de nanorobots para una enfermedad específica y la subsiguiente reparación de los tejidos dañados, substituyendo en medida a las propias defensas naturales del organismo.

Una de las aplicaciones inmediatas que se planea alcanzar con la nanomedicina es la de hacer un diseño que mejore la funcionalidad de la hemoglobina, la proteína encargada de la transportación de oxígeno y dióxido de carbono en los tejidos, la cual se encuentra en el eritrocito. Hoy en día hay avances en este campo, siendo los principales investigadores Chang y Yu los cuales están desarrollando un nuevo sistema basado en la encapsulación de hemoglobina a través de nanocápsulas.

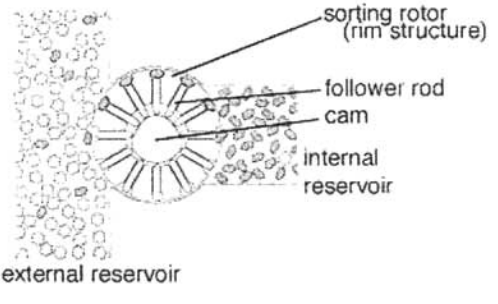


Figura 17.

En la figura se muestra un diseño de un nanoinvento el cual se encuentra en un pulmón, se observa un rotor el cual va a acarrear él oxigeno por diferencia de las

presiones parciales del oxigeno ya que por fuera hay mayor cantidad que adentro por lo tanto el nanoinvento va a introducir él oxigeno en un pequeño tanque. Todos estos procedimientos van a ser controlados por él medico, se supone que mediante mecanismos de ondas de baja frecuencia que el nanoinvento los interpreta como comandos a seguir. Este procedimiento será el mismo a nivel periférico. La utilidad de esto es que estos aparatos proporcionaran alrededor de un almacén de 530 litros de oxigeno aumentando 2000 veces el almacenamiento de oxigeno comparado con la hemoglobina.

Sin embargo también tenemos el termino de biostasis se aplica a la capacidad de tener un tejido que se mantenga en condiciones estables durante un lapso de tiempo indefinido. También es sinónimo de criogenia ya que para este tipo de método se propone utilizar alguna sustancia que vitrifique o congele los tejidos a fin de protegerlos. Este método es una esperanza para las personas que tienen alguna enfermedad que no puede ser curada en su tiempo. Aunque esta técnica por ahora no se le puede relacionar con la nanotecnologia, en un futuro sí, ya que la idea es reparar los tejidos de la persona en un futuro, y los nanorobots van a ser los encargados de este trabajo.

Aunque aun los médicos no se ponen de acuerdo si la resucitación del paciente puede ser viable, los investigadores de este tema sostienen que en un futuro se tendrán las técnicas para lograr hacer esto.

Otra de las expectativas que se pueden lograr con la nanomedicina será sin duda la modificación de material genético humano y por consiguiente la cura de las enfermedades genéticas asociadas. Aunque la ingeniería genética es la que se encarga de la investigación en especial de esta molécula, la nanotecnología va a ser la encargada de proporcionar las herramientas necesarias para la manipulación de tan preciada molécula.

Una de las cuestiones a superar para poder pensar en un ejemplar biónico tiene que ver con el tamaño de los componentes de ese sistema maravilloso que es el cuerpo humano. Una increíble multiplicidad de funciones tienen lugar en partes del sistema imposibles de reproducir... hasta ahora.

Cuando el cuerpo realiza un movimiento, digamos por ejemplo tomar una copa de cristal, está cumpliendo muchas y muy complicadas funciones al mismo tiempo, de las cuales en su mayoría ni siquiera tenemos conciencia. Mover los músculos de cinco dedos al mismo tiempo, a la vez que censamos la presión necesaria para sostener la copa sin dejarla caer pero sin romperla. Pero eso no es todo: mientras tomamos la copa, seguimos usando otros sistemas como el auditivo y el visual, mantenemos el equilibrio corporal, respiramos, medimos el nivel de glucosa, procesamos alimentos, etc., etc. ¿Cómo instalar componentes que cumplan esas funciones en espacios tan pequeños, y guardando las formas anatómicas?

El primer paso fue la reducción de los procesadores hasta convertirlos en micro-procesadores, pero eso no es suficiente. La Nanotecnología entra entonces en escena. Esta disciplina tiende a reducir los componentes a un tamaño increíblemente pequeño. El objetivo es reunir un grupo de funciones -que podríamos llamar lógicas- en reacciones dentro de un compuesto ideado para provocar los efectos deseados, en este caso, ciertas tareas. Este nano-componente realiza sus funciones de manera independiente, es decir, tiene un alto grado de autonomía. El reducido tamaño de estos elementos hace necesaria la intervención de robots que aportan su altísima precisión para su construcción.

Capítulo 5

Aplicaciones

Todas las cualidades del átomo de la física moderna, que sólo puede simbolizarse mediante una ecuación en derivadas parciales en un espacio abstracto multidimensional, son inferidas; no se le puede atribuir directamente propiedad material alguna. Así pues, cualquier representación suya que pueda crear nuestra imaginación es intrínsecamente deficiente; la comprensión del mundo atómico de ese modo primario y sensorial... es imposible

(Werner Heisenberg)

TELEPORTACIÓN

La utilización de un haz de taquiones[11] como sistema de comunicaciones ofrece unas perspectivas interesantes cuando se aplica al problema de transportar masa a velocidades lumínicas. En *El mundo al final del tiempo* de Frederick Pohl, se nos habla de la existencia de unas entidades de plasma que mora en el interior del núcleo de las estrellas. Dichas entidades gastan su tiempo en un entretenimiento muy divertido: enviar haces de gravitones hacia estrellas donde suponen residen semejantes suyos para hacerlas implosionar y convertirlas en novas. Eso determina que tengan que desplazarse a menudo entre diferentes estrellas para evitar tan molesto ejercicio de tiro al blanco. Para ello, lo que hacen es "codificarse" utilizando un haz de taquiones rápidos de baja energía y transportarse de este modo en forma de información en dirección al destino final de su viaje.

Este procedimiento recuerda mucho a lo que normalmente se conoce como teleportación. La teleportación se basa en un hecho bien conocido: la materia no puede viajar a la velocidad de la luz, pero la información si. Por tanto, si queremos trasladar un objeto desde el punto A al punto B, un procedimiento puede consistir en descomponer ese objeto en los átomos individuales que lo integran y enviar a la estación de destino la información sobre la posición y el tipo de cada uno de esos átomos. Con esa información, en el destino se procede a reconstruir el objeto

[11] Un taquión es un a partícula hipotética cuya velocidad supera a la de la luz. Las propiedades que tendría una partícula así se obtienen analizando las expresiones de energía y momento que aparecen en la Relatividad general.

transmitido a partir de las instrucciones reflejadas en el mensaje como si de un mecano se tratase.

Son muchas las novelas y series en las que se usan regularmente los teleportadores. La más emblemática, sin duda, es la serie de *Star Trek*, donde los teleportadores han asumido el papel de sistema de transporte de corto alcance para desplazar personal entre naves y hacia la superficie planetaria sin necesidad de usar lanzaderas convencionales. Larry Niven también usa tele portadores en su celebre novela *Mundo anillo*, donde el protagonista lleva a cabo una curiosa vuelta a la Tierra usando las cabinas locales de teleportacion en un viaje que resulta imposible a menos que nuestro planeta gire en sentido contrario al que realmente lo hace.

En otras ocasiones, los teleportadores forman parte integrante de un sistema de transporte y comunicaciones de largo alcance. Por ejemplo, en *Hyperion*, de Dan Simmons, los teleyectores forman una red que conecta todos los mundos colonizados y permite el libre desplazamiento de personas y mercancías entre los mismos. Los teleyectores de Simmons están gobernados por el Tecnonucleo, un conjunto de inteligencias artificiales que aportan a potencia de cálculo que un proceso de teleportacion precisa al tiempo, pero no precisamente de un modo altruista. En la novela de Charles Sheffield *La caza del Nimrod*, el Enlace Mattin es utilizado por la humanidad para expandirse a través de la galaxia hasta conseguir explorar una burbuja de unos cincuenta años luz en torno a la Tierra. Para ello siguen una estrategia sencilla pero eficaz: envian naves subluminicas dotadas de

receptores de Enlace Mattin en todas direcciones, de modo que cuando dichas naves llegan a un sistema solar que puede resultar interesante a efectos de colonización o de comercio, se establece una conexión con la base original y se añade un nuevo nodo, definido por sus coordenadas, a la red de tele portadores existentes. A partir de ese momento es posible la transmisión instantánea de materia e información hacia el nuevo mundo contactado. El mismo esquema de expansión a base de naves subluminicas para la creación de estaciones de teleportacion lumínicas o súper lumínicas aparece en una de las obras mas celebres del genero, la conocida *Estación de Transito*, de Clifford D. Simak, en la que se nos narran las experiencias de Enoch Wallace, guardián de una de esas estaciones en una Tierra que desconoce su existencia

La teleportacion no es un proceso exento de inconvenientes. El primero es, sin duda, el principio de incertidumbre de Heisenberg, quien demostró que es imposible conocer al mismo tiempo la posición y la cantidad de movimiento de una partícula a nivel cuántico: se podría conocer una o la otra, pero nunca las dos. Esto significaba que si se escaneasen todos los átomos que forman parte de nuestro cuerpo existiría una clara imprecisión, y el resultado de dicho escaneo no se correspondería al cuerpo que había sido originalmente explorado. Otro factor a tener en cuenta es la energía de desmaterialización. Nosotros mantenemos una existencia física tangible porque existe una energía que une nuestros átomos. Evidentemente si queremos desmaterializar algo tendremos que eliminar esa energía, para poder ir recogiendo cada átomo y determinar sus características. Pero resulta que la energía de

desmaterialización asociada a un cuerpo humano seria la asociada a una explosión atómica de un megatón de potencia, algo ciertamente a tener en cuenta al operar la maquina. Tampoco es despreciable el volumen de información asociado a está operación. En efecto, la determinación de la posición, la velocidad, el estado y el tipo de cada uno de los átomos que forman parte de nuestro cuerpo, equivaldría a unos 10^{28} bits de información, una cantidad de datos astronómica, sin duda. Pero lo más curioso es la existencia de una serie de problemas morales de muy difícil solución. Si el proceso de escaneado no destruye automáticamente el original, en un momento existirán dos copias idénticas del objeto transportado, una en el origen y otra en el punto de destino. Y si bien el transporte de objetos inanimados no tendría mayores dificultades, cuando son personas lo que se transporta las preguntas se multiplican. ¿No seria un asesinato la desmaterialización del original en la estación de origen?. ¿Qué sucede si el original no es destruido y se produce una duplicación?. ¿Se puede reconstruir la mente del que se transporta simplemente apilando los átomos originales en las posiciones correctas que ocupaban?. En "Piensa como un dinosaurio" de James Patrick Kelly se hace un estremecedor análisis de algunas de estas implicaciones sobre el teletransporte de seres humanos cuando en una de estas maquinas se produce un fallo mecánico y el original no resulta destruido durante el proceso de transporte.

En contra de lo que pudiera pensarse, la teleportación es un proceso completamente al alcance de nuestra tecnología. En 1993 un equipo de investigación consiguió tele portar fotones utilizando una característica fundamental de la mecánica cuántica: el

entrelazamiento. El entrelazamiento es una propiedad que exhiben determinadas partículas a nivel cuántico en virtud de la cual lo que sucede a una de ellas le sucede automáticamente a la otra. Y lo que es más importante, la transferencia de información entre ambas es instantánea. El entrelazamiento fue presentado en 1935 por Einstein, Rosen y Podolski como parte de un experimento mental destinado a demostrar que la teoría cuántica estaba incompleta y no funcionaba adecuadamente. Sin embargo, posteriormente parece haberse demostrado que la fantasmal transferencia de información que tanto molestaba a Einstein tiene lugar realmente.

¿Cómo puede utilizarse el entrelazamiento cuántico para producir un mecanismo de teleportación?. Para llevar a cabo la teleportación cuántica, primeramente se crean un par de fotones ERP. Nosotros sabemos que de acuerdo con la propiedad de entrelazamiento que tienen, lo que le sucede a un fotón le sucederá automáticamente al otro. El problema es que de acuerdo con el principio de incertidumbre nosotros no podemos mirar en qué estado se encuentra el fotón, porque en el mismo momento en que lo hagamos lo destruiremos. Esto es precisamente lo que impide usar estos curiosos pares ERP como sistema de comunicaciones instantáneo. ¿Cómo podemos solucionar este problema? Supongamos que queremos transportar un determinado fotón, y que disponemos para ello de dos fotones entrelazados que pueden estár tranquilamente situados en extremos diferentes de la galaxia. El truco de la teleportación consiste en combinar el fotón a transportar con uno de los pares ERP, el situado en la estación de origen, y a continuación medir la polarización relativa de ambos fotones. ¿Qué significa esto?

Con está estrategia no estamos haciendo una medida absoluta, sino indirecta de las propiedades del fotón, con lo cual no estamos vulnerando el principio de incertidumbre de Heisenberg. Está medida es lo que se conoce como "estado de Bell" y la información de la misma se transmite al punto de destino por métodos convencionales, como pueda ser una señal de radio. ¿Cuál es el paso siguiente?. La alteración derivada de la combinación del fotón que queremos transportar con el extremo del par ERP que tenemos en el origen se ha transmitido instantáneamente desde el mismo hasta el punto de destino. Sin embargo, el operador que se encuentra en el punto de destino no sabe lo que ha sucedido, porque no tiene modo de saber cual es el estado de Bell asociado a esa alteración. Cuando llega la información de la medida del estado relativo de ambos fotones por el canal convencional, el señor que está en la estación de destino puede aplicar la transformación correspondiente para obtener un fotón que tenga exactamente las mismas características del que utilizamos en el punto de origen... con lo que la teleportación del fotón ha concluido.

Aun cuando pueda parecer que con este proceso solo se transporta una propiedad del fotón, como es la polarización, en la práctica lo que se están transfiriendo son todas las características del fotón de origen, de modo que lo que obtenemos como salida en el punto remoto es una copia idéntica del mismo. Esto es debido a que tiene las mismas propiedades y la misma función de estado: a nivel cuántico, no hay manera de distinguir el fotón que entró del fotón que salió.

La teleportación cuántica a nivel fotónico es un hecho. El día de hoy, existen muchos laboratorios en el mundo donde han conseguido la teleportación de fotones de un sitio a otro a una distancia arbitrariamente grande. Existe así mismo un laboratorio francés que ha conseguido entrelazar cuánticamente átomos, con lo cual podemos considerar que la teleportación de los mismos se encuentra ya casi a la vuelta de la esquina. No es descabellado prever que la teleportación de moléculas más o menos complejas pueda tener lugar dentro de los próximos 10 años. Lo que pueda venir después de este hito, es algo que lógicamente no conocemos...

Se ha demostrado que la teleportación cuántica implica automáticamente la destrucción del fotón que se introduce en el tele portador. Es decir, no existe lo que se denomina la clonación cuántica, que nos serviría para vulnerar el principio de incertidumbre. Sin embargo, tampoco es un proceso exento de problemas Uno de los más importantes es lo que se conoce como decoherencia. La decoherencia es la perturbación de la fuente de origen debido a cualquier tipo de actuación externa, por ejemplo, la radiación térmica procedente de la cámara en la cual tiene lugar la experiencia. Este fenómeno puede alterar el estado cuántico de los pares ERP y hacer que la teleportación no tenga lugar. De hecho, el porcentaje más alto de teleportación que se ha conseguido a día de hoy está en un 80% de los casos lo que esta bien para el laboratorio, pero es inaceptable para una aplicación real. La decoherencia es un problema importante, cuya magnitud crece conforme aumenta el número de átomos que queremos transportar a través de este procedimiento, y que

puede constituir un obstáculo casi insalvable para la teleportacion de grandes objetos macroscópicos

El tele transporte es en esencia lo que su propio nombre indica. Puede no ser necesario enviar un qubit para hacer llegar información de un punto a otro.

Supongamos que tenemos dos usuarios, donde el usuario 1 esta interesado en hacer saber al usuario 2 el valor de un qubit particular, digamos $|\phi\rangle = |0\rangle$, que el usuario 1 conoce. No necesariamente hay que hacer llegar el qubit $|0\rangle$ al usuario 2. la posibilidad que pasa por medir antes el qubit, de todas formas, en caso de que éste fuera desconocido para el usuario 1 y de enviar después la inflación destruiría el estado inicial. Además de que un estado no se puede copiar si no es conocido. Así que el usuario 1 siempre conoce el estado del qubit.

El tele transporte cuántico, utiliza el entrelazamiento para resolver estas dificultades, veamos como:

Supongamos que el usuario 1 y el usuario 2 comparten un par entrelazado en el estado $\left(|00\rangle + |11\rangle / \sqrt{2}\left(|00\rangle + |11\rangle\right)\right)$. El usuario 1 pretende transmitir al usuario 2 un qubit en un estado desconocido. Este estado será representado como:

$$|\phi\rangle = a|0\rangle + b|1\rangle$$

El estado inicial de los tres qubits será:

$$[a|0\rangle + b|1\rangle] \otimes \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] = \alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle$$

desde luego, normalizado. El usuario 1 mide en la base de Bell los primeros dos qubits, que son aquél que es en principio desconocido, y que se desea transmitir, y su parte del par entrelazado. Esto se puede hacer mediante el esquema de la siguiente figura:

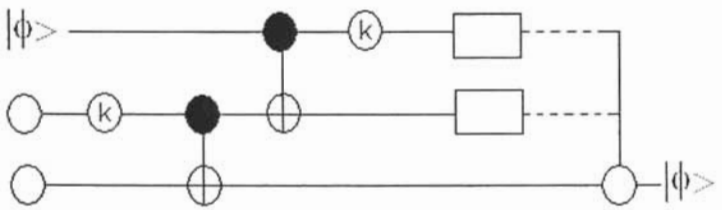


Figura 18. *Dispositivo para teletransporte cuántico*

Primero el usuario 1 aplica las operaciones XOR y de Hadamard, y después de esto el estado resultante es:

$$|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

inmediatamente después mide sus qubits. De acuerdo al postulado de la medida, el estado inmediatamente a continuación de ésta es el colapso sobre uno de los cuatro

estados de la base de Bell, que contiene dos bits de información. Enviamos estos dos bits al usuario 2, que con ellos será capaz de decidir que operación $\{I, X, Y, Z\}$ debe aplicar a su qubit, para pasarlo al estado $|\phi\rangle = a|0\rangle + b|1\rangle$. Así el usuario 2 ha sido capaz de recuperar el qubit sin que éste fuese en sí transmitido.

No es posible clonar un estado que no se conoce, y no se ha podido hacer llegar al usuario 2 el qubit sin que el usuario 1 lo perdiese. Por otra parte, $|\phi\rangle$ contiene información completa sobre el estado del qubit del usuario 1, de modo que no se ha perdido información. De estos dos hechos se deriva que el término teletransporte sea adecuado para esta situación.

CRIPTOGRAFÍA CUÁNTICA

Las comunicaciones forman parte de los sistemas computacionales hasta el punto de que éstos no son posibles sin ellas, lo contrario no ocurre, habiendo así un nivel de aplicabilidad que justifica por completo el desarrollo de esta técnica en ausencia de la computadora cuántica. Podemos utilizar mecanismos cuánticos de codificación para asistir la comunicación entre computadoras electrónicas o entre usuarios humanos que, por ejemplo, hablan por teléfono.

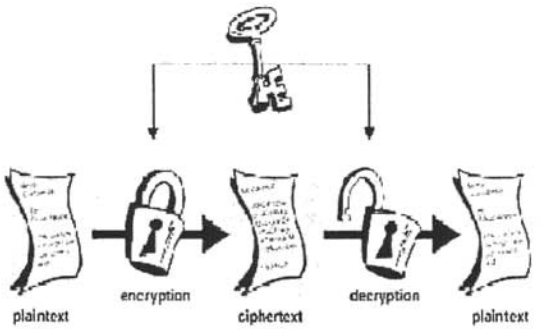


Figura 19

Para que podamos comprender este termino veamos a que se refiere la criptografía en las computadoras convencionales.

Un ejemplo habitual de problema que no es computable es la descomposición en factores primos. Un número que no sea primo se puede expresar como producto de números primos, naturalmente más bajos. Podemos ir dividiendo el número que tenemos que factorizar sucesivamente por los enteros menores que él, hasta encontrar uno que de resto cero. Procederíamos entonces de este modo con los factores encontrados, y así sucesivamente, hasta que el problema quede resuelto. Como vemos esto suena muy bien, hasta que nos enfrentamos a la posibilidad de que los factores primos sean también números grandes.

Los mejores métodos conocidos en la actualidad requieren 42 días a 10^{12} operaciones por segundo para factorizar un número decimal de 130 dígitos, pero si duplicamos L, el tiempo aumenta en un factor 10^{25}, es decir, un millón de años.

El hecho de que la factorización sea un problema intratable ha sido utilizado como base para los sistemas criptográficos modernos, tales como el RSA (Rivest, Shamir y Adleman). Para cualquier mensaje, podemos obtener fácilmente una versión encriptada.

$$E = M^s \bmod(c)$$

donde s y c son dos números enteros grandes, que pueden darse a conocer. El modo de desencriptar el mensaje consiste en calcular:

$$M = E^t \bmod(c)$$

donde el valor de t puede obtenerse sin problemas a partir de s y de los factores de c. Se suele utilizar $c = pq$, donde p y q son dos números primos grandes, conocidos sólo por quien publicó el valor de c. El usuario que conoce p y q es el único que puede leer los mensajes, mientras que cualquier otro puede enviárselos de manera segura.

El método anterior de comunicación es considerado actualmente seguro, el RSA, este método, al igual que todos los que actualmente existen resisten todos los ataques, basan su fiabilidad en la clase a la que pertenece el problema de descomponer un número en factores primos: no existen computadoras capaces de descifrar un mensaje de este tipo sin la clave primaria en un tiempo razonable. Pero

a la luz del método desarrollado por Shor vemos que la existencia de la computadora cuántica rompería por completo la seguridad de los códigos actuales. Esto quiere decir que, en ausencia de las computadoras cuánticas, emplear una tecnología más cara para resolver un problema que en la práctica no existe resulta como mínimo inadecuado. ¿Por qué entonces hacerlo? Básicamente porque la posibilidad de construir computadoras cuánticas es aún una incertidumbre, y hay numerosas instituciones (como pueden ser las militares) que no se pueden permitir arriesgar la seguridad de sus datos ante la evolución de la tecnología.

La posibilidad de realizar tareas, importa más que la viabilidad de las mismas. Toda computadora cuántica gira en torno a problemas de viabilidad: su misma realización pretende hacer viables tareas que no lo eran hasta ahora. Lo que es interesante de la criptografía cuántica, aparte de cómo problema particular de la teoría cuántica de la información, es que responde afirmativamente a la pregunta:

¿Existe algún modo de comunicar información que sea inherentemente seguro, es decir, cuya seguridad resida en las propias leyes de la física?

Los códigos tradicionales basan su seguridad en una cuestión de rendimiento. Los requisitos para descifrarlos crecen exponencialmente cuando lo hace linealmente al esfuerzo empleado en proteger la información, pero no hay ningún principio físico que niegue la posibilidad de que esto se consiga. La criptografía cuántica, en cambio, es totalmente segura desde este punto de vista.

Descripción de una transmisión cuántica

Los métodos criptográficos cuánticos pueden agruparse en dos categorías:

- Distribución de clave cuántica.

  En este procedimiento la llave secreta, en lugar de ser generada a partir de números primos, se obtiene mediante estados cuánticos. Una estrategia posible se describe a continuación:

  El usuario 1 envía 2n qubits al usuario 2, cada uno de ellos preparado en uno de los estados $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ de modo aleatorio. A continuación el usuario 2 recibe la información, y mide los estados en una base particular, ya sea $\{|0\rangle,|1\rangle\}$ o bien $\{|+\rangle,|-\rangle\}$. Finalmente el usuario 1 indica públicamente al usuario 2 la base utilizada para preparar cada qubit. En promedio el usuario 2 habrá usado para hacer las medidas la misma base que el usuario 1 al preparar los estados la mitad de tiempo. Los únicos resultados con sentido son precisamente estos. Por último, el usuario 1 y el usuario 2 comparten la misma cadena de n bits, donde por ejemplo $|0\rangle$ y $|+\rangle$ se asocian a "0" y $|1\rangle$ y $|-\rangle$ lo hacen a "1". A esta cadena la llamamos RQT, por Raw Quantum Transmisión (es decir, transmisión cuántica literal).

Un espía que pretendiese interceptar la cadena de qubits dejaría evidencia de su presencia, pues la información no puede clonarse, y para hacerse con ella ésta no podrá alcanzar nunca a su receptor legitimo. *Si el interceptor opta por realizar medidas y reenviar la información aproximadamente la mitad de las veces acertará con la base en la que hacerlas, de modo que no perturbará el qubit correspondiente, pero la otra mitad su intervención será evidente a la hora de comparar lo que el usuario 2 recibió al principio con la cadena RQT: de los n bits de la cadena la cuarta parte será inconsistente con el estado cuántico.*

Si el usuario 1 y el usuario 2 comparten públicamente $n/2$ bits elegidos aleatoriamente de la cadena RQT y encuentran que coinciden en sus valores, podrán estar seguros de que nadie ha interceptado el mensaje. La probabilidad de que con $n = 1000$ bits el usuario 1 y 2 hayan escogido sólo bits que no hayan sido modificados en el ataque es de $(3/4)^{n/2} \cong 10^{-125}$.

Hay otras estrategias posibles, y descifrar cadenas puede ser aún más complicado para un espía en función de ellas. Por otra parte, tenemos ruido, haciendo que algunos qubits varíen impredeciblemente su estado.

- Comunicación segura en presencia de ruido.

Si hay ruido en la comunicación aparecerán errores en la secuencia RQT que no estarán asociados a ningún ataque. Esos errores esperamos que sean escasos, pues los errores se espera que se produzcan de manera esporádica, mientras que los debidos a un ataque afectan a la mitad de los qubits y, por diseño, a la cuarta parte de los bits de la secuencia RQT. Así que, bajo el esquema anterior, una tasa de error inferior al 25% significa que la línea no ha sido modificada.

El siguiente paso es corregir los errores. Esto puede hacerse compartiendo resultados de bits de paridad en subconjuntos del mensaje elegidos aleatoriamente.

El último paso es extraer de la clave otra más pequeña, compuesta por valores de paridad obtenidos a partir de la original. De esta clave, de alrededor de $n/4$ bits, un espía solo conocería el 10^{-6} de un bit.

MÉTODOS DE ENCRIPTACIÓN

Richard Feynman inicia su curso de Mecánica Cuántica con un experimento ideal, basado en la doble rendija de Young, que le permite distinguir entre una situación clásica y una de cuántica. Una máquina lanza partículas (balas o electrones) sobre una pared con una doble rendija, por delante de una pantalla donde impactar.

En un sistema clásico las trayectorias de las balas son distinguibles, es decir, se puede seguir el camino que sigue cada una. Los impactos en la pantalla seguirán una distribución estadística, resultado de sumar los impactos individuales de las distribuciones que se obtendrían separando las balas que ha pasado por una rendija o por la otra. Se obtiene, pues, una distribución de probabilidad que es la suma de las distribuciones de probabilidad de las dos rendijas.

En un sistema cuántico las trayectorias individuales no se pueden seguir. Incluso enviando electrones uno a uno, los impactos en la pantalla dibujaran una distribución que mostrará una figura de interferencia, siempre que los dos agujeros estén abiertos.

Podríamos considerar este dispositivo como un canal de comunicación. Por ejemplo, variando la separación de las rendijas, la distribución de los impactos en la pantalla será distinta. Es fácil imaginar un código de comunicación basado en este efecto.

Si un espía accediera al canal de comunicación (entre las rendijas y la pantalla) podría fácilmente iluminar el camino de las partículas y deducir la figura sobre la pantalla y, por tanto, descifrar el mensaje. Ahora bien, esto sería cierto solamente en el caso clásico. Si se usa la misma técnica de espionaje para una comunicación cuántica, la acción del espía ¡eliminaría la formación de la figura de interferencia!.

La imposibilidad de observar un sistema cuántico sin perturbarlo está en la base de la aplicación de los sistemas cuánticos al tratamiento de la información. La criptografía, entendida como el conjunto de técnicas para mantener una comunicación segura entre dos partes, es por tanto, un campo de aplicación ideal de esta característica de los sistemas cuánticos: observar (espiar) modifica (destruye) el sistema observado. Es como si el espía al leer un documento secreto lo perturbara o incluso destruyera. ¿Es realmente posible implementar un sistema de comunicaciones seguro (inviolable) basándose en sistemas cuánticos? La respuesta es afirmativa: la mecánica cuántica ha abierto una nueva vía en la historia de la criptografía, pero, paradójicamente, también ha puesto en cuestión la seguridad de los métodos criptográficos más utilizados actualmente.

Cifras monoalfabéticas

En todas las épocas siempre ha existido la necesidad de comunicar información de forma secreta. Los primeros en usar un método de comunicación secreta sistemático fueron los antiguos habitantes de Esparta. No obstante, si una figura histórica se ha

asociado a los orígenes de la criptografía esta es Julio César. Veamos a que se refiere este método de cifrado.

Según cuenta Suetnio en Vida de los Césares, Julio César enviaba los mensajes a sus generales sustituyendo cada letra del alfabeto por la correspondiente tres posiciones más avanzadas:

Alfabeto llano	a	b	c	d	e	...	x	y	z
Alfabeto cifrado	D	E	F	G	H	...	A	B	C

Ejemplo:.

Texto llano	este es un mensaje cifrado
Texto cifrado	HVXH HV XQ PHQVDMH FLIUDGR

Puede complicarse un poco si se eliminan los espacios entre palabras:

Texto llano	esteesunmensajecifrado
Texto cifrado	HVXH HVXQPHQVDMHFLIUDGR

Evidentemente, no hace falta limitarse a avanzar tres letras. Tenemos 26 posibilidades de formar una cifra del César.

Esta sencilla cifra nos presenta ya los elementos básicos del proceso de encriptación de un texto:

1. **Cifra:** Método de codificación. En este caso el método es la transposición cíclica de las letras del alfabeto.

2. **Texto llano:** Texto del mensaje a codificar. Buscaremos siempre métodos que permitan codificar cualquier texto, es decir, que evitaremos considerar las claves que se basan en una serie de palabras previamente concertadas con un significado preacordado entre emisor y receptos.

3. **Texto cifrado:** Texto del mensaje cifrado.

4. **Clave:** En este caso es el número 3, es decir, que se avanza el alfabeto cifrado tres posiciones. Debemos distinguir entre el método de cifrado (cifra o código) y la llave (clave). Para estudiar el criptoanálisis se supone que el espía conoce (o puede deducir) el código, pero desconoce la llave.

Cifra monoalfabética

La cifra del César en un caso particular de cifrado monoalfabético en el que la asignación del alfabeto cifrado al alfabeto llano es una simple trasposición.

Cifra monoalfabética: es una aplicación:

$$\{a,b,c,...,z\} \rightarrow P\{a,b,c,...,z\},$$

donde $P\{a,b,c,...,z\}$ representa el conjunto de las permutaciones de las 26 letras del alfabeto, lo que da un total de $26! = 4 \times 10^{26}$ posibilidades de cifras distintas.

Evidentemente, la cifra del césar forma parte del conjunto de posibilidades cifras monoalfabéticas ya que las trasposiciones cíclicas en el conjunto de las letras del alfabeto son unas pocas de las posibles permutaciones. ¿Cómo es posible crear una cifra? Pues hay que establecer un diccionario que nos pase del alfabeto llano al alfabeto cifrado, una cualquiera de las 26! Posibilidades.

Cifrado mediante palabra clave

La ventaja de la cifra del César se basa en la simplicidad de la clave, transmitir al receptor un solo número. Una mejora consiste en usar una palabra clave, por ejemplo "SANTIAGO", y usarla como las primeras letras del alfabeto cifrado, eliminando las letras repetidas y disponiendo a continuación el resto de letras. Así:

Alfabeto llano	a	b	c	d	e	f	g	h	i	j
Alfabeto cifrado	S	A	N	T	I	G	O	B	C	D

Esta asignación de alfabetos constituye la cifra basada en la palabra clave "SANTIAGO", y como es fácil comprobar, no corresponde a ningún caso de cifra de césar. Veamos como se codifica el mensaje del ejemplo anterior:

Texto llano	esteesunmensajecifrado
Texto cifrado	IQRIIQUJHIJQSINCGPSTK

¿Es "seguro" enviar un mensaje usando este sistema? Evidentemente, al contrario del caso de la cifra del César un análisis exhaustivo de todos los 26! Distintos alfabetos llevará la fracaso. Por este motivo, las cifras monoalfabéticas se consideraron "seguras" durante muchos siglos.

El criptoanálisis

Al-Kindi (s. XI) encontró un punto débil de la codificación monoalfabética: cada letra del alfabeto se sustituye por otra, pero siempre la misma. Dado que el texto llano a codificar se encuentra escrito en un lenguaje natural, todas las características el mismo se trasmiten al texto codificado. Por ejemplo, la frecuencia de aparición de las distintas letras es una característica propia de cada lenguaje. Así, en inglés, la letra mas frecuente en un texto es la letra *e* que aparece en promedio un 12.702% de las veces. La letra *a* aparece un 8.167%, la letra *b* un 1.492%, etc.

A partir de esta observación Al-Kindi encontró un método de romper una cifra monoalfabética: si el texto cifrado es lo suficientemente largo, un análisis de frecuencias de los distintos símbolos comparado con el análisis de frecuencias del lenguaje en que está escrito permite deducir la tabla de conversiones de los dos alfabetos.

Cifras polialfabéticas

Para evitar que el análisis de frecuencias pueda romper una cifra, hay que conseguir que las frecuencias de aparición de los distintos símbolos en el texto cifrado sea lo más homogénea posible. Esto se consigue en las cifras polialfabéticas.

La cifra Vigenère

Blaise de Vigenère (1523 – 1596) publicó en el año 1586 el primer método de cifrado polialfabético. Básicamente se trata de codificar el texto llano con la cifra del César, pero usando un desplazamiento (llave) distinto para cada letra del mensaje. Así, si recordamos la cifra del César con la llave 3 para todo el mensaje:

Texto llano	M	E	N	S	A	J	E	C	I	F	R	A	D	O
Llave	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Texto cifrado	P	H	Q	V	D	M	H	F	L	I	U	D	G	R

Se puede cambiar ahora por el proceso

Texto llano	M	E	N	S	A	J	E	C	I	F	R	A	D	O
Llave	22	5	14	21	19	22	5	14	21	19	22	5	14	21
Texto cifrado	I	J	B	N	T	F	J	Q	D	Y	N	F	R	J

En este ejemplo diríamos que hemos empleado una cifra Vigenère con la llave 22-5-14-21-19. Podemos comprobar que la letra *a* del texto llano que aparece dos veces, la primera se codifica en una T y la segunda en una F. La principal característica de la cifra Vigenère es que una misma letra se codifica con símbolos distintos, lo que imposibilita un análisis de frecuencias.

Criptoanálisis de la cifra Vigenère

Durante dos siglos la cifra Vigenère fue efectivamente inviolable a todos los intentos de los criptoanalistas, hasta que entró en escena Charles Babagge (1792 – 1871) quien en 1854 encontró un método para romperla. Desgraciadamente para Babagge, su idea fue redescubierta y publicada unos años más tarde, en 1863, por Kasinski (1805 – 1881).

El test de Kasinski, se basa en la búsqueda de combinaciones de dos o tres letras que se repitan en el texto cifrado. Si la llave se repite, hay una cierta probabilidad de que un grupo de letras del texto llano que aparecen juntas a menudo (por ejemplo

"que") se codifique con el mismo fragmento de la llave, lo que implicará una repetición en el texto cifrado.

Texto llano	q	u	e	...	q	u	e	...
Llave	X	x	x	...	X	x	x	...
Texto cifrado	X	Y	Z	...	X	Y	Z	...

El método de criptoanálisis empieza por realizar un estudio estadístico de las distancias entre grupos repetidos. A continuación se descomponen estas distancias en factores primos y entonces se puede inferir que la longitud de la clave será un múltiplo del factor común entre ellos.

El siguiente paso lo dio Friedman (1925), al introducir el denominado índice de coincidencias o probabilidad de que sacadas dos letras al azar de un texto sean la misma. A partir del texto cifrado podemos calcularlo como:

$$I_t = \frac{1}{n(n-1)} \sum_{i=1}^{26} n_i (n_i - 1)$$

donde n es el número de caracteres en el texto y n_i el número de apariciones de la letra número i.

Por otra parte, si sabemos el lenguaje empleado, este valor deberá coincidir con el teórico:

$$I = \sum_{i=1}^{26} p_i^2$$

donde p_i es la probabilidad de aparición de cada letra, calculado a partir de la tabla de frecuencias del lenguaje.

Si el texto ha sido cifrado con una cifra monoalfabética (y la muestra es suficientemente larga) los dos índices coincidirán. Si se trata de una cifra Vigenère polialfabética, entonces el índice I_i disminuirá, tanto más cuanto más larga sea la palabra clave. En otras palabras, el índice de coincidencias nos da información sobre el grado de información de las frecuencias de las letras.

La estimación sobre la longitud de la palabra clave del índice de coincidencias nos permite elegir cual de los múltiplos del valor obtenido en el test de Kandiski debemos proponer como longitud de la palabra clave empleada en la codificación.

El conocer la longitud de la palabra clave permite romper fácilmente la codificación polialfabética. En efecto, basta estudiar con las técnicas habituales del criptoanálisis monoalfabetico los conjuntos de letras del mensaje que se han codificado con el mismo alfabeto, y habrá tantos conjuntos como letras tenga la palabra clave.

Criptografía e información

Un criptosistema o esquema de encriptación es un conjunto formado por (P, C, K, E, D) donde:

P	Conjunto de textos llanos.
C	Conjunto de textos cifrados.
K	Conjunto de claves de encriptación.
E	Familia de funciones de encriptación
D	Familia de funciones de desencriptación

Las funciones de encriptación actúan como:

$$E_k : P \to C, \forall k \in K$$

y las de desencriptación como:

$$D_k : C \to P, \forall k \in K$$

La condición de que un tal sistema constituya un criptosistema es que se verifique la propiedad:

$$\forall e \in K, \exists d \in K / D_k(E_e(p)) = p, \forall p \in P$$

Un criptosistema se denomina simétrico cuando d y e son iguales. Por el contrario, se denomina asimétrico si d y e son diferentes.

Criptoanálisis

Denominamos criptoanálisis al ataque a un criptosistema. Hay que considerar distintos tipos de criptoanálisis, básicamente:

- *Ataque de texto cifrado.* El criptoanalista sólo conoce el texto cifrado y se quiere conseguir el texto llano y la clave.
- *Ataque con texto llano conocido.* Se conoce el texto llano y el texto cifrado y se quiere determinar la llave.
- *Ataque con texto llano escogido.* Se pueden encriptar textos llanos pero se desconoce la clave.

En un criptosistema (P, C, K, E, D) denotamos por $P_{r_p}(p)$ a la probabilidad de que un texto llano p aparezca en P. De forma similar, la probabilidad de una clave se denota por $P_{r_k}(k)$. La probabilidad de que un texto llano p aparezca codificado por la clave k es, pues, $P_r(p,k) = P_{r_p}(p), P_{r_k}(k)$, función que define una distribución de probabilidad en el espacio producto $P \times K$.

Decimos que un criptosistema es secreto perfecto si:

$$P_r(p \mid c) = P_r(p), \forall p \in P, \forall c \in C$$

es decir, que la probabilidad de un cierto texto cifrado y la probabilidad de que un texto llano haya sido cifrado son independientes.

Bases físicas para una criptografía cuántica

Teorema de Shannon. Sea $|C| = |K|$ y $P_r(p) > 0, \forall p \in P$. El criptograma será secreto perfecto si y sólo si la distribución de probabilidad en el espacio de llaves es uniforme y si para cualquier texto llano p y texto cifrado c, existe una única llave k con $E_k(p) = c$.

El teorema de Shannon nos asegura que el cifrado digital simétrico es secreto perfecto siempre y cuando se cumplan los dos requisitos:

1. La llave ha de ser aleatoria.
2. La llave debe usarse sólo una vez.

Requisitos que no parecen muy difíciles de cumplir. Hay, sin embargo, una tercera dificultad: la llave, tan larga como el mensaje y de un solo uso, ha de estar en

posesión tanto del emisor como del receptor. El principal obstáculo de orden práctico es el de cómo compartir la clave, dado que si cae ésta en manos de terceros el secreto se perdería. Es en este punto donde la mécanica cuántica hace su aparición aportando métodos seguros de distribución de llaves (Quantum Key Distribution).

La seguridad de los mecanismos para QKD reside en las bases físicas de la mecánica cuántica:

1. El teorema de no cloning que nos asegura que un estado cuántico $|\Psi\rangle$ no puede ser copiado. Clásicamente un texto puede ser fotocopiado. Un sistema cuántico no puede ser copiado, y por tanto, espiado.

2. Cualquier intento de obtener información sobre un sistema cuántico lleva aparejado una cierta modificación del mismo.

3. Las medidas cuánticas son irreversibles. Después de realizar una medida, el sistema colapsa a uno de los estados propios del operador correspondiente a la magnitud que se ha medido, y este proceso es irreversible, es decir, no se puede volver a llevar al sistema a su estado original, el de antes de medir.

Veamos con más detalle estos efectos. Supongamos que queremos distinguir entre dos estados cuánticos $|\Psi\rangle$ y $|\Phi\rangle$ que no sean ortogonales, es decir, $|\langle\Phi|\Psi\rangle|^2 \neq 0$

El aparato de medida que usaremos para distinguirlos se representará por $|u\rangle$. El estado global será pues $|\Phi\rangle \otimes |u\rangle$ o bien $|\Psi\rangle \otimes |u\rangle$.

La evolución del sistema durante la medida conllevará a que el elemento $|u\rangle$ evolucione hasta un estado que, si queremos nos sirva para distinguir entre los dos, deberá ser distinto en cada caso: $|u_\Phi\rangle$ o bien $|u_\Psi\rangle$. Pero la evolución es unitaria, lo que implica que si queremos que los estados a medir queden inalterados, será imposible que los estados del elemento $|u\rangle$ sean distintos.

Protocolos para la generación cuántica de llaves (QKG)

Veremos ahora los protocolos básicos que se han implementado incluso experimentalmente para crear una llave compartida entre dos personas, que se pueden comunicar mediante un canal cuántico (fibra óptica por ejemplo).

BB84

Este protocolo fue presentado por Bennett y Brassard en la Internacional Conference on Computers, Bangalore (1984). Consideraremos la implementación que usa fotones polarizados. Recordemos que los fotones se polarizan transversalmente, cosa que se puede indicar por un vector en un plano transversal al movimiento. Si elegimos como base para escribir el vector polarización los vectores polarizados

según las direcciones de los ejes X e Y podemos escribir un vector polarización (y al estado cuántico correspondiente) según una dirección arbitraria como:

$$|\Psi\rangle = a|\rightarrow\rangle + b|\uparrow\rangle$$

donde hemos denotado los estados de la base como $|\rightarrow\rangle$ y $|\uparrow\rangle$.

No obstante, la elección de esta base es totalmente arbitraria. El mismo estado $|\Psi\rangle$ tiene su representación en otra base como por ejemplo la formada por los estados de polarización según las direcciones | ↗ ⟩ y | ↖ ⟩.

$$|\Psi\rangle = a'|\ \nearrow\ \rangle + b'|\ \nwarrow\ \rangle$$

Las dos bases, que representamos por base + y base X están relacionadas por las ecuaciones de cambio de base:

$$|\ \nearrow\ \rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + |\uparrow\rangle\right)$$

$$|\ \nwarrow\ \rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - |\uparrow\rangle\right)$$

Por convenio, el bit 0 lo representaremos por el $|\rightarrow\rangle$ en la base + o por el estado $|\ \nearrow\ \rangle$ en la base $\times$. Similarmente, al bit 1 lo asignamos a los estados $|\uparrow\rangle$ o $|\ \nwarrow\ \rangle$. El uso simultáneo de ambas bases permitirá asegurar la inviolabilidad de la transmisión.

Veamos como se implementa.

Se generan dos secuencias de bits aleatorios:

Secuencia 1	0	1	1	0	0	1	...
Secuencia 2	1	0	0	1	1	1	...

La primera secuencia indica el bit a transmitir y la segunda la base en la que debe preparar el estado que representa el citado bit, usando en convenio de que 0 indica la base + y 1 la base $\times$.

Así, en el ejemplo anterior tendríamos:

Bits	0	1	1	0	0	1	...
Bases	$\times$	+	+	$\times$	$\times$	$\times$	...
Estados	$\|\ \nearrow\ \rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\ \nearrow\ \rangle$	$\|\ \nearrow\ \rangle$	$\|\ \nwarrow\ \rangle$	...

La tercera línea de la tabla anterior indica los estados que se deben preparar para después enviarlos secuencialmente.

Por otro lado, debemos preparar los instrumentos de medida para analizar los estados (fotones) que llegarán. Para esto tenemos dos opciones para medir cada fotón que llegue, disponer del instrumento de medida según la base + o según la base ×. Debemos generar una serie de bits aleatorios y disponer de los instrumentos de acuerdo con el resultado, base + si sale 0 o base × si es 1. Por ejemplo, los instrumentos se preparan de siguiente forma:

Secuencia	0	1	0	0	0	1	...
Bases	×	×	+	+	+	×	...

¿Qué resultados mediríamos? Depende de si se recibe un estado preparado según una base y se lee con los aparatos preparados para la misma base o no. Si las bases coinciden, obtendremos el mismo estado que ha sido enviado. Si se mide con la base equivocada, el resultado que obtendrá es un elemento de esta base con probabilidad $\frac{1}{2}$, siendo, pues un resultado aleatorio. Continuando el ejemplo anterior:

Bits enviados	0	1	1	0	0	1	...
Bases enviadas	×	+	+	×	×	×	...
Estados enviados	$\lvert \nearrow \rangle$	$\lvert \uparrow \rangle$	$\lvert \uparrow \rangle$	$\lvert \nearrow \rangle$	$\lvert \nearrow \rangle$	$\lvert \nwarrow \rangle$	...
Bases recibidas	×	×	+	+	+	×	...
Estados recibidos	$\lvert \nearrow \rangle$	R	$\lvert \uparrow \rangle$	R	R	$\lvert \nwarrow \rangle$	...
Bits recibidos	0	-	1	-	-	1	...

Con este proceso, en los casos en que ha habido coincidencia de bases, se comparte el mismo bit. En los casos en que no ha habido coincidencia, los bits reconstruidos son aleatorios. Si encontramos la forma de eliminar de la secuencia de bits enviados de la secuencia recibida, los casos de no-coincidencia, tendrían la misma secuencia de bits aleatorios que podrían usar como clave aleatoria compartida para un proceso de encriptación tipo on time pad. En nuestro ejemplo se compartiría la secuencia $\{0,1,1,...\}$.

¿Cómo podríamos realizar este proceso de filtro? Pues basta que tanto la persona que envía como la que recibe hagan públicas las secuencias de bases que han usado para preparar y para medir los estados. Comparando las dos listas se puede pueden eliminar los resultados que se deben desechar.

Ahora la pregunta que surge inmediatamente es si esta comunicación pública pone en entredicho la seguridad del establecimiento de la clave. La respuesta es no.

Mientras que el usuario que envia no diga que bit ha codificado y el usuario que recibe el resultado que obtuvo, publicar las bases no da ninguna información útil para un eventual espía.

Eavesdropping

¿Cómo podría un eventual espía interferir en este proceso? Evidentemente, si el usuario que envía interfiere el canal de comunicación (la fibra optica por la que circulan los fotones) lo que no puede hacer es "apuntar" los estados de los fotones que pasan por la fibra (lo prohíbe el no-cloning). Ahora bien, el usuario que recibe puede cortar la comunicación midiendo el fotón que llega del usuario que envio y enviando un fotón que genere el usuario que envia para el que recibe. ¿Puede detectarse este efecto?

La única forma que tienen para asegurarse de si hay o no la presencia de un eventual espía es hacer pública, antes incluso de filtrar los resultados, una secuencia de bits emitidos y bits medidos. Es fácil comprobar que la probabilidad de acertar el bit (si no hay un eventual espía presente) es de $3/4$, siendo la probabilidad de fallar de $1/4$. En cambio, si el espía esta presente, absorbiendo y emitiendo fotones, la probabilidad de acertar es ahora de $5/8$, o la de fallar de $3/8$. En otras palabras, la presencia de un espía se traduce en un incremento del 50% en el número de fallos.

B92

Bennet publicó en 1992 un nuevo protocolo para la generación e intercambio cuántico de claves. Consideramos el mismo sistema anterior pero ahora se escogen como representación de los bits 0 y 1 los estados:

Bit	Estado
0	$\|\rightarrow\rangle \equiv \|0\rangle$
1	$\| \nwarrow \rangle \equiv \|1'\rangle$

Donde la prima recuerda que se trata del estado correspondiente al bit 1 en la que habíamos llamado base $\times$.

El usuario que envía prepara una cadena de bits aleatorios y prepara los estados a enviar de acuerdo con la tabla anterior. Así:

Bits	0	1	1	0	0	1	...
Estados	$\|0\rangle$	$\|1'\rangle$	$\|1'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1'\rangle$	...

Por otro lado el usuario que recibe genera su cadena de bits para elegir las bases en que realiza sus medidas (0 base +, 1 base $\times$), pero en lugar de aplicar una medida de Von Neuman, se aplicarán ahora a los estados que recibe los operadores de proyección siguientes:

- Si su bit es 0 (base +), aplica el proyector $P_{not0} = \left(1 - |0\rangle\langle 0|\right)$.
- Si su bit es 1 (base ×), aplica el proyector $P_{not1'} = \left(1 - |1'\rangle\langle 1'|\right)$.

El resultado de la aplicación del proyector será cero o uno, ahora como interpretamos los resultados? Si la aplicación de P_{not0} sobre un estado lo deja invariante (autovalor 1), el usuario que recibe puede estar seguro de que su estado no es $|0\rangle$ y por lo tanto que ha recibido el estado $|1'\rangle$, pero si obtiene cero, no puede deducir que estado ha recibido. De forma similar ocurre con el otro proyector.

La estrategia consiste en eliminar de la secuencia los bits en los que el usuario que recibe ha medido cero, sea cual sea el proyector que ha aplicado, y quedarse con los que ha medido 1. Una vez realizada la secuencia de medidas, el usuario debe comunicar a quien le envía, que bits debe desechar y en los demás el acuerdo será total.

Protocolo B92 modificado

El protocolo B92 fue modificado en 1994. La modificación consiste en usar medidas generalizadas (Positive Operador Valued Measurements) (POVM'S) en lugar de aplicar directamente proyectores. Así, introducimos los operadores herméticos y positivos.

$$A_0 = \frac{P_{not\,0}}{1+\left\|\langle 0|1'\rangle\right\|}$$

$$A_{1'} = \frac{P_{not\,1'}}{1+\left\|\langle 0|1'\rangle\right\|}$$

$$A_? = 1 - A_0 - A_{1'}$$

En conjunto los tres operadores $\{A_0, A_{1'}, A_?\}$ constituye un POUM.

En los protocolos anteriores la forma de controlar los errores del canal así como la presencia de un espía consiste en comparar un determinado número de bits de la clave final, así estimar la tasa de error y ver si está dentro de los márgenes de los errores estimados. Hay, sin embargo, otros protocolos en los que la presencia del espía se controla por mecanismos cuánticos, como las desigualdades de Bell. Para ello, estos protocolos usan parejas de estados entrelazados.

Protocolo E91

Este protocolo presentado en 1991 por Ekert usa parejas de fotones entrelazados creados a partir de una fuerte EPR (Einstein, Podolski, Rosen). Se consideran tres preparaciones distintas de parejas entrelazadas:

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1\left|\frac{3\pi}{6}\right\rangle_2 - \left|\frac{3\pi}{6}\right\rangle_1|0\rangle_2\right)$$

$$|\Omega_1\rangle = \frac{1}{\sqrt{2}}\left(\left|\frac{\pi}{6}\right\rangle_1\left|\frac{4\pi}{6}\right\rangle_2 - \left|\frac{4\pi}{6}\right\rangle_1\left|\frac{\pi}{6}\right\rangle_2\right)$$

$$|\Omega_2\rangle = \frac{1}{\sqrt{2}}\left(\left|\frac{2\pi}{6}\right\rangle_1\left|\frac{5\pi}{6}\right\rangle_2 - \left|\frac{5\pi}{6}\right\rangle_1\left|\frac{2\pi}{6}\right\rangle_2\right)$$

donde el valor del ket indica la dirección del eje de polarización de cada fotón.

Para la codificación se consideran tres alfabetos alternativos, que denominamos A_0, A_1 y A_2, con la representación de los bits $(0,1)$ como:

Bits	0	1
A_0	$\|0\rangle$	$\left\|\frac{3\pi}{6}\right\rangle$
A_1	$\left\|\frac{\pi}{6}\right\rangle$	$\left\|\frac{4\pi}{6}\right\rangle$
A_2	$\left\|\frac{2\pi}{6}\right\rangle$	$\left\|\frac{5\pi}{6}\right\rangle$

Como operadores de media pueden escoger entre $M_0 = |0\rangle\langle 0|$, $M_1 = \left|\frac{\pi}{6}\right\rangle\left\langle\frac{\pi}{6}\right|$ y $M_2 = \left|\frac{2\pi}{6}\right\rangle\left\langle\frac{2\pi}{6}\right|$.

El protocolo sigue los siguientes pasos:

1. Se genera un estado $|\Omega_j\rangle$ con $j = 1,2,3$ de forma aleatoria.

2. Se manda uno de los fotones al usuario que envía y al que recibe.

3. Los usuarios separadamente y de forma aleatoria eligen uno de los tres operadores de medida y lo aplican a su fotón.

4. Después de las medidas, los usuarios hacen públicas las listas con los operadores que han usado en cada medida (manteniendo reservados los resultados obtenidos).

5. En los casos en que los dos han usado el mismo operador, tienen asegurada la concordancia de los bits medidos. Rechazan todos lo demás bits y se quedan con la clave común

BIT COMMITMENT

Partamos de la situación en la que el usuario 1 decide el valor de su qubit de modo que el usuario 2 puede a partir de cierto instante estar seguro de que el usuario 1 ha decidido el valor, pero no puede saber de que valor se trata hasta algún instante posterior, escogido también por el usuario 1. En el marco clásico esto podría hacerse guardando el mensaje dentro de una caja fuerte, para, después de elegido el momento en que el usuario 1 permita al usuario 2 leerlo, y facilitarle la combinación.

El modelo cuántico del quantum commitment consiste en una implementación particular de un protocolo en el que el usuario 1 envía un qubit al usuario 2, y solo el 1 puede elegir el momento de decirle en que base fue preparado. Ni el usuario 2 ni un tercero pueden permitirse tratar de medir el qubit sin conocer la base, pues además de no poder interpretarlo echarían a perder el estado cuántico dotado de la información.

La realización que se ha llevado a la práctica es la distribución de clave cuántica. Uno de los primeros experimentos, que fue realizado por Bennett y Bassard en 1989, demostró la fiabilidad de la idea. De ahí a los 23km de distancia que Zbinden comunicó por debajo del lago Geneva pasaron sólo ocho años.

En el experimento de Zbinden los qubits eran estados de polarización de pulsos láser. Los pulsos contenían 0.1 fotones en promedio, es decir, pulsos con más de un fotón eran muy probables. Más de un fotón por pulso implica duplicidad de la información, y abre el camino a un tercero para interceptar el mensaje sin ser detectado. La tasa de error del sistema era del 1.35%. Vimos antes que para la estrategia descrita, un error menor del 25% permite estar seguro de que cierto mensaje no ha sido robado y la tasa de error en este caso es claramente inferior, de modo que el sistema es adecuado para la comunicación segura.

También hay más alternativas. Los pares EPR pueden usarse, de modo que el usuario 1 y 2 pueden preparar estados y realizar medidas a lo largo de diferentes ejes, pero un espía introduciría correlaciones EPR que serían detectables.

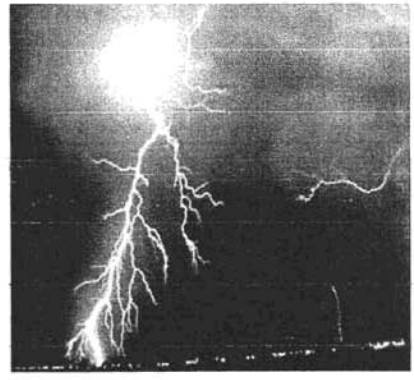
EN PERSPECTIVA

Imaginemos que en el futuro se logra construir un chip con tecnología de la computación cuántica, teniendo en cuenta que los estados con qué esta trabaja son 1 (que en cualquier momento puede tomar valor de "0" o "1"), y 0 (que también en cualquier momento puede tomar el valor de "0" o "1"), y se coloca el chip en el lugar adecuado del cerebro de una persona que sufre trastornos mentales, y que este chip tiene la capacidad de captar y regular algunas de las señales que el cerebro manda incorrectamente a los órganos del sistema. Para mejorar la situación física se debe programar la función del chip para que actúe de manera adecuada: primero se deberán capturar todas esas señales que el cerebro envía y posteriormente ver el comportamiento de cada una de éstas con el fin de saber cuáles son las señales que ocasionan que un ser humano tenga alguna alteración o deficiencia en su organismo. De esta forma se podrán manipular mediante el uso de una computadora cuántica o en su defecto molecular, ya que la computadora convencional no tiene la tecnología suficiente para poder trabajar con un número tan extenso de variables. De esta manera podemos reducir el envió de las señales parásitas para que se tenga un comportamiento adecuado en el organismo.

Para entender lo anterior, fijemos nuestra atención en algunos fenómenos de la naturaleza:

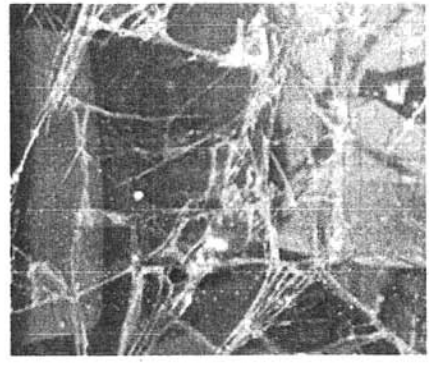
1. Forma física de un árbol:

2. Forma de un relámpago.



3. Forma de una grieta.

4. Forma de un cristal estrellado.



Vemos que el árbol crece y del tronco común se desprenden varias ramas lo cual facilita que el agua y todos los nutrientes necesarios para sobrevivir lleguen hasta el extremo más alejado; recordemos que el árbol no tiene locomoción para

procurárselos y estas formas ramificadas son consecuencia de una ley de la naturaleza: el principio de mínima acción – máximo beneficio. El tratar de simular con una computadora convencional sería una tarea muy difícil de realizar de ahí que necesitamos esta nueva tecnología. En la actualidad no podemos pensar que los fenómenos naturales ocurren como si se desarrollaran en una sola línea, pues como se ha mostrado con el ejemplo del árbol, no tendría la suficiente fuerza para abastecerse de sustancias suficientes como para subsistir.

En las otras imágenes existe un paralelismo, tanto el relámpago como la grieta y el cristal al fracturarse tienen su formas particulares de liberarse de una manera rápida y eficiente de un exceso de energía que de alguna forma fue inyectado al sistema, tratar de simular esto con la tecnología actual resulta difícil o casi imposible lograrlo.

Entonces, si aplicáramos este principio para crear el chip, y se pudiese colocar en el cerebro, éste sería capaz de captar señales que envía el medio ambiente, y crearía líneas de comunicación que no existierán o repararía otras que por alguna razón hubiesen sido desconectadas. Asimismo se podrían resolver problemas que en la actualidad la medicina, por ejemplo, no ha logrado solucionar, tal es el caso de los tipos de cáncer, diabetes, SIDA, etc., el mismo modo se crearían algoritmos como los de Grover para realizar las búsquedas de dichas señales y al encontrar los parámetros que, de acuerdo con el órgano que se desee reparar serían las variables que se controlarían.

Anexo

LA NOTACIÓN DE DIRAC

Los vectores base u_i se denotan como $|i\rangle$ y son llamados vectores abrir corchete. Los vectores base en el espacio dual, u_i^+, son llamados vectores cerrar corchete, o base que se cierra y se denota con $\langle i|$, la imagen bajo espejo para los corchetes usando convenciones usuales, tenemos resultados conocidos.

$$I = |i\rangle \langle i|$$

En notación de Dirac, también la condición de ortonormalidad será:

$$\langle i|i'\rangle = \delta_{ii'} = \begin{cases} 1 & si \quad i = i' \\ 0 & si \quad i \neq i' \end{cases}$$

Es decir, una yuxtaposición de los símbolos para los vectores corchete, las dos líneas verticales se reducen a una par brevedad de notación.

La notación de Dirac, nos lleva a escribir, cualquier vector corchete arbitrario (en el lenguaje ortodoxo, cualquier vector) en términos de los vectores corchete. Así un vector que cierra $|x\rangle$, le corresponde al vector arbitrario $\bar{x}$, en la notación clásica:

$$|x\rangle = |i\rangle \langle i|x\rangle$$

Bastando con multiplicar $I = |i\rangle \langle i|$ por $|x\rangle$ a la derecha, comparando $|x\rangle = |i\rangle \langle i|x\rangle$, con la clásica, $\bar{x} = \sum_{i=1} \bar{u}_i x_i$ muestra que las componentes x_i del vector arbitrario $\bar{x}$ en la base $\bar{u}_i$, se denotan con $\langle i|x\rangle$ en la notación de Dirac.

De manera análoga, multiplicando $I = |i\rangle \langle i|$ por $\langle x|$ por la izquierda nos da:

$$\langle x| = \langle x|i\rangle \langle i|$$

a la que le corresponde en el espacio dual

$$\bar{x}^+ = \sum \bar{x}_i u_i^+$$

en notación clásica. Luego se sigue que

$$\langle x|i\rangle = \overline{\langle i|x\rangle}$$

Cambio de base

Multiplicando $I = |i\rangle \langle i|$ por la derecha con la base cerrar corchete $|j\rangle$ da:

$$|j\rangle = |i\rangle \langle i|j\rangle$$

esta es la notación de Dirac, para el cambio de base:

$$\overline{v_i} = \sum_i u_i t_{ij}$$

en la notación clásica, luego el corchete $\langle i|j\rangle$ se identifica con los elementos t_{ij} de la matriz de transformación t. Observe que mientras en la notación clásica, los vectores base se distinguen con el uso de diferentes letras (p.e. $\overline{u_i}, \overline{v_i}, \overline{w_i}$, etc) únicamente índices diferentes, se utilizan en la notación de Dirac. Los n vectores base diferente, que constituyen una base son denotados con el uso de primas $|i\rangle$, $|i'\rangle$, $|i''\rangle$, etc.

El cambio de base en el espacio dual que corresponde, al vector $\overline{v_i} = \sum_i u_i t_{ij}$, a saber $\overline{v_j^+} = \sum_i \overline{t_i}, \overline{u_i^+}$ será en la notación de Dirac:

$$\langle \cdot j| = \overline{\langle i|j\rangle}\ \langle i| = \langle j|\ \rangle\ \langle i|$$

la que se obtiene, al multiplicar $I = |i\rangle\ \langle i|$ donde la izquierda con la base corchete izquierdo $\langle j|$.

Multiplicando por la izquierda $|x\rangle = |i\rangle\ \langle i|x\rangle$ con $|j\rangle\ \langle j|$ nos da:

$$|x\rangle = |j\rangle\ \langle j|x\rangle = |j\rangle\ \langle j|i\rangle\ \langle i|x\rangle$$

Luego los componentes del corchete derecho $|x\rangle$ en la base j se dan en términos de los componentes en la base i mediante la relación:

$$\langle j|x\rangle = \langle j|i\rangle \ \langle i|x\rangle$$

las componentes del corchete izquierdo $\langle x|$ que corresponden al corchete que cierra $|x\rangle$ se dan con el conjugado del anterior:

$$\overline{\langle j|x\rangle} = \overline{\langle j|i\rangle \ \langle i|x\rangle} = \langle x|i\rangle \ \langle i|j\rangle$$

Operadores lineales en la notación de Dirac.

La expresión para cualquier operador $\mathcal{T}$ en la notación de Dirac se obtiene al multiplicar $\mathcal{T}$ tanto en la izquierda como a la derecha de $I = |i\rangle \ \langle i|$:

$$\mathcal{T} = |i\rangle \ \langle i| \ \mathcal{T} |i'\rangle \ \langle i'|$$

Comparando lo anterior con la expresión clásica:

$$\mathcal{T} = \sum_{i,i'} \bar{u}_i \cdot \mathcal{T}_{ii'} \bar{u}_{i'}^{+}$$

Nos muestra que los elementos de la matriz $\mathcal{T}_{ii'}$ son denotados con $\langle i|\mathcal{T}|i'\rangle$ en la notación de Dirac.

Análogamente, la notación de Dirac para el operador $\mathcal{T}^+$, la transpuesta de la conjugada o la adjunta hermitiana de $\mathcal{T}$ es:

$$\mathcal{T}^+ = |i\rangle\ \langle i|\ \mathcal{T}^+|i'\rangle\ \langle i'|$$

Que corresponde a la expresión:

$$\mathcal{T}^+ = \sum_{i,i'} \bar{u}_i\ \mathcal{T}_{ii'}\ \bar{u}_{i'}{}^+ = \sum_{i,i'} \overline{u_i}\ \mathcal{T}_{ii'}\ \bar{u}_{i'}{}^+$$

En la notación clásica, De esto se sigue que:

$$\langle i|\ \mathcal{T}^+|i'\rangle = \overline{\langle i'|\mathcal{T}|i\rangle}$$

Observe que si $\mathcal{T}$ es el operador idéntico entonces

$$\mathcal{T} = |i\rangle\ \langle i|\ \mathcal{T}|i'\rangle\ \langle i'|$$

se reduce a

$$\mathcal{I} = |i\rangle\ \langle i|\mathcal{I}\ |i'\rangle\ \langle i'| = |i\rangle\ \langle i|i'\rangle\ \langle i'| = |i\rangle\delta_{ii'}\langle i'| = |i\rangle\ \langle i|$$

de acuerdo con $I = |i\rangle \langle i|$.

El resultado de aplicar $\mathcal{T}$ sobre un corchete que cierra arbitrario $|x\rangle$ se da según:

$$\mathcal{T}|x\rangle = |i\rangle \langle i|\mathcal{T}|i'\rangle \langle i'|$$

Al que corresponde

$$\mathcal{T}\bar{x} = \sum_{i,i'} \bar{u}_i \mathcal{T}_{ii'} x_{i'}$$

La adjunta hermitiana de $\mathcal{T}|x\rangle$ es:

$$\langle x|\mathcal{T}^+ = \langle x|i\rangle \langle i|\mathcal{T}^+|i'\rangle \langle i'| = \overline{\langle i|x\rangle} \overline{\langle i'|\mathcal{T}|i\rangle} \langle i'|$$

Vectores y valores propios.

Se sabe que si $\mathcal{T}\bar{u}_l = t\bar{u}_l$ entonces $\bar{u}_l$ se dice el vector propio del operador $\mathcal{T}$ que corresponde al valor propio l. En la notación de Dirac, esta relación se expresa:

$$\mathcal{T}|l\rangle = |l\rangle l$$

Luego en cualquier base i,

$$\mathcal{T}|i'\rangle\ \langle i'|l\rangle = \langle i'\rangle\ \langle i'|l\rangle l$$

$$|i\rangle\ \langle i|\mathcal{T}|i'\rangle\ \langle i'|l\rangle = |i\rangle\ \langle i|i'\rangle\ \langle i'|l\rangle l$$

Así que

$$\langle i|\mathcal{T}|i'\rangle\ \langle i'|l\rangle = \langle i|i\rangle\ \langle i'|l\rangle l = \langle i|l\rangle l$$

es la ecuación matricial desde cual la cual se pueden determinar los valores propios de l.

Representación espectral de un operador.

En la notación clásica la representación de un operador lineal $\mathcal{T}$ en la base l cuyos vectores base son los vectores propios de $\mathcal{T}$ se da como:

$$\mathcal{T} = \sum_l \bar{u}_l l \tilde{u}_l^+$$

La expresión correspondiente en la notación de Dirac es:

$$\mathcal{T} = |l\rangle\ \ l\ \langle l|$$

La representación de $\mathcal{T}$ en términos de una base arbitraria l es entonces:

$$\mathcal{T} = |i\rangle \langle i|l\rangle \, l \, \langle l|i'\rangle \langle i'|$$

De esto se sigue que la representación de $\mathcal{T}^n$ en está base es:

$$\mathcal{T}^n = |i\rangle \langle i|l\rangle l^n \langle l|i'\rangle \langle i'|$$

Y en general, la representación de cualquier función de $\mathcal{T}$, digamos $f(\mathcal{T})$ es:

$$f(\mathcal{T}) = |i\rangle \langle i|l\rangle \, f(l) \langle l|i'\rangle \langle i'|$$

Teorema sobre operadores hermitianos:

A manera de ilustración de la facilidad en el manejo de la notación de Dirac. Probaremos dos teoremas útiles e importantes sobre operadores hermitianos. Un operador lineal $\mathcal{H}$ que cumple la condición $\mathcal{H} = \mathcal{H}^+$ es llamado hermitiano.

Teorema.

Los valores propios de un operador hermitiano son reales en efecto, considere la ecuación:

$$\mathcal{H}|h\rangle = |h\rangle h$$

Multiplicando por la izquierda con $\langle h|$ nos da:

$$\langle h|\mathcal{H}|h\rangle = h$$

Luego $\mathcal{H}$ es hermitiano, de aquí que:

$$\langle h|\mathcal{H}|h\rangle = \langle h|\mathcal{H}^{+}|h\rangle = \overline{\langle h|\mathcal{H}|h\rangle} = \bar{h}$$

Luego igualando, las dos últimas expresiones, se sigue que $h = \bar{h}$ si un número complejo es igual que su conjugado, entonces h es real.

Teorema:

Una condición necesaria y suficiente para que dos operadores hermitianos puedan diagonalizarse con la misma transformación unitaria, es que ellos se conmuten.

1. Si $\mathcal{H} = |\lambda\rangle\, h(\lambda)\, \langle\lambda|$ y $\mathcal{J} = |\lambda\rangle\, j(\lambda)\langle\lambda|$, entonces $\mathcal{H}\mathcal{J} = \mathcal{J}\mathcal{H}$. En efecto:

$$\mathcal{H}\mathcal{J} = |\lambda\rangle\, h(\lambda)\langle\lambda|\lambda'\rangle j(\lambda')\langle\lambda'| = |x\rangle h(\lambda) j(\lambda)\langle\lambda| = |\lambda\rangle\, j(\lambda) h(\lambda)\langle\lambda| = \mathcal{J}\mathcal{H}$$

2. Si $\mathscr{H}\mathscr{I} = \mathscr{I}\mathscr{H}$, entonces existe una base λ tal que $\mathscr{H} = |\lambda\rangle h(\lambda)\langle\lambda|$ y $\mathscr{I} = |\lambda\rangle j(\lambda)\langle\lambda|$.

En efecto; si h es un valor propio no degenerado de $\mathscr{H}$ entonces $\mathscr{H}|h\rangle = |h\rangle h$ y $\mathscr{H}\mathscr{I}|h\rangle = \mathscr{I}\mathscr{H}|h\rangle = \mathscr{I}|h\rangle h$ pero establece que $\mathscr{I}|h\rangle$ es un corchete cierre de $\mathscr{H}$ que corresponde al valor propio h, y es entonces un múltiplo de $|h\rangle$, luego:

$$\mathscr{I}|h\rangle = |h\rangle j(h)$$

Si $|h\rangle$ es un valor propio degenerado de $\mathscr{H}$, etiquetamos los diversos corchetes que cierran con un índice λ, entonces:

$$\mathscr{H}|h,\lambda\rangle = |h,\lambda\rangle h$$

$$\mathscr{H} = |h,\lambda\rangle\, h\, \langle h,\lambda|$$

Entonces escribimos

$$\mathscr{I} = |h,\lambda\rangle\, \langle h,\lambda|\mathscr{I}|h',\lambda'\rangle\, \langle h',\lambda'|$$

Y formamos

$$\langle h,\lambda|\ \mathscr{H}\mathscr{I} - \mathscr{I}\mathscr{H}\ |h',\lambda'\rangle = (h-h')\, \langle h,\lambda|\mathscr{I}|h',\lambda'\rangle = 0$$

Se sigue entonces, que aquellos elementos $\langle h,\lambda|\mathcal{J}|h',\lambda'\rangle$ para los cuales $h \neq h'$ deben anularse, luego:

$$\mathcal{J} = |h,\lambda\rangle\ \langle h,\lambda|\mathcal{J}|h,\lambda'\rangle\ \langle h,\lambda'|$$

Observando los corchetes que cierran propios de $\mathcal{J}$, que son también corchetes propios que cierran de $\mathcal{H}$ (no sumas sobre h):

$$\mathcal{J}\ |h,j\rangle = |h,j\rangle j\ ,\ |h,j\rangle = |h,\lambda\rangle\ |h,\lambda'\rangle$$

$$\mathcal{Y}\ \langle h,\lambda|\ \mathcal{J}\ |h,\lambda'\rangle\ \langle h,\lambda'|h,j\rangle = \langle h,\lambda|h,j\rangle j$$

Si esta última ecuación se resuelve para $\langle h,\lambda|h,j\rangle$ y j para encontrar $|h,j\rangle$. Es fácil obtener que $|h,j\rangle$ es un valor propio corchete de cierra tanto de $\mathcal{H}$ e $\mathcal{J}$. Por definición $\mathcal{J}\ |h,j\rangle = |h,j\rangle j$ también:

$$\mathcal{H}\ |h,j\rangle = \mathcal{H}\ |h,\lambda\rangle\ \langle h,\lambda|h,j\rangle = |h,\lambda\rangle\ \langle h,\lambda|h,j\rangle = h|h,j\rangle \text{ como se deseaba.}$$

Un conjunto de operadores $\mathcal{H}$, $\mathcal{J}$, $\mathcal{T}$, etc., tal que sus correspondientes valores propios de corchete cierra son no degenerados, es llamado, un conjunto completo de observables y un conjunto completo de estos, esta determinado unívocamente excepto por un múltiplo escalar complejo de magnitud unitaria.

TRANSFORMADA CUÁNTICA DE FOURIER

La transformada cuántica de Fourier de un *n*-qubit es el operador lineal $F_n : H_n \to H_n$ que se define sobre el vector $|j\rangle$ de la base de computación, $0 \leq j < 2^n$, del siguiente modo:

$$F_n|j\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \sigma_n^{jk} |k\rangle$$

donde σ_n es la raíz 2^n - ésima de la unidad $e^{\frac{2\pi}{2^n}}$ y $Q = 2^n$. Realmente se trata de la transformada discreta de Fourier cuya expresión habitual $(\hat{f}_0, \cdots, \hat{f}_{Q-1}) = F_n(f_0, \cdots, f_{Q-1})$, en coordenadas de la base de computación, es la siguiente:

$$\hat{f}_k = \frac{1}{\sqrt{Q}} \sum_{j=0}^{Q-1} \sigma_n^{kj} f_j$$

La transformada cuántica de Fourier es una transformación unitaria. Para obtener su inversa basta sustituir en la expresión de F_n el parámetro $\sigma_n = e^{-\frac{2\pi i}{2^n}}$. Y actúa sobre el vector $|0\rangle$ del mismo modo que la transformada de Walsh – Hadamard:

$$F_n|0\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} |k\rangle$$

Si denominamos periodo de la función discreta f al menor número T, $1 \le T \le Q$, que verifica $f_{j+T} = f_j$ para todo $0 \le j < Q$, considerando los índices módulo Q, entonces T es un divisor de Q. Si no lo fuera $T' = mcd(T,Q) < T$ cumpliría $f_{j+T'} = f_j$ para todo $0 \le j < Q$, contradiciendo la minimalidad de T. En efecto, según el teorema de Bèzout, existirían $m_1, m_2 \in Z$ tales que $T' = m_1 T + m_2 Q$ y, por tanto, se satisfaría $f_{j+T'} = f_{j+m_1 T + m_2 Q} = f_j$. Entonces, dada una función f de período T su transformada cuántica de Fourier $\hat{f}$ se anula en todos los elementos del dominio salvo en los múltiplos de la frecuencia w de la función, definida en términos del periodo por la relación $wT = Q$. Es decir:

$$F_n\left(\sum_{j=0}^{Q-1} f_j |j\rangle\right) = \sum_{k=0}^{T-1} \hat{f}_{wk} |wk\rangle$$

Esta propiedad permite obtener fácilmente la frecuencia w de la función f y, en consecuencia, también el período T. Para ello se aplica la transformada cuántica de Fourier a f y, a continuación, se miden todos los qubits. De este modo obtenemos un valor wk tal que $0 \le k < T$ y devolvemos como resultado $w' = mcd(wk, Q)$. Si se cumple que el $mcd(k,T) = 1$ entonces $w' = w$, puesto que

$Q = wT$. En caso contrario w' es un múltiplo de w. Si todos los valores de k entre 0 y $T - 1$ son equiprobables entonces se verifica:

$$P(w' = w)\log\log(T) = \frac{\phi(T)}{T}\log\log(T) \xrightarrow[lim\ inf]{} e^{-\gamma} = 0.561459...$$

Siendo $\gamma = 0.577215...$ la constante de Euler. En el cálculo del límite inferior anterior se ha tenido en cuenta el siguiente resultado clásico de teoría de números:

$$\lim_{T\to\infty} inf \frac{\phi(T)\log\log(T)}{T} = e^{-\gamma}$$

Para conseguir una probabilidad positiva, independiente de T y de Q, habría que repetir el proceso $O(\log\log(Q))$ veces. Por tanto, tendríamos un algoritmo polinomial en el número de dígitos de Q. La transformada cuántica de Fourier se puede definir para valores de Q arbitrarios, en particular para Q igual al número $\phi(N)$. Sin embargo, para evaluarla de forma eficiente, por ejemplo mediante el algoritmo de la transformada rápida, se necesitaría factorizar previamente tanto N como $\phi(N)$.

La elección más simple para implementar la transformada cuántica de Fourier consiste en tomar $Q = 2^n$. En la siguiente figura se muestra el primer algoritmo que se propuso para calcular la transformada cuántica de Fourier en este caso.

Las líneas horizontales representan qubits que evolucionan temporalmente de izquierda a derecha y se numeran desde arriba. El símbolo H sobre una línea especifica la aplicación de la puerta cuántica H sobre el qubit correspondiente a la línea. La aplicación de la puerta CR_k (Controlled R_k) se indica uniendo con un segmento vertical los símbolos ∘ y R_k que se colocan sobre el qubit de control y el qubit afectado respectivamente. Finalmente la puerta S (swap) se representa uniendo con un segmento vertical dos símbolos × colocados sobre los dos qubits afectados.

El algoritmo anterior calcula la transformada de Fourier de un vector de longitud $Q = 2^n$ aplicando $O(n^2)$ puertas cuánticas mientras que, clásicamente, el algoritmo de la transformada rápida de Fourier realiza $O(Q\log(Q)) = O(n2^n)$ operaciones. Shor utiliza la ganancia exponencial del algoritmo cuántico para obtener un factor propio del número natural N en tiempo $O(\log^4(N)\log\log(N))$.

Ahora comprobemos que el algoritmo de la transformada cuántica de Fourier de la figura anterior sea correcto. Utilizaremos la notación $H(k)$ para indicar la aplicación de la puerta H al qubit k-esímo, $S(k,j)$ para representar la puerta

Swap actuando sobre los qubits k y j y $CR_k(j,m)$ para aplicar la puerta R_k sobre el qubit m-ésimo si el j-ésimo está en estado $|1\rangle$.

Dado un número natural de n dígitos binarios $k = k_n...k_1$ llamamos k' al número de $n-1$ dígitos que se obtiene al suprimir el dígito más significativo de k, es decir $k' = k_{n-1}...k_1$. Esta notación nos permite expresar la transformada cuántica de Fourier de forma recursiva:

$$F_n|k\rangle = F_{n-1}|k'\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \sigma_n^k|1\rangle\right)$$

Para probarlo necesitamos establecer algunas relaciones para $0 \le j < 2^{n-1}$:

$$|2j\rangle = |j\rangle \otimes |0\rangle \qquad \text{y} \qquad |2j+1\rangle = |j\rangle \otimes |1\rangle$$

$$\sigma_n^{k(2j)} = \sigma_n^{\left(2^{n-1}k_n + k'\right)(2j)} = \sigma_n^{2^n k_n j}\sigma_n^{k'(2j)} = \sigma_n^{k'(2j)} = \sigma_{n-1}^{k'j}$$

$$\sigma_n^{k(2j+1)} = \sigma_n^{k(2j)}\sigma_n^k = \sigma_{n-1}^{k'j}\sigma_n^k$$

A partir de estas ecuaciones se obtiene de forma sencilla la expresión recursiva de F_n:

$$F_n|k\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\sigma_n^{kj}|j\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^{n-1}-1}\sigma_n^{k(2j)}|2j\rangle + \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^{n-1}-1}\sigma_n^{k(2j+1)}|2j+1\rangle$$

$$= \frac{1}{\sqrt{2^{n-1}}}\sum_{j=0}^{2^{n-1}-1}\sigma_{n-1}^{k'j}|j\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \sigma_n^k|1\rangle\right)$$

$$= F_{n-1}|k'\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \sigma_n^k|1\rangle\right)$$

Dado un número natural de n dígitos $k = k_n \ldots k_1$ llamamos $\bar{k}$ al número de n dígitos que se obtiene al invertir el orden de los dígitos de k, es decir $\bar{k} = k_1 \ldots k_n$. Si k y j son dos números naturales de n dígitos, entonces se verifica $\bar{k}j = k\bar{j}$. Este hecho permite demostrar la siguiente propiedad de la transformada cuántica de Fourier:

$$S(1,n)S(2,n-1)\ldots F_n|\bar{k}\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\sigma_n^{\bar{k}j}S(1,n)S(2,n-1)\ldots|j\rangle$$

$$= \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\sigma_n^{\bar{k}j}|\bar{j}\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\sigma_n^{k\bar{j}}|\bar{j}\rangle = F_n|k\rangle$$

El algoritmo de la transformada cuántica de Fourier, prescindiendo de las puertas Swap, también se puede expresar recursivamente:

$$W_n = W_{n-1}CR_n(n,1)CR_{n-1}(n,2)\ldots CR_2(n,n-1)H(n)$$

Esta expresión se obtiene reordenando las puertas cuánticas:

$$CR_n(n,1), CR_{n-1}(n,2) \ldots CR_2(n,n-1),$$

respecto a las posiciones en las que aparecen en la figura anterior, y colocándolas al final del algoritmo. Para ello basta aplicar reiteradamente la siguiente propiedad: dos puertas cuánticas que actúan sobre qubits diferentes conmutan. Teniendo en cuenta la propiedad vista anteriormente, para demostrar la corrección del algoritmo sólo es necesario probar que:

$$W_n|\bar{k}\rangle = F_n|k\rangle$$

La demostración se puede hacer por inducción en el número n de qubits:

1. Paso base: $n=1$. En este caso $|\bar{k}\rangle = |k\rangle$ y, además, se cumple $W_1 = F_1 = H$.

2. Paso de inducción: supongamos por $H.I.$ que $W_n|\bar{k}\rangle = F_n|k\rangle$ para un $n \geq 1$. Entonces:

$$F_{n+1}|k\rangle = F_n|k'\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \sigma_{n+1}^{k}|1\rangle\right) = W_n|\bar{k}'\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \sigma_{n+1}^{k}|1\rangle\right)$$

$$= W_n\left(|\bar{k}'\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \sigma_{n+1}^{2^n k_{n+1} + \cdots + 2^0 k_1}|1\rangle\right)\right)$$

$$= W_n\left(|\bar{k}'\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \sigma_{n+1}^{k_1} \ldots \sigma_2^{k_n}\sigma_1^{k_{n+1}}|1\rangle\right)\right)$$

$$= W_n CR_{n+1}(n+1,1)\ldots CR_2(n+1,n)\left(|\bar{k}'\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \sigma_1^{k_{n+1}}|1\rangle\right)\right)$$

$$= W_n CR_{n+1}(n+1,1)\ldots CR_2(n+1,n)H(n+1)\left(|\bar{k}'\rangle \otimes |k_{n+1}\rangle\right)$$

$$= W_{n+1}\left(|\bar{k}'\rangle \otimes |k_{n+1}\rangle\right) = W_{n+1}|\bar{k}\rangle$$

ALGORITMO DE EUCLIDES

El algoritmo de Euclides es un método eficaz para calcular el máximo común divisor (mcd) entre dos números enteros. El algoritmo consiste en varias divisiones euclidianas sucesivas. En la primera división, se toma como dividendo el mayor de los números y como divisor el otro. Luego, el divisor y el resto sirven respectivamente de dividendo y divisor de la siguiente división. El proceso se termina cuando se obtiene el resto nulo. El mcd es entonces el penúltimo resto del algoritmo.

Formalmente, si llamamos a, b los enteros iniciales r_1, $r_n \ldots r_{n-1}$ y $r_n = 0$ los restos sucesivos, entonces: $mcd(a,b) = mcd(b,r_1)$, con $r_1 = a - b \cdot q$ (q es el cociente de a por b).

En efecto los divisores comunes de a y b son los de $a - b \cdot q$ y b:

$$\left.\begin{matrix} q/a \\ q/b \end{matrix}\right\} \Leftrightarrow \begin{cases} q/a \\ q/(a-bq) \end{cases}$$

porque si q divide a y b, obviamente divide $a-b\cdot q$ es una combinación lineal de ambos, y recíprocamente $a=(a-b\cdot q)+b\cdot q$ es una combinación lineal de b y $a-b\cdot q$. Luego el menor de los divisores comunes es el mismo, y repitiendo la operación:

$$mcd(b,r_1)=mcd(r_1,r_2)=mcd(r_2,r_3)=\ldots=mcd(r_{n-1},r_n)=mcd(r_{n-1},0)=r_{n-1}$$

Esto nos permite detallar el algoritmo efectivo:

- Datos de entrada a y b - si hace falta, cambiarlos a positivos.
- El algoritmo:

  Mientras $b\neq 0$ repetir las tres instrucciones siguientes:

  $r\leftarrow$ resto de a por b (dar a r el valor del resto de a por b).

  $a\leftarrow b$ (el nuevo valor de a es el antiguo valor de b).

  $b\leftarrow r$ (el nuevo valor de b es el valor de r).

- El resultado es a (su último valor).

Este algoritmo da como resultado 0 si a y b son nulos, mientras que en matemáticas, el mayor divisor de cero no existe.

Ejemplos:

Se busca el máximo común divisor de $a = 945$ y $b = 651$, números escogidos al azar:

$945 = 1 \times 651 + 294$
$651 = 2 \times 294 + 63$
$294 = 4 \times 63 + 42$
$63 = 1 \times 42 + 21$
$42 = 2 \times 21 + 0$

Entonces $mcd(945;294) = 21$ (el último resto no nulo)

Como segundo ejemplo, tomemos números de tamaños parecidos a los anteriores: $a = 987$ y $b = 610$:

$987 = 1 \times 610 + 377$
$610 = 1 \times 377 + 233$
$377 = 1 \times 233 + 144$
$233 = 1 \times 144 + 89$
$144 = 1 \times 89 + 55$
$89 = 1 \times 55 + 34$
$55 = 1 \times 34 + 21$
$34 = 1 \times 21 + 13$
$21 = 1 \times 13 + 8$
$13 = 1 \times 8 + 5$
$8 = 1 \times 5 + 3$
$5 = 1 \times 3 + 2$
$3 = 1 \times 2 + 1$

Entonces $mcd(987;610) = 1$

El segundo ejemplo es sustancialmente más largo que el primero, y esto se debe a que todos los cocientes valen 1. Aquí a y b no fueron escogidos a la azar: son

dos términos consecutivos de la sucesión de Fibonacci; es el pero de los casos para este algoritmo.

Fracciones continuas

Las divisiones euclidianas del algoritmo son idénticas a las que permiten hallar la expresión en facción continua de a/b.

En efecto, $a = bq_1 + r_1$ se puede escribir $a/b = q_1 + \frac{r_1}{b}$. Del mismo modo, $b = r_1q_2 + r_2$ se puede escribir como $\frac{b}{r_1} = q_2 + \frac{r_2}{r_1}$ y si lo inyectamos en la igualdad anterior obtenemos $\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \frac{r_2}{r_1}}$ y el proceso se repite hasta utilizar todas las divisiones euclidianas, y da lugar a fracciones con muchos "pisos". Los ejemplos numéricos del párrafo anterior dan:

$$\frac{945}{651} = 1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{1 + \frac{1}{2}}}}$$

y

$$\frac{987}{610} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}}}}}}}}}$$

En este proceso funciona tamibén con valores irracionales de a/b (con a y b reales), en tal caso, el algoritmo no se para, lo que da una fracción continua finita. Son de especial inter´res estas fracciones, como en los casos de π y e.

Volviendo al caso a y b enteros, el algoritmo de Euclides permite encontrar los coeficientes enteros u y v de la identidad de Bézout $au + bv = mcd(a,b)$ de fundamental importancia en la aritmética.

Generalización a los polinomios

Este algoritmo sólo precisa de la división euclidiana, y por consiguiente se extiende a todos los dominios donde existe tal división: es el caso de las álgebras de polinomios, como $Q[x]$ o $R[x]$, (polinomios con coeficientes racionales o reales). Obviamente, los cálculos se vuelven mucho más largos. Un ejemplo no demasiado complicado, pero tampoco trivial es:

Sea $P = x^3 - 6x^2 + 63x + 392$ un polinomio que se cree que tiene una raíz doble.

Como resolver una ecuación de tercer grado no es evidente, para hallar la raíz múltiple empleamos la propiedad que dice las raíces múltiples son en común entre el polinomio y su polinomio derivado.

Para simplificar las divisiones, nos permitimos multiplicarlos por factores constantes no nulos, en fin de cuentas el *mcd* de dos polinomios está definido un módulo de un factor multiplicativo, así que esta manipulación no alter el resultado.

El polinomio derivado de P es $P'=3x^2-12x-63$ que se puede simplificar por 3, según lo dicho anteriormente. Tomemos entonces $Q=\frac{P'}{3}=x^2-4x-21$ y efectuemos el algoritmo con P y Q.

$P=(x-2)Q-50x+350$. El resto se factoriza en $-50(x-7)$: tomemos entonces $R=x-7$.

$Q=(x+3)R+0$ lo que implica que el *mcd* buscado es $x-7$. Entonces 7 es la raíz doble de P.

En efecto: $P=(x-7)^2(x+8)$ y de paso $P'=3(x-7)(x+3)$.

CONCLUSIONES

En la actualidad, en el área de computación se precisa satisfacer ciertas necesidades como el manejo de grandes cantidades de información, aumento de la velocidad en los procesadores, mayor capacidad de almacenamiento y también el tiempo de transferencia de datos de un lugar a otro en grandes distancias. Para lograr esto con éxito, se necesita de una gran infraestructura en todos los medios posibles. Lo que tenemos hoy en día ya es insuficiente para llevar a cabo estas tareas, por lo que se requiere de una nueva tecnología que realice estas actividades con prontitud y eficiencia.

Como se pudo comprobar a lo largo de este trabajo, la computación cuántica es una opción viable para lograr este objetivo, si bien no sólo es útil para enviar información a diferentes lugares en cuestión de nanosegundos, también lo es usando simulación con modelos en la medicina, la biología, química, física y demás ciencias, donde hasta ahora no había sido posible por la complejidad subyacente.

BIBLIOGRAFÍA

1. SATINOVER Jeffrey, The Quantum Brain, the search for freedom and the next Generation of man, ed. John Wiley & Sons, Inc, 2000, Pgs. 243.

2. GRÖSSING Gerhard, Quantum Cybernetics, toward a unification of relativity and quantum theory via circularly causan modeling, ed. Springer, Pgs. 153.

3. NIELSEN Michael A., Isaac L. Chuang, Quantum Computation and quantum information, ed. Cambridge University, 2000.

4. DEUTSCH D., Quantum theory, the Church – Turing principle an the universal quantum computer, ed. Proc Roy Soc. Lond, pp. 97 – 117.

5. FEYNMAN, R. P., Simulating physics with computers, ed. International journal of theoretical physics, vol. 21, 1982, pp. 467 – 488.

6. FEYNMAN, R. P., Lecturas de física, vol. 3, ed. Fondo educativo, 1980.

7. RUBO Yuri, Tagüeña Julia, ¿Cómo ves?, Revista de divulgación de la ciencia de la UNAM, Año 6, No. 67.

8. http://www.qubit.org

9. http://www.ieee.com.