PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
FACULTAD DE INGENIERIA
ESCUELA DE SISTEMAS

DISERTACION PREVIA A LA OBTENCION DEL TITULO DE INGENIERO DE SISTEMAS Y COMPUTACION

"SIMULADOR DE UN COMPUTADOR CUANTICO UTILIZANDO EL ALGORITMO DE SHOR PARA FACTORIZAR NUMEROS ENTEROS"

NOMBRE:

HERRERA MANOSALVAS CHRISTIAN JAVIER

DIRECTOR:

MSC. JORGE AGUILAR

QUITO, 2016

A mi Padre,
simplemente gracias

TABLA DE CONTENIDO

Introducción **1**
1. Introducción 1
2. Justificación 3
3. Objetivos 4
3.1. Objetivo General 4
3.2. Objetivos Específicos 4
4. Alcance 5
5. Metodología 6
Capítulo I **7**
1. Conceptos Generales 7
1.1. ¿Qué es un computador cuántico? 7
1.2. Breve historia de la computación cuántica 11
1.3. El potencial y poder de la computación cuántica 13
1.4. Obstáculos e Investigación 17
1.5. Candidatos para un computador cuántico 20
1.6. Problemas propuestos 24
1.6.1. Encriptación Cuántica 25
1.7. Mirada al futuro de la computación cuántica 27
1.7.1 Puntos Cuánticos 28
1.7.2. Computador cuántico D-Wave 29
1.7.3. Microsoft LIQUi|> 31
Capítulo II **32**
2. Conceptos Específicos 32
2.1. Motivación experimental para la mecánica cuántica 32
2.1.1. Superposición 34
2.1.2. Entrelazamiento 35
2.2. Bits y Qubits 36
2.2.1. Operaciones reversibles sobre bits 40
2.2.2. Manipular operaciones 44
2.2.3. Qubits y sus estados 49
2.2.4. Operaciones reversibles sobre qubits 51

2.3. Diagramas de circuitos 53
2.4. Puertas de medición 55
2.5. Preparación de estados 60
2.5.1. Construcción de estados arbitrarios de 1 y 2 qubits 61
2.6. Bits vs Qubits 64
2.7. El proceso computacional cuántico 65
2.8. Encontrar el periodo, factorización y criptografía 71
2.8.1. Teoría de los números elemental 72
2.8.2. Utilizar un grupo con respecto a la multiplicación 74
2.8.3. Encriptación RSA 76
2.8.4. Búsqueda cuántica del periodo 77
2.8.5. La transformada de Fourier Cuántica 79
2.8.6. Encontrar el periodo 83
2.8.7. Calculo de la función periódica 84
2.8.8. Búsqueda del Periodo y Factorización 85
2.8.9. Ejemplo de aplicación del Algoritmo de Shor 86
2.9. Decoherencia 88
2.9.1. Corrección de errores cuánticos 89
Capítulo III **90**
3. Simulador 90
3.1. Teoría del caos aplicada al desarrollo de software 90
3.1.1. Conceptos de teoría del caos 90
3.1.2. Conceptos de desarrollo de software aplicables 91
3.2. Desarrollo del simulador 93
3.2.1. Diseño 93
3.2.2. Implementación 94
3.2.3. Pruebas 96
3.3. Manual de usuario 97
3.4. Manual técnico 101
Capítulo IV **103**
4. Conclusiones 103
Capítulo V **105**
5. Recomendaciones 105
Capítulo VI **106**

6. Bibliografía 106
Anexos **109**
Mecánica Cuántica 109
La Luz 109
Los Cuantos de Plank 110
El átomo en mecánica cuántica 112
La naturaleza de la luz 113
El gato de Schrödinger 115
La paradoja EPR 115
Teletransportación cuántica 117

INTRODUCCIÓN

1. INTRODUCCIÓN

El computador representa la culminación de años de avances tecnológicos empezando por las tempranas ideas de Charles Babbage y la eventual creación del primer computador. Pero sorprendentemente la alta velocidad de los computadores modernos no es diferente de sus ancestros de 30 toneladas equipados con 18000 tubos al vacío y 200 kilómetros de cables. A pesar de que los computadores han llegado a ser más compactos y considerablemente más rápidos en cumplir su tarea, esta tarea es la misma: manipular e interpretar una codificación de bits para obtener un resultado computacional útil.

Este avance tecnológico tiene un límite, del cual deriva la computación cuántica. Esta se refiere a los fenómenos que tendrá que enfrentar la tecnología de las computadoras cuando el tamaño de sus componentes rebase un límite inferior determinado, para el cual las leyes de la física son fundamentalmente diferentes a las que se aplican en el mundo macroscópico.

El computador actual se basa en los bits. Un bit es la unidad fundamental de la información, clásicamente representado por 1 o 0 en un computador digital. Cada bit clásico es físicamente representado en un sistema físico macroscópico, como la magnetización en un disco duro o la carga en un capacitor.

En un computador cuántico la unidad fundamental de información (llamada bit cuántico o qubit) no es binaria, sino más bien cuaternaria en naturaleza. Las propiedades del qubit surgen como consecuencia directa de su adherencia a las leyes de la mecánica cuántica, las cuales difieren radicalmente de las leyes de la física clásica. Un qubit puede existir no solamente en un estado correspondiente a los estados lógicos 0 o 1 como en un bit clásico, sino también en estados correspondientes a una combinación o superposición de estos estados clásicos. En otras palabras, un qubit puede existir como un cero, un uno, o simultáneamente como ambos 0 y 1, con un coeficiente numérico representando la probabilidad de cada estado.

La computación cuántica está basada en las interacciones del mundo atómico, y tiene elementos como el bit cuántico, las compuertas cuánticas, los estados confusos, la tele transportación cuántica, el paralelismo cuántico, y la criptografía cuántica. Sus implementaciones 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.

Estas características, entre otras, hacen que la investigación actual en computación cuántica no sea solamente una continuación de la idea actual de un computador, sino una rama entera del pensamiento.

2. JUSTIFICACIÓN

El campo del procesamiento de información cuántica ha hecho numerosos avances prometedores desde su concepción. Al momento, los computadores cuánticos y la teoría de la información cuántica permanecen en su estado pionero. Por ello todo estudio y experimento realizado en el tema es generador de nueva información y expande problemas y soluciones por igual para el advenimiento de una mejor era tecnológica y un cambio innovador en el área de la información. El conocimiento de un computador tradicional es muy extenso en toda institución superior, sin embargo los nuevos campos como el de la computación cuántica permanecen ocultos, por ello se desea investigar en el campo tanto a nivel teórico como a nivel práctico y realizar una implementación que resuelva el problema de factorizar un número, que en caso de números grandes es uno de los problemas nada trivial para los computadores actuales, utilizando las técnicas cuánticas propuestas en la actualidad y los algoritmos más conocidos y confiables del tema, de manera que se demuestre el potencial de esta nueva rama de la ciencia.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

- Desarrollar un sistema que simule el procesamiento que realizaría un computador cuántico que utilice el algoritmo de Shor para factorizar números enteros

3.2. OBJETIVOS ESPECÍFICOS

- Exponer las motivaciones y el propósito para realizar el desarrollo de un simulador de computador cuántico como tema para la disertación de grado.

- Definir los conceptos necesarios para comprender el funcionamiento de un computador cuántico, las posibilidades que presenta tecnológicamente y las ventajas en la resolución de problemas informáticos actuales.

- Plantear los algoritmos y el método de funcionamiento del simulador, conjuntamente con todos los procesos para obtener un resultado correcto superando las limitantes a nivel teórico y práctico.

- Desarrollar el simulador de acuerdo con la metodología escogida, cubriendo las pruebas necesarias para asegurar la correcta operación del sistema.

4. ALCANCE

La presente disertación de grado se considerará como concluida al entregar el documento de respaldo con la información correspondiente a los principios de computación cuántica que definen los objetivos y detalla el temario y al entregar el sistema que simula la aplicación del algoritmo de Shor para factorizar números enteros. En este caso se tomarán en cuenta números enteros pequeños, debido a la complejidad de hardware y algoritmo utilizados.

5. METODOLOGÍA

Trabajo Escrito

- Investigación
- Recopilación de datos
- Texto bibliográfico
- Revistas
- Informes
- White papers

Simulador

- Aplicación a 2 capas:
- Desarrollo de librerías base
- Front End apoyado en las librerías base
- Metodología de desarrollo: Teoría del Caos aplicada al desarrollo de sistemas
- Documentación: Manuales Técnico y de Usuario

CAPÍTULO I

1. CONCEPTOS GENERALES

1.1. ¿Qué es un computador cuántico?

Ilustración 1

Ilustración 1. **:** Utilizado originalmente por Neil Gershenfeld en un paper sobre computación cuántica publicado en Scientific America [1]

El computador representa la culminación de años de avances tecnológicos empezando con las primeras ideas de Charles Babbage[2][3] (1791-1871) y la eventual creación del primer computador por el ingeniero alemán Konrad Zuse en 1941. Sorprendentemente sin embargo, la alta velocidad de un computador moderno en frente de nosotros no es fundamentalmente diferente de sus ancestros gargantua de 30 toneladas, los cuales estaban equipados con unos 18000 tubos al vacío y 800 kilómetros de cables. A pesar de que los computadores han llegado a ser más compactos y considerablemente más rápidos en llevar a cabo su tarea, la tarea continúa siendo la misma: manipular e interpretar un código de bits binarios en un resultado computacional útil. Un bit es fundamentalmente una unidad de información, clásicamente representado como un 0 o un 1. Cada bit clásico se representa físicamente mediante un sistema físico macroscópico, como la magnetización en un disco duro o la carga en un capacitor. Un documento, por ejemplo, compuesto de *n* caracteres guardado en el disco duro de un computador típico se representa de acuerdo a una cadena de

[1] Neil Gershenfeld e Isaac L. Chuang, Quantum Computing with Molecules, http://cba.mit.edu/docs/papers/98.06.sciqc.pdf, Acceso: 13/12/2015

[2] Charles Babbage empezó su trabajo en la máquina analítica en 1833. En contraste con los dispositivos de cálculo existentes en esa época, el suyo se suponía que sería un computador universal. Babbage dedicó toda su vida a este proyecto, pero no pudo realizar su sueño (En 1991 la máquina fue producida de acuerdo con el diseño de Babbage).

[3] Varios, A Modern Sequel, http://www.computerhistory.org/babbage/modernsequel/ , Acceso: 13/12/2015

8n ceros y unos. Aquí yace la diferencia fundamental entre un computador clásico y un computador cuántico. Mientras que un computador clásico obedece las bien establecidas leyes de la física clásica, un computador cuántico es un dispositivo que hace uso de fenómenos físicos propios de la mecánica cuántica (especialmente la interferencia cuántica) para llevar a cabo fundamentalmente nuevas formas de procesamiento de la información.

La clave de esta expresión es "cuántico", que deriva de la locución latina quantum (que significa cantidad). En la jerga científica de hoy en día, esta expresión hace referencia a la cantidad más pequeña posible – o unidad discreta – de energía o materia. Un computador cuántico es un dispositivo para computación que hace uso directo de los fenómenos de la mecánica cuántica, como la superposición y el entrelazamiento, para realizar operaciones sobre los datos. [4]

En un computador cuántico, la unidad fundamental de información (llamada un bit cuántico o qubit), no es binario sino más bien de naturaleza quaternaria. Esta propiedad del qubit se presenta como consecuencia directa de su adherencia a las leyes de la mecánica cuántica las cuales difieren radicalmente de las leyes de la física clásica. Un qubit no solo puede existir en un estado correspondiente a los estados lógicos 0 o 1 como un bit clásico, sino también en estado correspondientes a una mezcla o superposición de estos estados clásicos. En otras palabras, un qubit puede existir como un cero, un uno, o simultáneamente como cero y uno, con un coeficiente numérico representando la probabilidad de cada estado. Esto puede ser poco intuitivo debido a que los fenómenos de cada día son gobernados por la física clásica, no la mecánica cuántica, la cual se refiere al nivel atómico. Este concepto más bien difícil tal vez se explica mejor mediante un experimento. Considerando la figura siguiente:

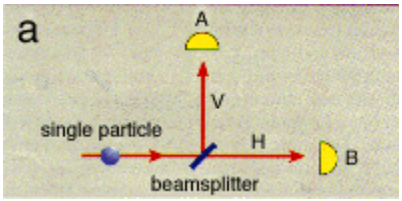


Ilustración 2. Un espejo semiplateado separa un fotón reflejándolo vertical y horizontalmente hacia los detectores A y B [5]

[4] Neil Gershenfeld e Isaac L. Chuang, Quantum Computing with Molecules, http://cba.mit.edu/docs/papers/98.06.sciqc.pdf, Acceso: 13/12/2015

[5] David Deutsch y Artur Ekert, Machines, Logic and Quantum Physics, http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=9052179&fileId=S1079898600006387, Acceso: 13/12/2015

Una fuente de luz emite un fotón hacia un espejo semiplateado. El espejo divide la luz, reflejándola mitad verticalmente hacia el detector A y transmitiendo mitad hacia el detector B. Un fotón, sin embargo, es un paquete cuántico simple de luz y no puede ser dividido, así que es detectada con igual probabilidad tanto en A como en B. La intuición diría que el fotón aleatoriamente deja el espejo en la dirección vertical u horizontal. Sin embargo, la mecánica cuántica predice que el fotón viaja por ambas rutas simultáneamente.

En un experimento como el de Ilustración 1, donde un fotón es disparado hacia un espejo semiplateado, se puede demostrar que el fotón en realidad no se divide, verificando que si un detector registra una señal, entonces ningún otro detector lo hace. Con esta información, se puede pensar que un determinado fotón viaja bien vertical u horizontalmente, escogiendo al azar uno de los dos caminos. Sin embargo, la mecánica cuántica predice que el fotón viaja por los dos caminos al mismo tiempo, colapsando hacia un camino solamente al momento de la medición. Este efecto conocido como *interferencia de una partícula simple*, puede ser ilustrado mediante un experimento más elaborado, como se muestra en la figura siguiente:

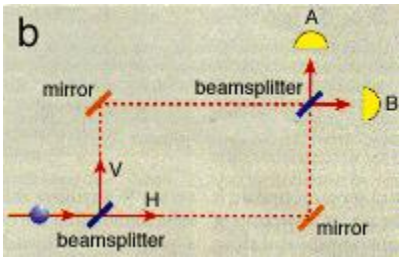


Ilustración 3: *El fotón pasa por un espejo semiplateado, luego por un espejo completamente plateado y finalmente por otro espejo semiplateado* [6]

En este experimento, el fotón inicialmente encuentra un espejo semiplateado, luego un espejo completamente plateado y finalmente otro espejo semiplateado, antes de alcanzar un detector, donde cada espejo semiplateado introduce la probabilidad de que el fotón siga un camino o el otro. Una vez que el fotón golpea el espejo sobre uno de los dos caminos luego de la primera división, el arreglo es idéntico a aquel de la Ilustración 1, de manera que se podría suponer que el fotón alcanzará el detector A o el detector B con igual probabilidad.

[6] David Deutsch and Artur Ekert, Machines, Logic and Quantum Physics, http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=9052179&fileId=S1079898600006387, Acceso: 13/12/2015

Sin embargo, el experimento muestra que en la realidad este arreglo causa que el detector A registre el 100% de los intentos, y nunca alcancen al detector B. ¿Cómo puede ser posible?.

La Ilustración 2 representa un experimento interesante que demuestra el fenómeno de la interferencia de partículas simples. En este caso, el experimento muestra que el fotón siempre alcanza el detector A y nunca el detector B. Si un solo fotón viaja verticalmente y golpea el espejo, entonces, por comparación al experimento en la Ilustración 1, debería existir una probabilidad igual de que el fotón golpee el detector A o el detector B. el mismo razonamiento aplica al fotón que viaja por el camino horizontal. Sin embargo, el resultado verdadero es drásticamente diferente. La única conclusión concebible es que por lo tanto el fotón de alguna manera viajó por ambos caminos simultáneamente, creando una interferencia en el punto de intersección que destruyó la posibilidad de que la señal alcanzara el detector B. Esto se conoce como *Interferencia Cuántica* y resulta de la *superposición* de los posibles *estados* del fotón, o caminos potenciales. De manera que aun cuando un solo fotón es emitido, pareciera ser que un fotón idéntico existe y viaja por el "camino no tomado", solamente detectable por la interferencia que causa con el fotón original cuando sus caminos se encuentran de nuevo. Si, por ejemplo, alguno de los caminos es bloqueado con una pantalla absorbente, entonces el detector B empieza a registrar señales de nuevo como en el primer experimento. Esta característica única, entre otras, hace de la investigación actual en la computación cuántica no sea solamente una continuación de la idea de hoy de un computador, sino más bien una rama enteramente nueva de pensamiento. Y es la razón por la cual los computadores cuánticos poseen características especiales que les dan el potencial para ser dispositivos computacionales increíblemente poderosos.

1.2. Breve historia de la computación cuántica

"La idea de un dispositivo computacional basado en mecánica cuántica fue explorada inicialmente en los 70's y principios de los 80's por físicos y científicos como Charles H. Bennett del Centro de Investigación Thomas J. Watson de IBM, Paul A. Benioff del Laboratorio Nacional Argonne en Illinois, David Deutsch de la Universidad de Oxford, y Richard P. Feynman del Intituto de Tecnología de California (Caltech)".[7]

La idea emergió cuando los científicos se cuestionaron sobre los límites fundamentales de la computación. Entendieron que si la tecnología seguía el sendero de la Ley de Moore[8], entonces la continua disminución de tamaño de los circuitos empacados en un chip de silicio eventualmente alcanzaría un punto donde los elementos individuales no contendrían más que un par de átomos. Es difícil imaginar que el tamaño de un transistor o algún otro elemento alguna vez será menor que 10^{-8} cm (el diámetro de un átomo de hidrógeno) o que la frecuencia de reloj será mayor a 10^{15} Hz (la frecuencia de las transiciones atómicas).

Es en este punto en el cual surge un problema, porque a escala atómica las leyes física que gobiernan el comportamiento y las propiedades del circuito son inherentemente de naturaleza cuántica, no clásica. Esto por tanto planteó la cuestión de si un nuevo tipo de computador podría ser concebido sobre los principios de la física cuántica.

Feynman estuvo entre los primeros en tratar de responder a la pregunta produciendo un modelo abstracto en 1982 que mostraba como un sistema cuántico podría ser utilizado para realizar cálculos computacionales. También explicó como tal máquina sería capaz de actuar como un simulador de física cuántica. En otra palabras, un físico tendría la habilidad de llevar a cabo experimentos de física cuántica dentro de un ordenador de mecánica cuántica.

Benioff consideró un modelo mecánico cuántico de computadores y el proceso computacional[9]. Mientras que Feynman empezó desde una perspectiva diferente,

[7] Manasi Karkare, Applied Physics II, Nueva Delhi, I.K. International Publishing House, 2008, pag 157

[8] La ley de Moore expresa que aproximadamente cada dos años se duplica el número de transistores en un microprocesador.

[9] Paul Benioff, The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines, Journal of Statistical Physics, Volumen 22 - Issue 5, 1980, pag 563-591

preguntándose qué tipo de computadores podrían ser utilizados para simular Física[10]. Deutsch analizó el rol del paralelismo cuántico, el cual es el elemento clave en la teoría de los algoritmos cuánticos y comentó sobre el rol de la teoría de la complejidad cuántica[11], también expandió el concepto de los circuitos computacionales cuánticos[12].

En 1985, Deutsch cayó en cuenta que la afirmación de Feynman podría eventualmente llevar a un computador cuántico de propósito general y publicó un documento teórico mostrando que cualquier proceso físico, en principio, podría ser modelado perfectamente por un computador cuántico. Por tanto, un computador cuántico tendría habilidades más allá de aquellas encontradas en un computador clásico. Después de que Deutsch publicara su estudio, la investigación empezó para encontrar aplicaciones interesantes para tal máquina.

Desafortunadamente, todo lo que fue posible encontrar fueron unos pocos problemas matemáticos, hasta que Shor divulgó en 1994 una reimpresión de un documento en el cual establecía un método para utilizar un computador cuántico para atacar un importante problema en la teoría de los números, denominado factorización. Demostró como un conjunto de operaciones matemáticas, designadas específicamente para un computador cuántico podían ser organizadas para permitir a tal máquina factorizar grandes números en tiempos extremadamente cortos, mucho más rápido de lo que es posible en computadores convencionales. Con este avance, la computación cuántica se transformó de una curiosidad meramente académica directamente a un interés mundial.

En 1998, científicos del Laboratorio Nacional de los Álamos lograron construir el primer computador cuántico de 3 qubits, capaz de realizar operaciones matemáticas de carácter simple. En el año 2000, el mismo laboratorio logró crear un computador cuántico de 7 qubits en una gota de líquido. Investigaciones de NEC (Nipon Electronic Company), empresa electrónica de Japón, demostraron en febrero de 2003 que tenía la capacidad para entrelazar 2 qubits en un superconductor, un componente que puede construirse dentro de un chip de silicio. Seis meses después un equipo australiano logró construir una puerta cuántica lógica con partículas de luz.

[10] Richard Feynman, The Feynman Lectures on Physics, New York, Addison Wesley, 1970, pag 467
[11] David Deutsch, Quantum Theory: The Church-Turing Principle and the Universal Quantum Computer, The Royal Society, Volumen 400 - Issue 1818, 1985, pag 70
[12] David Deutsch, Quantum Computational Networks, Proc. Royal Society London, Volumen 425, 1989, pag 73-90

1.3. El potencial y poder de la computación cuántica

En un computador tradicional, la información es codificada en una serie de bits, y estos bits son manipulados mediante puertas lógicas booleanas arregladas en una sucesión para producir un resultado final. De forma similar, un computador cuántico manipula qubits ejecutando una serie de puertas cuánticas, con una transformación unitaria actuando sobre un solo qubit o par de qubits. Al aplicar estas puertas en sucesión, un computador cuántico puede realizar complicadas transformaciones unitarias a un conjunto de qubits en algún estado inicial. Los qubits pueden entonces ser medidos, esta medida es el resultado computacional final. Esta similitud en cálculos entre un computador clásico y un computador cuántico permite que en teoría, un computador clásico pueda adecuadamente simular un computador cuántico. En otras palabras un computador clásico puede ser capaz de hacer cualquier cosa que un computador cuántico puede. Entonces, ¿por qué molestarse con computadores cuánticos? Aun cuando un computador clásico puede teóricamente simular un computador cuántico, es increíblemente ineficiente, tanto que un computador clásico es efectivamente incapaz de realizar muchas tareas que un computador cuántico podría realizar con facilidad. La simulación de un computador cuántico en un computador clásico es un problema computacionalmente difícil debido a que las correlaciones entre los bits cuánticos son cualitativamente diferentes de las correlaciones entre los bits clásicos, como explicó en un inicio John Bell. Tomando por ejemplo un sistema de solo unos cientos de qubits, que existe en un espacio de Hilbert de dimensión $\sim 10^{90}$, que en simulación requeriría que un computador clásico trabaje con matrices exponencialmente grandes (para realizar cálculos sobre cada estado individual, el cual también se representa como una matriz), lo cual significa que tomaría un tiempo exponencialmente más grande que incluso en un computador cuántico primitivo.

Richard Feynman estuvo entre los primeros en reconocer el potencial de la superposición cuántica para resolver tales problemas mucho más rápido. Por ejemplo un sistema de 500 qubits, el cual es imposible de simular clásicamente, representa una superposición cuántica de hasta 2^{500} estados. Cada estado puede ser clásicamente equivalente a una lista simple de 500 1's y 0's. Cualquier operación cuántica sobre ese sistema – un pulso particular de ondas de radio, por ejemplo, cuya acción puede ser ejecutar una operación NOT controlada sobre dos qubits – simultáneamente operaría sobre todos los 2^{500} estados. Por lo tanto haciendo una analogía, con un ciclo del reloj del computador, una operación cuántica

podría computar no solo en un estado de la máquina, como lo harían los computadores clásicos, sino sobre los 2^{500} estados de la máquina al mismo tiempo. Eventualmente, sin embargo, observar el sistema podría causar que colapse a un solo estado cuántico correspondiente a una sola respuesta, una sola lista de 500 1's o 0's, como es dictado por el axioma de medida de la mecánica cuántica. La razón de este interesante resultado se debe a esta respuesta, derivada del paralelismo cuántico alcanzado mediante la superposición, es el equivalente a realizar la misma operación en un super computador clásico con $\sim 10^{150}$ procesadores separados (lo cual es por supuesto imposible).

Los primeros investigadores en este campo estuvieron claramente emocionados por el potencial de tan inmenso poder computacional, y tan pronto como descubrieron este potencial, el objetivo fue encontrar algo interesante para hacer con un computador cuántico. Peter Shor, un investigador y científico en los Laboratorios Bell de AT&T en New Jersey, proveyó tal aplicación al divisar el primer algoritmo para la computación cuántica en 1994. [13]

La factorización de enteros se considera computacionalmente imposible para grandes enteros que son el producto de solo unos pocos números primos (dos números primos de 300 dígitos)[14]. En comparación, un computador cuántico puede eficientemente resolver este problema utilizado el Algoritmo de Shor para encontrar sus factores.

El método obvio para factorizar un número entero x en primos es intentar dividir x para todos los números comprendidos entre 2 y $\sqrt{x}$, si x tiene *n* dígitos (representado en su forma binaria), se requiere realizar aproximadamente $2^{n/2}$ intentos. Existe un ingenioso algoritmo que resuelve el problema en aproximadamente $\exp(cn^{1/3})$ pasos (c es una contante). Pero incluso así, para factorizar un número de un millón de dígitos, un tiempo igual a la edad del universo no sería suficiente. Pueden existir algoritmos más efectivos, pero al parecer es imposible deshacerse del exponencial.

El Algoritmo de Shor utiliza el poder de la superposición cuántica para factorizar rápidamente números muy grandes (en el orden de $\sim 10^{200}$ dígitos y superior) en cuestión de segundos. La primera aplicación de un computador cuántico capaz de implementar este algoritmo descansa en el campo de la encriptación, en el sentido de que sería posible en un

[13] Peter Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal of Computing, No 26, 1997, pag 1489-1509
[14] Varios, Proceedings of the International Conference on Inter Disciplinary Research in Engineering and Technology, Association of Scientists Developers and Faculties, 2da edición, 2015, pag 147

tiempo polinomial resolver el problema donde un común (y el mejor) de los códigos de encriptación, conocido como RSA, se basa principalmente en la dificultad de factorizar números compuestos muy grandes (o el problema del logaritmo discreto que también puede ser resuelto por el algoritmo de Shor). Un computador que pueda hacer esto fácilmente es naturalmente de gran interés para numerosas agencias del gobierno que usan RSA – anteriormente considerado como "inviolable" – y cualquiera interesado en privacidad electrónica y financiera.

Estos métodos son utilizados para asegurar páginas web, encriptar correos electrónicos y muchos otros tipos de datos. Romperlos tendría implicaciones importantes en la privacidad y seguridad electrónica. El único camino para incrementar la seguridad de un algoritmo como RSA sería incrementar el tamaño de la clave y esperar que un adversario no tenga los recursos suficientes para construir y utilizar un computador cuántico suficientemente poderoso.

Una forma de escapar a este dilema sería utilizar algún tipo de criptografía cuántica. También existen algunos esquemas de firmas digitales que se creen son seguros frente a un computador cuántico. Como por ejemplo las firmas Lamport.

"La encriptación sin embargo, es solo una de las aplicaciones de un computador cuántico. Además, Shor ha juntado una caja de herramientas de operaciones matemáticas que solo pueden ser realizadas por un computador cuántico, muchas de las cuales ha utilizado en su algoritmo de factorización. Feynman ha afirmado que un computador cuántico podría funcionar como un simulador de física cuántica, potencialmente abriendo puertas a muchos descubrimientos en el campo."[15]

El bien conocido problema de la búsqueda de base de datos cuántica, el cual puede ser resuelto por el algoritmo de Grover utiliza cuadráticamente menos consultas a la base de datos de las que son requeridas por los algoritmos clásicos. En este caso la ventaja es palpable. Muchos otros casos similares han sido descubiertos, como por ejemplo encontrar colisiones en funciones dos a uno y evaluar árboles NAND.

Tomando en consideración un problema con estas cuatro propiedades:

1. La única manera de resolverlo es proponer respuestas repetidamente y verificarlas,
2. Existen *n* respuestas posibles por verificar,
3. Cada respuesta posible toma la misma cantidad de tiempo en ser verificada, y

[15] Varios, Proceedings of the International Conference on Inter Disciplinary Research in Engineering and Technology, Association of Scientists Developers and Faculties, 2da edición, 2015, pag 147

4. No existe una indicación sobre cuales respuestas pueden ser mejores; generar posibilidades aleatoriamente es tan bueno como verificarlas en un orden específico.

Un ejemplo de esto es encontrar la palabra clave de un archivo protegido. Para problemas con estas cuatro propiedades, el tiempo que un computador cuántico tardaría en resolverlo sería proporcional a la raíz cuadrada de n. Lo cual puede ser un gran adelanto, reduciendo problema de años a segundos. Puede ser utilizado para atacar sistemas de cifrado simétrico como Triple DES y AES intentando dar con la clave privada.

Actualmente el poder y capacidad de un computador cuántico es principalmente especulación teórica; el advenimiento del primer computador cuántico completamente funcional indudablemente traerá muchas, nuevas e interesantes aplicaciones.

1.4. Obstáculos e Investigación

El campo del procesamiento de información cuántica ha hecho numerosos avances prometedores desde su concepción, incluyendo la construcción de computadores de dos y tres qubits capaces de algunas operaciones matemáticas simples y clasificación de datos. Sin embargo, unos pocos obstáculos potencialmente grandes todavía restan, los cuales evitan simplemente construir un computador cuántico que pueda rivalizar con los computadores modernos.

Existen algunas dificultades prácticas al momento de construir un computador cuántico, y por tanto, los computadores cuánticos solo han resuelto una serie de problemas triviales. David DiVincenzo, de IBM, ha listado algunos de los requerimientos para un computador cuántico práctico[16]:

- Escalabilidad física para incrementar el número de qubits.
- Qubits que puedan ser inicializados a valores arbitrarios.
- Puertas cuánticas más rápidas que el tiempo de decoherencia.
- Un conjunto de puertas universal.
- Qubits que puedan ser leídos fácilmente.

Para resumir los problemas desde la perspectiva de un ingeniero, es necesario resolver el reto de construir un sistema el cual esté aislado de todo, excepto de los mecanismos de medida y manipulación. Incluso, es necesario apagar el acoplamiento de los qubits a la medida, de manera que no se presente decoherencia mientras se realizan operaciones sobre ellos.

Entre estas dificultades la corrección de errores, decoherencia, y arquitectura del hardware son probablemente las más formidables. La corrección de errores prácticamente se explica a sí misma, pero, ¿qué errores necesitan corrección? La respuesta es principalmente aquellos productos de la decoherencia, o la tendencia de un computador cuántico a decaer de un estado cuántico dado a un estado incoherente mientras interactúa, o se "entrelaza", con el estado del ambiente. Estas interacciones entre el ambiente y los qubits son inevitables, e inducen el decaimiento de la información almacenada en un computador cuántico y, por tanto, errores en el cálculo. Antes de que cualquier computador cuántico sea capaz de

16 David P. DiVincenzo, IBM (2000-04-13). "The Physical Implementation of Quantum Computation". Retrieved on 2006-11-17.

resolver problemas complicados, la investigación debe idear un camino para lidiar con la decoherencia y otras potenciales fuentes de error en un nivel aceptable. Gracias a la teoría (y ahora realidad) de la corrección de errores cuánticos, propuesta inicialmente en 1995 y desarrollada continuamente desde entonces, computadores cuánticos de pequeña escala han sido construidos y las perspectivas de computadores cuánticos más avanzados son prometedoras.

Probablemente la idea más importante en este campo es la aplicación de corrección de errores en fase de coherencia como un medio de extraer la información y reducir el error en un sistema cuántico sin tomar mediciones en el sistema. En 1998, investigadores del Laboratorio Nacional de los Alamos y el MIT liderados por Raymond Laflamme lograron propagar un solo bit de información cuántica (qubit) a través de tres espines nucleares en cada molécula de una solución líquida de alanita o moléculas de tricloroetileno. Lo lograron utilizando técnicas de resonancia magnética nuclear (NMR por sus siglas en inglés). Este experimento es significativo, porque propagar la información la hace difícil de corromper. La mecánica cuántica nos dice que una medición directa del estado de un qubit, invariablemente destruye la superposición de estados en la cual existe, forzándolo a convertirse en 0 o 1. La técnica de propagar la información permite a los investigadores utilizar la propiedad de "entrelazamiento" para estudiar las interacciones entre estados como un método indirecto para análisis de la información cuántica en lugar de una medición directa; el grupo comparó los spines para verificar si alguna diferencia surgía entre ellos sin conocer la información en sí. Esta técnica les dio la habilidad para detectar y corregir errores, en la fase de coherencia de un qubit, y por tanto mantener un mayor nivel de coherencia en el sistema cuántico. Este hito ha proveído un argumento contra los escépticos, y esperanza para los creyentes. Actualmente, la investigación en la corrección de errores continúa con grupos en el Caltech (Preskill, Kimble), Microsoft, Los Alamos, y cualquier otro lugar.

Hasta este punto, solo unos pocos de los beneficios de la computación cuántica y los computadores cuánticos son palpables, pero antes de que más posibilidades sean develadas, la teoría debe ser puesta a prueba. Para ello, dispositivos capaces de computación cuántica deben ser construidos. El hardware para computación cuántica está, sin embargo, todavía en su infancia. Como resultado de algunos experimentos significativos, la resonancia magnética nuclear (NMR) ha llegado a ser el componente más popular dentro de la arquitectura de hardware cuántico. En 1999 un grupo del Laboratorio Nacional de los Alamos y el MIT construyeron las primeras demostraciones experimentales de un computador cuántico

utilizando tecnología basada en resonancia magnética nuclear (NMR). Actualmente, investigaciones están en curso para combatir los efectos destructivos de la decoherencia, para desarrollar una arquitectura de hardware óptima para el diseño y construcción de un computador cuántico, y para avanzar más en los algoritmos cuánticos que utilicen el inmenso poder computacional que yace en estos dispositivos. Naturalmente esta búsqueda está íntimamente relacionada a códigos de corrección de errores cuánticos y algoritmos cuánticos, de manera que un sinnúmero de grupos avanzan simultáneamente sobre estos campos de investigación. A la fecha, los diseños involucran trampas de iones, electrodinámica de cavidades cuánticas (QED por sus siglas en inglés) y NMR. A pesar de que estos dispositivos han tenido un éxito moderado en desarrollar experimentos interesantes, cada tecnología tiene serias limitaciones. Los computadores de trampas de iones se ven limitados en velocidad por la frecuencia de vibración de los modos en la trampa. Los dispositivos NMR tienen una atenuación exponencial de la señal al ruido de manera proporcional al número de qubits en el sistema. QED es ligeramente más prometedor, sin embargo, todavía solo ha sido demostrado con unos pocos qubits. Seth Lloyd de MIT es actualmente un prominente investigador en hardware cuántico. El futuro de la arquitectura de hardware cuántico probablemente será muy diferente de lo que conocemos hoy, sin embargo, las investigaciones en curso han ayudado a proporcionar una visión sobre los obstáculos que el futuro guarda para estos dispositivos.

1.5. Candidatos para un computador cuántico

Existe un cierto número de candidatos para un computador cuántico, entre ellos:

- Computadores cuánticos basados en superconductores[17].
- Computadores cuánticos de trampas de iones.

Esta es la idea inicialmente propuesta y mejor desarrollada, y existe en algunas variaciones. Para representar un bit cuántico se pueden utilizar tanto los niveles de electrones usuales como los niveles de estructuras finas y superfinas. Existe una técnica experimental para almacenar un ion o átomo en la trampa de un campo magnético estable o un campo eléctrico alternante durante un periodo de tiempo razonable (una hora). El ion puede ser enfriado (su movimiento de vibración es eliminado) con la ayuda de un rayo láser. Seleccionando la vibración y la frecuencia de los pulsos láser es posible preparar una superposición arbitraria. En esta forma es bastante fácil controlar los iones individuales. Dentro de la trampa se pueden colocar dos o más iones a distancia de unos pocos micrones uno de otro, y controlar cada uno de ellos individualmente. Sin embargo, es bastante difícil coordinar las interacciones entre los iones. Ha sido propuesto que modos de vibración colectiva (vibraciones mecánicas ordinarias con una frecuencia de algunos MHz) sean utilizados. Interacciones dipolo-dipolo también podrían ser utilizadas con la ventaja de ser bastante más rápidas. Un segundo método (para átomos neutrales) consiste en colocar átomos en resonadores electromagnéticos separados que están conectados uno con otro (al momento no está claro todavía como lograrlo). Finalmente un tercer método utiliza varios rayos láser creando un potencial periódico el cual atrapa varios átomos sin excitar; un átomo en estado excitado se puede mover libremente interactuando con sus vecinos.

- Computadores cuánticos topológicos o Aniones.

Los aniones son cuasi-partículas (excitaciones) en ciertos sistemas cuánticos de dos dimensiones, por ejemplo un líquido de electrones bidimensional en un campo magnético. Lo que los hace especiales son sus propiedades topológicas, las cuales son estables a las variaciones moderadas de los parámetros del sistema.

La dificultad fundamental en construir un computador cuántico es la necesidad de realizar transformaciones unitarias con una precisión $\delta < \delta_0$ en donde δ_0 se encuentra entre

17 Clarke, John; Wilhelm, Frank (June 19, 2008), "Superconducting quantum bits", Nature 453: 1031–1042, doi:10.1038/nature07128, http://www.nature.com/nature/journal/v453/n7198/full/nature07128.html

10^{-2} y 10^{-6}.[18] Para lograr esto es necesario, como regla, controlar los parámetros del sistema todavía con mayor precisión. Sin embargo, que sucedería si existiera un sistema en donde la alta precisión es alcanzada automáticamente, por ejemplo donde la corrección de error ocurra en el nivel físico. Un ejemplo es el sistema propuesto bidimensional con excitaciones de aniones.

Es de notar que la discusión no se trata sobre partículas fundamentales, como un electrón, sino sobre excitaciones ("defectos") en un líquido de electrones bidimensional. Tales excitaciones se pueden mover o transformarse entre sí, tal como partículas "genuinas"[19]. Sin embargo las excitaciones en un líquido bidimensional muestran algunas propiedades inusuales. Una excitación puede tener un cambio fraccional (por ejemplo 1/3 de la carga de un electrón). Si una excitación realiza un cambio completo sobre otra, el estado del líquido de electrones circundante cambia en una forma precisamente definida que depende de los tipos de excitaciones y la topología del camino, pero no de la trayectoria específica. En el caso más simple, la función de onda se multiplica por un número (el cual es igual a $e^{2\pi i/3}$ para aniones en un líquido de electrones dos dimensional en un campo magnético al factor de llenado 1/3). Excitaciones con tales propiedades son conocidas como aniones abelianos.

Más interesantes son los aniones no abelianos; en cuya presencia, el estado del líquido de electrones circundante degenera, la multiplicidad de la degeneración depende del número de aniones. En otras palabras, no existe uno, sino muchos estados, los cuales pueden presentar superposiciones cuánticas arbitrarias. Es imposible actuar sobre tal superposición sin mover los aniones, de manera que el sistema está idealmente protegido contra perturbaciones. Si un anión se mueve alrededor de otro, la superposición pasa por una cierta transformación unitaria. Esta transformación es absolutamente precisa (Un error puede ocurrir solamente si el anión se torna fuera de control como resultado de un túnel cuántico).

Para realiza un computador cuántico, se necesita controlar cada excitación en el sistema, las cuales probablemente se encuentren apartadas entre sí por una fracción de un micrón. Este es un problema técnico extremadamente complejo.

- Puntos cuánticos sobre superficie.

18 Ver corrección de errores cuánticos.
19 Las partículas fundamentales también pueden considerarse como excitaciones en el vacío, el cual es, en realidad, un sistema cuántico no trivial. La diferencia es que el vacío es único, mientras que el líquido de electrones u otro "medio cuántico" pueden ser diseñados de acuerdo a las necesidades.

Un punto cuántico es una microestructura que puede contener unos pocos electrones o incluso un solo electrón. El spin de este electrón puede ser utilizado como qubit. Bajo temperaturas superfrías, el único grado de libertad de un pequeño punto cuántico es su carga. Cambiando el potencial eléctrico externo se puede alcanzar una situación en donde dos estados de carga tienen casi la misma energía y utilizarlo como estado inicial. La dificultad es que se necesita controlar cada punto cuántico individualmente con alta precisión. Esto es más difícil que en el caso de átomos libres porque todos los átomos del mismo tipo son idénticos, mientras que los parámetros de las estructuras fabricadas fluctúan.

- Resonancia magnética nuclear sobre moléculas en solución (NMR).

En una molécula con varios spines nucleares diferentes, una transformación unitaria arbitraria puede ser realizada mediante una sucesión de pulsos de campo magnético. Esto ha sido probado experimentalmente a temperatura ambiente. Sin embargo para la preparación de un estado inicial viable una temperatura menor a 10^{-3}K es necesaria. Además de estas dificultades con el enfriamiento, las interacciones indeseables entre las moléculas se incrementan a medida que el líquido se enfría. Y es muy difícil seleccionar un spin dado selectivamente si la molécula tiene varios spines del mismo tipo.

Estos son algunos ejemplos de propuestas de computadores cuánticos con esta técnica:

- NMR de estado sólido o computadores cuánticos Kane.
- Computadores cuánticos de electrones en helio.
- Electrodinámica de cavidad cuántica (CQED).
- Magneto molecular,
- Computador cuántico ESR basado en fullereno.
- Computador cuántico basado en óptico.
- Computador cuántico basado en diamantes[20].
- Computador cuántico basado en condensación Bose-Einstein[21].
- Computador cuántico basado en transistores.

20 Wolfgang Gruener, TG Daily (2007-06-01). "Research indicates diamonds could be key to quantum storage". Retrieved on 2007-06-04.
Neumann, P.; Mizuochi, N.; Rempp, F.; Hemmer, P.; Watanabe, H.; Yamasaki, S.; Jacques, V.; Gaebel, T.; et al. (June 6, 2008), "Multipartite Entanglement Among Single Spins in Diamond", Science 320 (5881): 1326–1329, doi:10.1126/science.1157233, PMID 18535240, http://www.sciencemag.org/cgi/content/abstract/320/5881/1326
21 Rene Millman, IT PRO (2007-08-03). "Trapped atoms could advance quantum computing". Retrieved on 2007-07-26.

- Computador cuántico basado en spin.
- Computador cuántico adiabático[22].

El gran número de candidatos muestra explícitamente que el tema, a pesar del rápido progreso, está todavía en su infancia, pero al mismo tiempo existe una gran flexibilidad.

En 2005, investigadores en la Universidad de Michigan construyeron un chip semiconductor el cual funcionaba como una trampa de iones. Tal dispositivo, producido con técnicas de litografía estándar, puede apuntar hacia el camino para herramientas de computación cuántica escalables[23]. Una versión mejorada fue construida en 2006.

22 William M Kaminsky, MIT (Date Unknown). "Scalable Superconducting Architecture for Adiabatic Quantum Computation". Retrieved on 2007-02-19.
23 Ann Arbor (2005-12-12). "U-M develops scalable and mass-producible quantum computer chip". Retrieved on 2006-11-17.

1.6. Problemas propuestos

En un computador cuántico es posible modelar un sistema cuántico arbitrario en muchos pasos de manera polinómica. Esto permitiría predecir las propiedades de las moléculas y los cristales y diseñar dispositivos electrónicos microscópicos, por ejemplo, de un tamaño de 100 átomos. Tales dispositivos descansan en el abismo del poder tecnológico al momento, pero en el futuro es posible que sean los elementos comunes de los computadores ordinarios.

Un segundo ejemplo es la factorización de enteros en primos y los problemas de la teoría de números análogos. El algoritmo cuántico que propuso Shor en 1994 permite factorizar un entero de n dígitos en aproximadamente n^3 pasos[24]. Aun cuando este resultado puede tener consecuencias negativas, pues la factorización permitiría romper el criptosistema más comúnmente utilizado: RSA, los usuarios pueden descansar tranquilos pues no existe el computador cuántico que lo pueda hacer todavía.

Un tercer ejemplo es la búsqueda de un registro dentro de una base de datos no ordenada. La ganancia no es tan significativa, para localizar un registro entre N elementos se necesita $\sqrt{N}$ de pasos en un computador cuántico en comparación con los N pasos en uno clásico.

Existen mucho más en el tema de la computación cuántica y los campos similares. Por ejemplo, en 1984 Charles Bennett y Giles Brassard [25]introdujeron un sistema de distribución de llaves basado en los principios de la computación cuántica. El objetivo es permitirle al emisor y al receptor (llamados comúnmente Alice y Bob) construir de forma segura una secuencia de llaves para encriptación utilizando las propiedades de los fotones. De esta manera, concurrentemente con computadores cuánticos y algoritmos cuánticos, los campos de la criptografía cuántica y la comunicación cuántica han sido desarrollados, llevando a la teoría de la información cuántica y a los problemas de complejidad relacionados.

24 “Algoritmos para computación cuántica: logaritmos discretos y factorización” por Peter Shor
25 “Criptografía cuántica: distribución de llaves públicas y lanzamiento de la moneda” por Charles H. Bennett y Guilles Brassard

1.6.1 Encriptación Cuántica

La gente ha enviado mensaje codificados durante miles de años. Pero siempre que los criptógrafos piensan que han logrado crear un método indescifrable – como ocurrió con la máquina Enigma en la Segunda Guerra Mundial – alguien, – los polacos en este caso - logra descifrar el código. Los códigos modernos evitan este problema teniendo una estructura tan complicada que la solución, aunque posible de obtener, tardaría años en ser calculada aun utilizando el más potente de los computadores. En este punto es donde la encriptación cuántica muestra un gigantesco potencial. Ciertamente, se trata de uno de los campos de desarrollo más prometedores en el mundo de la mecánica cuántica.

La encriptación cuántica fue una creación de Charles Bennett y Giles Brassard (que formaban parte del equipo que propuso inicialmente la idea del teletransporte). Se trataba de encriptar un mensaje utilizando la polarización de fotones (las distintas direcciones en las que puede vibrar una partícula de luz). Si alguien trata de interceptar un mensaje codificado mediante técnicas cuánticas, el propio acto de la interceptación haría que las partículas estuvieran en un estado especial y el mensaje quedaría alterado. Asimismo, estas técnicas permitirían que el emisor y el receptor (Alice y Bob) supieran que su línea cuántica ha sido franqueada. Y, lo que resulta más importante, debido a la naturaleza cuántica de esta clase de encriptación, todos los mensajes codificados mediante técnicas cuánticas serían indescifrables.

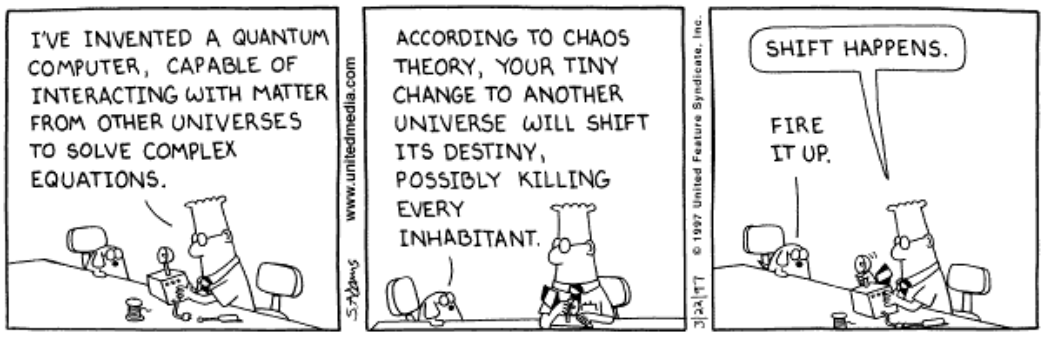
La teoría de Brassard y Bennett fue llevada a la práctica en 1988 cuando se envió el primer código cuántico entre dos computadores situados a una distancia de 30 centímetros. En 1995, un equipo de la Universidad de Ginebra incrementó esta distancia hasta 23 kilómetros utilizando fibra óptica para enviar los fotones. En enero de 2003, la Universidad de Ginebra volvió a anunciar un avance en este campo: se trataba del primer proceso de teletransporte a larga distancia, hecho publicado en la revista Nature. Los científicos han teletransportado fotones a una distancia de 2 kilómetros utilizando la fibra óptica que se emplea en los cables de comunicación estándar. Esto constituyó un desarrollo significativo para todos aquellos que estaban interesados en el envío de mensajes encriptados, ya que los fotones solo pueden desplazarse utilizando sus propios medios, lo cual permite pensar en la posibilidad de utilizar el teletransporte como repetidor para copiar el mensaje, permitiendo enviar dicho mensaje a través de cables y alcanzar cualquier sitio deseado. Este no es el

único método posible, Arthur Ekert sugirió utilizar el entrelazamiento para la encriptación, procedimiento que también fue comprobado experimentalmente.

En junio de 2003, científico británicos de Toshiba Research Europe Ltd. en Cambridge, lograron utilizar criptografía cuántica en una red de 100 kilómetros de fibra óptica.

1.7. Mirada al futuro de la computación cuántica

Al momento, los computadores cuánticos y la tecnología de la información cuántica siguen siendo pioneros. En este mismo instante los obstáculos están siendo superados de manera que proveerán el conocimiento necesario para empujar los computadores cuánticos hasta su correspondiente posición como las máquinas computacionales más rápidas existentes. La corrección de errores ha hecho progresos prometedores a la fecha, acercándose al punto en el cual podríamos tener las herramientas requeridas para construir un computador cuántico suficientemente robusto como para adecuadamente resistir los efectos de la decoherencia. El hardware quántico, por otro lado, se mantiene en un estado emergente, pero el trabajo hecho hasta la fecha sugiere que solo es cuestión de tiempo antes de que tengamos dispositivos los suficientemente grandes como para probar el algoritmo de Shor y algunos otros. Por ello, los computadores cuánticos emergerán como dispositivos computacionales superiores al final, y tal vez un día volverán los computadores modernos obsoletos. La computación cuántica tiene sus orígenes en campos altamente especializados de la física teórica, pero su futuro indudablemente descansa en el efecto profundo que tendrán en la vida de toda la humanidad.

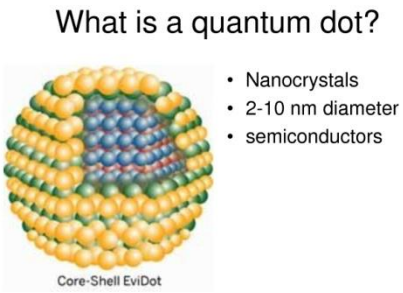


Los problemas involucrados en crear dispositivos microfísicos estables para bits cuánticos han motivado experimentos que se encuentran al borde mismo de la tecnología actual. En verdad, todavía existen preguntas sobre la última viabilidad de un computador cuántico suficientemente complejo como para implementar el algoritmo de Shor para un incluso modesto N.

Es muy posible que el diseño de un computador ordinario haya sido percibido como una idea muy atractiva y muy irreal en la época de Charles Babbage, cuya invención se llegó a realizar luego de cien años. Es de esperar que en la época actual la ciencia y la tecnología se desarrollen mucho más rápido, de manera que la espera no sea tan grande.

1.7.1 Puntos Cuánticos

Los puntos cuánticos son pequeñas partículas de materiales semiconductores con diámetros de 2 a 10 nm (10 a 50 átomos)[26].



Tienen propiedades eléctricas únicas, una de las cuales es la electroluminiscencia, dependiendo del material y diámetro utilizados se producen diferentes colores.

[26] Varios, Quantum Dots, http://www.sigmaaldrich.com/materials-science/nanomaterials/quantum-dots.html, Acceso: 13/12/2015

Su utilización como candidatos para un computador cuántico se debe a que pueden ser afectados por diferentes longitudes de ondas electromagnéticas, de manera que solo reaccionan en presencia de dicha onda.

Sin embargo también se consideran en la industria de aparatos electrónicos de consumo masivo, específicamente en la producción de televisores. En el evento internacional CES (Consumer Electronics Show) del año 2015 varios fabricantes presentaron sus dispositivos utilizando puntos cuánticos. La ventaja de su utilización radica en el consumo eficiente de energía, mejor al de un panel LCD y comparable a un OLED y en los colores nítidos que son capaces de producir.[27]

Samsumg llama a la tecnología que utiliza puntos cuánticos "semiconductores de nano-cristales", mientras que Sony la denomina Triluminos.

1.7.2 Computador cuántico D-Wave

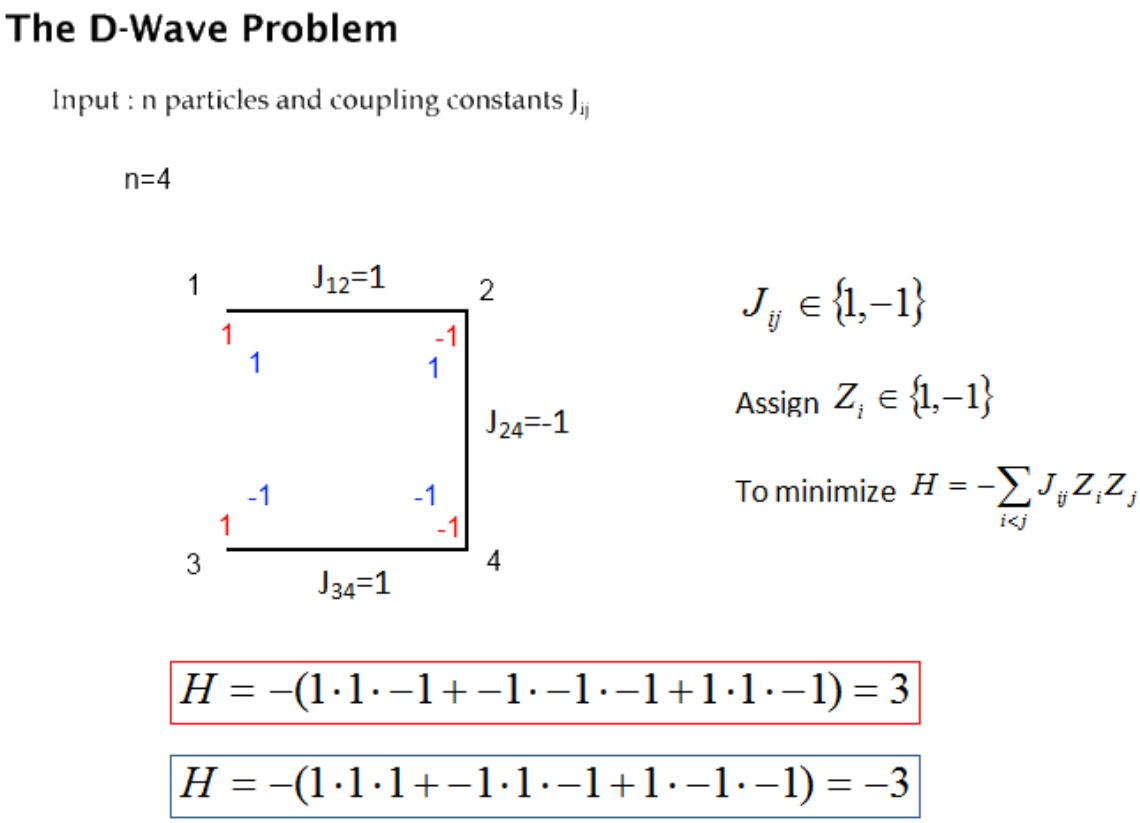
D-Wave es el computador cuántico de la compañía canadiense del mismo nombre, el cual ha sido publicitado desde el 2007 y en mayo del 2013 fue comprado por una asociación entre Google y la Nasa por 15 millones de dólares.[28]

Este computador utiliza una aplicación de la mecánica cuántica denominada computación cuántica adiabática y el acceso al mismo es restringido solo a unos pocos grupos de investigadores. Es por ello que su veracidad ha sido puesta en duda y luego de que un equipo de investigadores publicara los datos de prueba y resultados obtenidos, se he podido replicar el problema de minimización para el cual D-Wave fue diseñado en computadores clásicos como una laptop obteniendo las mismas velocidades de respuesta e igual o mejor probabilidad de alcanzar la solución.[29]

El problema que resuelve D-Wave es el siguiente: dados n puntos, conectados entre sí por constantes que pueden ser 1 o -1 (no necesariamente todos los puntos se conectan entre sí), se debe minimizar la sumatoria de la multiplicación de los puntos por la constante que

[27] Tim Moynihan, What Are Quantum Dots, and Why Do I Want Them in My TV?, http://www.wired.com/2015/01/primer-quantum-dot/, Acceso: 13/12/2015
[28] Nicola Jones, Google and NASA snap up quantum computer, http://www.nature.com/news/google-and-nasa-snap-up-quantum-computer-1.12999, Acceso: 13/12/2015
[29] Clive Thompson, The Revolutionary Quantum Computer That May Not Be Quantum at All, http://www.wired.com/2014/05/quantum-computing/, Acceso: 13/12/2015

los une. El objetivo del problema es asignar 1 o -1 a cada punto a fin de encontrar la configuración de menor energía.



Recientemente Google publicó un paper explicando que su computador D-Wave alcanzó una ganancia de velocidad de 100 millones, respecto a un computador clásico de un solo núcleo, en un problema específico cuidadosamente elaborado como prueba de concepto, lo cual indicaría que efectivamente han tocado el corazón de la computación cuántica, ya que esa sería la única explicación para tal mejora en rendimiento. Sin embargo la comunidad científica permanece escéptica, pues una mejora al algoritmo que permite resolver el problema permitiría a un computador normal rivalizar, y hasta mejorar, los tiempos obtenidos por D-Wave.[30]

[30] Tom Simonite, Google Says It Has Proved Its Controversial Quantum Computer Really Works, http://www.technologyreview.com/news/544276/google-says-it-has-proved-its-controversial-quantum-computer-really-works/, Acceso: 13/12/2015

1.7.2 Microsoft LIQUi|>

El 6 de Noviembre de 2015 Microsoft lanzó su lenguaje de simulación cuántica en GitHub, luego de trabajar en el simulador de operaciones cuánticas por más de 3 años con un grupo internacional de científicos.[31]

El objetivo es que LIQUi|> se utilizado para traducir un algoritmo cuántico escrito en forma de sentencias de programación de alto nivel en instrucciones de máquina de bajo nivel para un dispositivo cuántico.

LIQUi|> incluye simulación de circuitos para hasta 30 qubits en una máquina con 32 GB de RAM. El número más grande factorizado utilizando el sistema es de 13 bits (puede representar el hasta el número 8191), el cual requirió 27 qubits, medio millón de puertas cuánticas y 5 días de ejecución.[32]

[31] Mehedi Hassan, Microsoft releases its quantum simulator, Liquid, http://microsoft-news.com/microsoft-releases-its-quantum-simulator-liquid/, Acceso: 13/12/2015
[32] Varios, Language-Integrated Quantum Operations: LIQUi|>, http://research.microsoft.com/en-us/projects/liquid/, Acceso: 13/12/2015

CAPÍTULO II

2. CONCEPTOS ESPECÍFICOS

2.1. Motivación experimental para la mecánica cuántica

Primeramente el experimento de las dos rendijas para electrones: una fuente produce una corriente mono-energética de electrones que se mueven en la dirección *x* positiva. Una pantalla absorbente, perpendicular a la corriente de electrones, tiene dos delgadas rendijas a través de las cuales los electrones pueden pasar en su camino a los contadores en una segunda pantalla colocada detrás de la primera. Si solo una de las rendijas está abierta, los contadores registran un patrón de impactos que se asemeja a una distribución normal truncada, por ejemplo, el tipo de distribución que se esperaría de una corriente de partículas incidiendo en una rendija. Sin embargo, si las dos rendijas están abiertas y suficientemente juntas, la distribución de los impactos muestra interferencia, es decir, la misma distribución de intensidad que se puede observar con ondas de luz monocromática incidiendo en la segunda pantalla. En particular, el patrón de número de incidencias no es la suma de los patrones de incidencias obtenidos al abrir las dos rendijas individualmente.

Es más, dado que el experimento puede ser llevado a cabo de manera que las incidencias de electrones estén separadas en el tiempo, el comportamiento de tipo onda de la interferencia sugiere que cada electrón está de alguna manera interfiriendo con sí mismo, lo cual es completamente inconsistente con la presunción de partículas de que cada electrón pasa solamente por una de las rendijas. Y para hacer las cosas más confusas, se puede demostrar que no importa cuán inteligentemente se intente medir por cual rendija el electrón pasó, el patrón de interferencia es afectado.

El experimento Stern-Gerlach es otro de los experimentos fundamentales que motivan la estructura matemática de la mecánica cuántica. Se ha determinado que una partícula “elemental” tiene un momento angular intrínseco o un “spin” el cual puede ser experimentalmente detectado al emitir una corriente de partículas a través de un campo magnético no homogéneo apropiado. Es más, es un hecho experimental que un efecto de cuantización se observa: en lugar de mostrar un continuo de desviaciones, el haz de partículas es desviado en un número finito de caminos. En particular, se observa que ciertas

partículas tienen "spin ½", lo cual significa que el haz incidente de partículas se divide en exactamente dos sub-haces.

Concretamente, si un haz de partículas preparado cuidadosamente se mueve a través del eje x, y si el campo magnético se genera de manera que tenga un gran componente no homogéneo en una dirección perpendicular al eje x, por ejemplo una dirección z, entonces un sub-haz diverge (arriba) en la dirección z positiva y el otro diverge (abajo) en la dirección z negativa. A pesar de que no se puede predecir si una partícula individual ira hacia arriba o abajo, los dos haces tiene igual intensidad, y se describe a las partículas en el primer sub-haz como spin z arriba o en un estado (z,+) y a las partículas en el segundo sub-haz como spin z abajo o en un estado (z,-). Es más, si una subsecuente medición Stern-Gerlach se realiza sobre el sub-haz (z,+) con la misma orientación relativa, entonces solo un haz emerge, el mismo haz (z,+), como se esperaría intuitivamente. Por tanto, antes del segundo experimento, el comportamiento de las partículas en el sub-haz (z,+) puede ser predicho, emergerán en el estado (z,+).

El mismo fenómeno se observa en otras direcciones, de manera que un subsecuente experimento Stern-Gerlach con la diferencia de homogeneidad en la dirección y, se realiza sobre el sub-haz (z,+), dos nuevos sub-haces se observan, denotados por (y,+) y (y,-) en la notación obvia. De la misma forma, los dos nuevos haces tendrán igual intensidad a pesar de que determinar en cual dirección y una partícula individual va no se puede predecir.

Sin embargo, extrañas cosas empiezan a suceder. Si una segunda medición Stern-Gerlach orientada en z se realiza sobre el sub-haz (y,+) el cual fue seleccionado del sub-haz (z,+), se detectan con igual intensidad tanto un sub-haz (z,+) como uno (z,-). En otras palabras, la medición sobre la dirección y de alguna manera eliminó el efecto de la medición previa sobre la dirección z en las partículas sobrevivientes, y este no es un resultado intuitivo para partículas.

Asumiendo la validez de estas afirmaciones para partículas y el hecho de que la física clásica no puede dar cuenta de ellas, algunas conclusiones se puede hacer. Una de ellas es que, dependiendo de la naturaleza de la observación, las partículas evidencian comportamiento tipo onda y, de acuerdo a otros experimentos, la luz exhibe comportamiento tipo partícula. Una segunda conclusión es que cualquier teoría describiendo el comportamiento de la materia a nivel micro físico no puede ignorar el efecto que una observación tiene sobre el sistema.

Una tercera conclusión es aquella del indeterminismo, la cual se basa en que el resultado de una futura medición en un sistema no puede ser siempre predicha con certeza. En lugar de ello, a nivel micro físico, solo es posible predecir el comportamiento futuro con una cierta probabilidad.

Como parte del análisis subyacente del experimento de las dos rendijas, una cuarta conclusión es que hay un límite a la precisión de mediciones simultáneas de ciertas propiedades físicas como la posición y el momento. Esta conclusión fue alcanzada por Heisenberg en los terrenos físicos y se conoce como el popular principio de incertidumbre de Heisenberg.

Una quinta y crucial conclusión es que se debe distinguir entre la evolución del sistema y la medición del sistema. Enviar una partícula de spin ½ a través de una dispositivo Stern-Gerlach es un ejemplo de lo primero, mientras que medir la trayectoria de la partícula es un ejemplo de lo último.

Estas conclusiones no son triviales para obtenerse a partir de solamente dos ejemplos. Basta con decir que hay todo un cuerpo de evidencia experimental detrás de ellas aun cuando su aceptación y la de los modelos matemáticos subsecuentes no es fácil y la historia del debate sobre varios aspectos de la teoría es extensa y fascinante.

2.1.1 Superposición

La superposición surge fundamentalmente a través de la matemática y del denominado análisis de Fourier, que muestra como una función de onda puede ser contemplada como la suma de distintas funciones de onda. En otras palabras, una onda de gran tamaño puede ser contemplada como la suma superpuesta de muchas ondas más pequeñas. En este caso, cualquier partícula podría ocupar numerosas posiciones y tener varias propiedades. Sólo cuando se efectúa una medición se escoge una determinada posibilidad. Es como tener una bolsa llena de caramelos redondos, y al extraer un caramelo, la posición del resto de caramelos cambiase repentinamente.

En la teoría cuántica una partícula no tiene propiedades definitivas hasta que hayan sido medidas. Es como lanzar una moneda al aire. No se puede afirmar si la moneda caerá de cara o de cruz hasta que caiga definitivamente. Así, mientras la moneda está girando, experimenta una superposición de estados. Las probabilidades son que salga cara, que salga cruz o que al mismo tiempo salga cara y cruz. Una vez que se efectúa la medida (la moneda

cae) aparecen un conjunto particular de propiedades (cara por ejemplo) y el resto de posibilidades se desvanece.

2.1.2 Entrelazamiento

El estado entrelazado (de donde proviene el término "Entrelazamiento" o "Entanglement" en inglés) constituye un concepto que genera mucha confusión. Así mismo, probarlo de una forma experimental no resulta demasiado sencillo. No obstante hay varias formas de producir partículas entrelazadas. Un método se denomina cascada atómica e implica la excitación de un átomo, utilizando radiación ultravioleta o un láser. Los electrones de los átomos obtienen energía extra y cuando alcanzan una determinada cantidad, pueden saltar hasta dos niveles de energía. Cuando vuelven a caer desde dichos niveles, se emiten dos fotones. Estos dos fotones están entrelazados. Sin embargo esto no ocurre con demasiada frecuencia.

Los pares entrelazados también pueden obtenerse cuando un electrón rompe con un positrón – su equivalente en antimateria – y se aniquilan entre sí. También se obtienen como resultado de la aplicación de un láser aun tipo especial de cristales no lineales. Cuando un láser pasa a través de un cristal no lineal, a veces un fotón se divide en dos. Los dos fotones más pequeños tienen una frecuencia que es la mitad de la frecuencia del fotón original y su nivel de energía también es menor. Sólo uno de cada 10 000 millones de fotones ultravioleta produce un par, pero lo más destacable en este caso es que los dos fotones están entrelazados.

Jeff Kimble, del Instituto de Tecnología de California, ha formulado una de las mejores definiciones del estado entrelazado. Dicha definición se formuló en relación con la conexión entre dos partículas entrelazadas: "El estado entrelazado significa que si le haces cosquillas a uno, el otro se ríe".

2.2. Bits y Qubits

Un computador clásico opera sobre una cadena de ceros y unos, por ejemplo 110010111011000, convirtiéndola en otras cadenas similares. Cada posición en dicha cadena se denomina bit y puede contener 0 o 1. Para representar tales cadenas de bits el computador debe contener una colección correspondiente de sistemas físicos, cada uno de los cuales puede existir en dos estados físicos distinguibles no ambiguos, asociados con el valor (0 o 1) del bit abstracto que el sistema físico representa. Tales sistemas físicos podrían ser un interruptor con posiciones de encendido y apagado o un magneto con orientación arriba o abajo.

Una manera de representar el estado de cada bit es mediante el símbolo $|\ \rangle$, dentro del cual se coloca el valor, 0 o 1, representando el estado. Por tanto los dos estados distinguibles de un bit se representan con los símbolos $|0\rangle$ y $|1\rangle$. Como práctica común se llama a estos símbolos el estado del bit; aun cuando en el caso cuántico, "estado" se refiere solamente al símbolo, sin existir una propiedad interna del Qubit que el símbolo represente.

Tomando el caso de la cadena 11001, la caracterización de los estados de los 5 bits es:

$$|0\rangle|1\rangle|0\rangle|0\rangle|1\rangle,$$

Y se puede referir a este objeto como el "estado" de todos los cinco bits. Por tanto, un par de bits pueden tener (o estar) en cualquiera de los cuatro estados posibles:

$$|0\rangle|0\rangle,\ |0\rangle|1\rangle,\ |1\rangle|0\rangle,\ |1\rangle|1\rangle,$$

Tres bits pueden estar en cualquiera de los ocho estados posibles:

$$|0\rangle|0\rangle|0\rangle,\ |0\rangle|0\rangle|1\rangle,\ |0\rangle|1\rangle|0\rangle,\ |0\rangle|1\rangle|1\rangle,\ |1\rangle|0\rangle|0\rangle,\ |1\rangle|0\rangle|1\rangle,\ |1\rangle|1\rangle|0\rangle,\ |1\rangle|1\rangle|1\rangle$$

Y así sucesivamente.

La siguiente representación hace evidente que cuando existen muchos bits , sus productos son a menudo fáciles de leer si se encierra toda la cadena de ceros y unos en un solo símbolo de la forma $|\quad\rangle$ en lugar de tener símbolos separados para cada bit:

$$|000\rangle,\ |001\rangle,\ |010\rangle,\ |011\rangle,\ |100\rangle,\ |101\rangle,\ |110\rangle,\ |111\rangle$$

Cualquiera de las dos formas de representación es válida y depende del contexto para su utilización.

Existe además una tercera forma, la cual es útil cuando se considera que los ceros y unos constituyen la expresión binaria de un entero. Es posible reemplazar las representaciones de los estados de 3 bits por las formas más cortas:

$$|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle$$

A diferencia de las formas de representación anteriores, esta última es ambigua, a menos que se exprese de alguna manera que los símbolos representan los estados de 3 bits. Para ello se utiliza un índice con el número de bits explícitamente:

$$|0\rangle_3, |1\rangle_3, |2\rangle_3, |3\rangle_3, |4\rangle_3, |5\rangle_3. |6\rangle_3. |7\rangle_3$$

Sin embargo, cuando no existe necesidad de notar cuantos bits se representan, puede ser útil utilizar dichos índices para otros propósitos. Por ejemplo, si Alice y Bob poseen cada uno un bit, puede ser conveniente describir el estado del bit de Alice (si tiene el valor de 1) como $|1\rangle_a$ y el Bob (si tiene el valor de 0) como $|0\rangle_b$, y el estado conjunto de los dos como $|1\rangle_a|0\rangle_b$ o $|10\rangle_{ab}$.

Dirac introdujo la notación $|\ \rangle$ en los primeros días de la teoría cuántica, como una manera útil de escribir y manipular vectores. A tales vectores los llamó kets, una terminología que ha sobrevivido hasta este día. En la notación Dirac se puede colocar dentro del símbolo $|\ \rangle$ cualquier cosa que sirva para especificar lo que es el vector. Si, por ejemplo, se habla acerca del desplazamiento de vectores en un espacio tridimensional ordinario, se podría tener el vector:

$$|5 \text{ centimetros al noroeste}\rangle$$

Al utilizar la notación Dirac para representar le estado de un bit o una colección de bits se está sugiriendo que puede haber alguna utilidad al pensar en el estado de bits como vectores. En el caso de bits, no existe mucha, pero puede haber alguna. Sin embargo al generalizar la representación a qubits, llega a ser absolutamente esencial considerarlos como vectores, tanto que el término estado es a menudo tomado como un sinónimo de vector (o precisamente, el vector que representa al estado).

Es necesario explorar que se puede hacer con bits tomando los dos estados $|0\rangle$ y $|1\rangle$ de un solo bit y los representa por dos vectores unitarios ortogonales en un espacio bidimensional. Mientras que esta es una manera curiosa e innecesariamente elaborada de

representar bits, es fundamental e inevitable al tratar con qubits. De manera que trabajar con operaciones simples sobre bits, permite familiarizarse con el formalismo de la mecánica cuántica.

Para representar los vectores en términos de componentes, se pueden representar los dos estados ortogonales de un solo bit, $|0\rangle$ y $|1\rangle$, como vectores columna:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

En el caso de dos bits, el vector corresponde a un espacio de cuatro dimensiones con una base orto normal:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

La notación alternativa para esta base:

$$|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$$

Está deliberadamente diseñada para sugerir multiplicación, y en realidad es una notación abreviada para el producto tensor de los dos vectores de cada uno de los dos bits, escrito en una notación matemática formal como:

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$$

En términos de componentes, el producto tensor $|a\rangle \otimes |b\rangle$ de un vector **a** de *M* componentes denominados a_u y un vector **b** de N componentes denominados b_v es el vector de (MN) componentes indexados por todos los posibles pares MN de índices (*u*, *v*), cuyo componente en la posición (*u*, *v*) es precisamente el producto $a_u b_v$.

Una vez que se mira a los dos estados de un bit como vectores ortogonales unitarios, el producto tensor es en realidad la forma natural de representar estados de varios bits, dado que lleva a la obvia generalización para varios bits de la representación de los estados de un bit como vectores columna. Si se expresan los estados $|0\rangle$ y $|1\rangle$ de cada bit como vectores columna, entonces se puede obtener el vector columna que representa el estado de varios bits mediante la repetida aplicación de la regla para los componentes del producto tensor de dos vectores. El resultado se ilustra en el producto tensor de tres vectores:

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \otimes \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 z_0 \\ x_0 y_0 z_1 \\ x_0 y_1 z_0 \\ x_0 y_1 z_1 \\ x_1 y_0 z_0 \\ x_1 y_0 z_1 \\ x_1 y_1 z_0 \\ x_1 y_1 z_1 \end{pmatrix}$$

Al aplicar esto, por ejemplo, al caso de $|5\rangle_3$, se obtiene:

$$|5\rangle_3 = |101\rangle = |1\rangle|0\rangle|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Si se denominan los componentes verticales del vector de 8 filas 0,1,…,7 desde arriba hacia abajo, el único componente con un valor diferente de cero está en la quinta posición, precisamente la posición especificada por el vector estado en su forma inicial. Esta es en realidad la obvia generalización para varios bits de la representación del vector columna para estados de un bit.

De manera general: la estructura del producto tensor de los estados de varios bits es todo lo que se necesita para que el vector columna de dimensiones 2^n que representa al estado $|m\rangle_n$ tenga todas sus entradas en cero excepto por un único 1 en la m-ésima posición desde arriba.

Es posible cambiar este desarrollo, de manera que el punto de inicio corresponda a la simple regla de que un entero *x* en el rango $0 \le x < N$ es representado por uno de los vectores orto normales N en un espacio N-dimensional. Se puede escoger la base de manera que 0 es representado por un vector columna de N componentes $|0\rangle$ que contiene 0 en cada posición excepto por un 1 en la primera posición y *x* es representado por el vector columna de N componentes $|x\rangle$ que contiene 0 en cada posición excepto por un 1 en la posición *x* de

arriba hacia abajo. Se deriva entonces a partir de la naturaleza del producto tensor que si $N=2^n$ y x corresponde a la expansión binaria $x = \sum_{j=0}^{n-1} x_j 2^j$, entonces el vector columna $|x\rangle_n$ es el producto tensor de los vectores columna de dos componentes $|x_j\rangle$:

$$|x\rangle_n = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes ... \otimes |x_1\rangle \otimes |x_0\rangle$$

Al tratar con estados de *n* bits de la forma anterior, se debe identificar cada uno de los estados individuales del bit *n*, de los cuales están compuestos, dando la potencia de 2 asociada con el bit que representa. De manera que el estado del bit en el extremo derecho representa el bit 0, el estado inmediatamente a su izquierda representa el bit 1 y así sucesivamente.

Esta relación entre el producto tensor de vectores y la notación posicional para enteros no es aplicable solo al sistema binario. Se puede suponer, por ejemplo, que un digito decimal x = 0, 1, …, 9 se representa como un vector columna de 10 componentes $v^{(x)}$ con todos sus componentes en 0 excepto por un 1, x posiciones de arriba hacia abajo. Si el número decimal de n dígitos $X = \sum_{j=0}^{n-1} x_j 10^j$ se representa por el producto tensor $V = v^{(x_{n-a})} \otimes v^{(x_{n-1})} \otimes ... \otimes v^{(1)} \otimes v^{(0)}$, entonces V será un vector columna de 10^n componentes con todos sus componentes en 0 excepto por un 1, x posiciones desde arriba hacia abajo.

A pesar de que las representaciones de los estados de bits mediante vectores columna claramente muestran por que el producto tensor brinda una descripción natural de los estados de múltiples bits, para casi todos los propósitos es mejor y mucho más simple dejar de lado los vectores columna y componentes y trabajar directamente con los vectores estado en sus formas abstractas.

2.2.1 Operaciones reversibles sobre bits

Los computadores cuánticos realizan una importante parte de su cálculo mediante operaciones reversibles, las cuales transforman el estado inicial de los qubits en su forma final utilizando solo procesos cuya acción puede ser invertida. Existe solamente un componente irreversible en la operación de un computador cuántico, llamado medición, el cual es la única manera de extraer información útil de los qubits luego de que su estado ha adquirido su forma final. A pesar de que la medición es una parte no trivial y crucial de

cualquier computador cuántico, en un computador clásico la extracción de información de estado de bits es tan conceptualmente directa que no se considera como una parte inherente al proceso computacional aun cuando es una preocupación no trivial para quienes diseñan presentaciones digitales o impresoras.

En una operación reversible cada estado final surge de un único estado inicial. Un ejemplo de una operación irreversible es BORRAR, la cual fuerza al bit al estado $|0\rangle$ sin importar si su estado inicial es $|0\rangle$ o $|1\rangle$. BORRAR es irreversible en el sentido de que, dado únicamente el estado final y el hecho de que fue resultado de la operación BORRAR, no hay manera de recuperar el estado inicial.

La única operación reversible no trivial que se puede aplicar a un solo bit es la operación NOT, denotada por el símbolo X, el cual intercambia los dos estados $|0\rangle$ y $|1\rangle$:

$$X : |x\rangle \to |\tilde{x}\rangle; \qquad \tilde{1} = 0, \qquad \tilde{0} = 1$$

NOT es reversible porque tiene una inversa; aplicar X una segunda vez restaura el estado del bit a su forma original:

$$X^2 = 1$$

Donde 1 es el operador unitario (identidad). Si se representan los dos estados de un bit por sus vectores columna, entonces se puede expresar NOT con el operador lineal X sobre el espacio vectorial bidimensional, cuya acción sobre los vectores columna es daba por la matriz:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

De manera que las dos acciones reversibles que se pueden efectuar sobre un solo bit – dejarlo tal como está o voltearlo – corresponden a los dos operadores lineales X y 1,

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

Sobre su espacio vectorial bidimensional. Dado que la multiplicación por el escalar 1 y la acción por el operador unitario 1 alcanza el mismo resultado, es una práctica común entre los físicos no distinguir notacionalmente entre ellos. Las mismas libertades se toman con el escalar 0, el vector cero 0 y el operador cero 0.

Las posibilidades para operaciones reversibles se enriquecen al pasar de un solo bit a un par de bits. La operación reversible más general sobre dos bits es cualquier permutación

de sus cuatro posibles estados. Existen 4!=24 de tales operaciones. Tal vez el ejemplo no trivial más simple es el operador de intercambio **S**$_{ij}$, el cual simplemente intercambia el estado de los bits *i* y *j*:

$$S_{10}|xy\rangle = |yx\rangle$$

Dado que el operador S_{10} intercambia $|01\rangle = |1\rangle_2$ y $|10\rangle = |2\rangle_2$, mientras $|00\rangle = |0\rangle_2$ y $|11\rangle = |3\rangle_2$ se mantienen, su matriz en la base $|0\rangle_2$, $|1\rangle_2$, $|2\rangle_2$, $|3\rangle_2$ es:

$$S_{10} = S_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

El operador de 2 bits cuya extensión a qubits juega el papel más importante en la computación cuántica es el NOT controlado u operador cNOT **C**$_{ij}$. Si el estado del i-ésimo bit (bit de control) es $|0\rangle$, **C**$_{ij}$ deja el estado del j-ésimo bit (el bit objetivo) sin cambios, pero, si el estado del bit de control es $|1\rangle$, **C**$_{ij}$ aplica el operador NOT al estado del bit objetivo. En cualquier caso, el estado del bit de control se mantiene inalterado.

Se puede resumir la operación de la siguiente manera:

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle, \qquad C_{01}|x\rangle|y\rangle = |x \oplus y\rangle|y\rangle,$$

Donde $\oplus$ denota la adición módulo 2:

$$y \oplus 0 = y, \qquad y \oplus 1 = \tilde{y} = 1 - y$$

La suma módulo 2 $x \oplus y$ es también llamada "O exclusivo" o XOR de *x* y *y*.

Es posible construir la operación de intercambio a partir de tres operaciones cNOT:

$$S_{ij} = C_{ij} C_{ji} C_{ij}$$

Para construir la matriz de la operación cNOT en el espacio 4-dimensional de dos bits, se observa que si el bit de control está a la izquierda entonces cNOT deja $|00\rangle = |0\rangle_2$ y $|01\rangle = |1\rangle_2$ sin cambios e intercambia $|10\rangle = |2\rangle_2$ y $|11\rangle = |3\rangle_2$. De manera que la matriz 4x4 representando **C**$_{10}$ es:

$$C_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Si el bit de control está a la derecha, entonces los estados $|01\rangle = |1\rangle_2$ y $|11\rangle = |3\rangle_2$ son intercambiados y, los estados $|00\rangle = |0\rangle_2$ y $|10\rangle = |2\rangle_2$ se mantienen. De manera que la matriz que representa $\mathbf{C}_{01}$ es:

$$C_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Para asuntos prácticos es casi siempre más eficiente establecer la identidad del operador, tratándolos directamente como operadores y evitar la representación matricial.

Un tipo muy común de operador de dos bits consiste en el producto tensor de dos operadores de un bit:

$$(a \otimes b)|xy\rangle = (a \otimes b)|x\rangle \otimes |y\rangle = a|x\rangle \otimes b|y\rangle$$

De lo cual se deduce que:

$$(a \otimes b)(c \otimes d) = (ac) \otimes (bd)$$

Esta notación del producto tensor para operadores puede ser muy útil cuando se trabaja con una gran cantidad de bits y se desea escribir un operador de dos bits que afecte solo un cierto par de bits. Si, por ejemplo, un operador de dos bits actúa solo sobre el segundo y cuarto bits desde la derecha en un estado de 6 bits, entonces el operador sobre el estado de 6 bits debe ser escrito como:

$$1 \otimes 1 \otimes a \otimes 1 \otimes b \otimes 1$$

Y para evitar tales monstruosidades tipográficas, se simplifica a:

$$1 \otimes 1 \otimes a \otimes 1 \otimes b \otimes 1 = a_3 b_1 = b_1 a_3$$

En donde el subíndice indica sobre cual bit actúa el operador de un bit, y se entiende que aquellos estados cuyos subíndices no aparecen se mantienen sin modificación – es decir, sobre ellos actúa el operador unitario. Como se puede apreciar, cada estado de un bit se nombra por la potencia de dos que tendría si los n bits representaran un entero: el estado en el extremo derecho se nombra 0, el que está a su izquierda 1, etc. Dado que el orden en el cual **a** y **b** se escriben es claramente irrelevante si sus subíndices especifican diferentes estados de un bit, el orden no importa: operadores de un bit que actúan sobre diferentes estados de un bit son conmutativos.

Algunas veces se trabaja con operadores de un bit que ya tienen subíndices en sus nombres, bajo tales condiciones es más conveniente especificar sobre cual estado del bit

actúa el operador con un superíndice encerrado en paréntesis para evitar la confusión con exponentes: de manera que $X^{(2)}$ representa el operador de un bit que intercambia el tercer estado de un bit desde la derecha, pero X^2 represente el cuadrado del operador de intercambio sin referencia al estado del bit sobre el cual actúa.

2.2.2 Manipular operaciones

Es útil introducir el operador de un bit **n** que es simplemente el operador proyección sobre el estado $|1\rangle$:

$$n|x\rangle = x|x\rangle, \qquad x=0 \text{ o } 1$$

Dado que $|0\rangle$ y $|1\rangle$ son vectores propios de **n** con valores propios 0 y 1, **n** es llamado el operador numérico de 1 bit. También se define el operador complementario:

$$\tilde{n} = 1 - n$$

El cual proyecta sobre el estado $|0\rangle$, de manera que $|0\rangle$ y $|1\rangle$ son vectores propios de $\tilde{n}$ con valores propios 1 y 0. Estos operadores tienen las representaciones matriciales:

$$n = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \tilde{n} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Se deduce directamente de sus definiciones que

$$n^2 = n, \qquad \tilde{n}^2 = \tilde{n}, \qquad n\tilde{n} = \tilde{n}n = 0, \qquad n + \tilde{n} = 1$$

También se tiene que

$$nX = X\tilde{n}, \qquad \tilde{n}X = Xn$$

A pesar de que **n** no tiene interpretación como una operación física sobre bits – reemplazar el estado de un bit con el vector cero no corresponde a una operación física – puede ser útil para derivar relaciones entre operaciones que no tienen significado físico. Dado, por ejemplo, que el operador de intercambio $\mathbf{S}_{ij}$ actúa como la identidad si los estados de los bits i y j son iguales, e intercambia los números representados por ambos bits si sus estados son diferentes, puede ser escrito como:

$$S_{ij} = n_i n_j + \tilde{n}_i \tilde{n}_j + (X_i X_j)(n_i \tilde{n}_j + \tilde{n}_i n_j)$$

De la misma forma $\mathbf{C}_{ij}$ puede ser expresado en términos de **n**s y **X**s por:

$$C_{ij} = \tilde{n}_i + X_j n_i$$

Un operador que no tiene un rol tan importante en computación clásica, pero que es tan importante como el operador NOT en computación cuántica es el operador Z, definido por:

$$Z = \tilde{n} - n = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Se deduce de las representaciones matriciales de X y Z (o de las relaciones previas entre *X*, *n* y *ñ*) que **X** es anti conmutativo con **Z**:

$$ZX = -XZ$$

Dado que $n + \tilde{n} = 1$, es posible definir los operadores proyección de un bit **ñ** y **n** en términos de **1** y **Z**:

$$n = \frac{1}{2}(1 - Z), \qquad \tilde{n} = \frac{1}{2}(1 + Z)$$

Utilizando estas equivalencias, es posible escribir el operador cNOT en términos de los operadores **X** y **Z**:

$$\begin{aligned} C_{ij} &= \frac{1}{2}(1 + Z_i) + \frac{1}{2} X_j (1 - Z_i) \\ &= \frac{1}{2}(1 + X_j) + \frac{1}{2} Z_i (1 - X_j) \end{aligned}$$

La segunda forma se deriva de la primera porque $\mathbf{X}_j$ y $\mathbf{Z}_i$ son conmutativos cuando $i \neq j$. Se puede notar que si se intercambian Z y X en la segunda línea del operador anterior, se obtendría la expresión directamente arriba de ella excepto por el intercambio de *i* y *j*. De manera que intercambiar los operadores **X** y **Z** tiene el efecto de cambiar cual es el bit de control y cual el bit objetivo, convirtiendo $\mathbf{C}_{ij}$ en $\mathbf{C}_{ji}$. Un operador que produce exactamente el mismo efecto es la *transformación Hadamard* (también conocido como *transformación Walsh-Hadamard*),

$$H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Este es otro operador de fundamental importancia en computación cuántica.

Dado que $\mathbf{X}^2 = \mathbf{Z}^2 = \mathbf{1}$ y que **XZ** = **– ZX**, es fácilmente demostrable de la definición anterior de **H** en términos de **X** y **Z** que:

$$\mathbf{H}^2 = \mathbf{1}$$

Y que:

$$\mathbf{HXH} = \mathbf{Z}, \qquad \mathbf{HZH} = \mathbf{X}$$

Lo cual muestra como **H** puede ser utilizado para intercambiar los operadores **X** y **Z** en $\mathbf{C}_{ji}$ de manera que se obtiene:

$$C_{ji} = (H_i H_j) C_{ij} (H_i H_j)$$

Esta simple relación puede ser llevada a usos muy notables en un computador cuántico. Aun cuando se puede lograr este intercambio en un computador clásico utilizando el operador de intercambio, $C_{ji} = S_{ij} C_{ij} S_{ij}$, la diferencia crucial entre $\mathbf{S}_{ij}$ y $\mathbf{H}_i\mathbf{H}_j$ radica en que el último es producto de dos operadores de un bit, mientras que el primero no lo es.

Por supuesto, la acción de **H** sobre el estado de un bit que se deduce de

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

Describe una transformación sin ningún significado sobre bits. No obstante cuando se combinan con otras operaciones, las operaciones Hadamard dan como resultado una operación completamente sensata tal como $\mathbf{C}_{ji}$. En un computador cuántico, la acción de H sobre el estado de un qubit resulta ser no solo muy significativa sino también fácil de implementar, y la posibilidad de intercambiar los qubits de control y objetivo utilizando solamente operadores de un qubit resulta tener consecuencias determinantes.

El uso de Hadamards para intercambiar los qubits de control y objetivo en una operación cNOT es suficientemente importante en computación cuántica para ameritar una segunda derivación, la cual ilustra más ampliamente la manera en la cual se utiliza el formalismo de operadores. En estricta analogía a la definición de cNOT se puede definir una operación controlada Z, C_{ij}^{Z}, la cual deja el estado del bit objetivo *j* sin cambios si el estado del bit de control *i* es $|0\rangle$ y opera sobre el bit objetivo con **Z** si el estado del bit de control es $|1\rangle$. Como resultado, $C_{10}^{Z}|xy\rangle$ actúa como la identidad sobre $|xy\rangle$ al menos que tanto x como y sean 1, en cuyo casi simplemente transforma $|11\rangle$ en $-|11\rangle$. Este comportamiento es completamente simétrico en los dos bits, así:

$$C_{ij}^{Z} = C_{ji}^{Z}$$

Es una consecuencia directa que intercalar el bit objetivo de un operador cNOT entre Hadamards lo convierte en un $\mathbf{C}^{z}$:

$$H_j C_{ij} H_j = C_{ij}^{Z}, \qquad H_i C_{ji} H_i = C_{ji}^{Z}$$

A la vista de las dos equivalencias anteriores se obtiene:

$$H_j C_{ij} H_j = H_i C_{ji} H_i$$

Lo cual es equivalente a $C_{ji} = (H_i H_j) C_{ij} (H_i H_j)$ dado que $\mathbf{H}^2=\mathbf{1}$

Un ejercicio final en el tratamiento de operaciones sobre bits como operaciones lineales sobre vectores consiste en construir una forma alternativa para el operador de intercambio. Si se expresan **n** y **ñ** en términos de **Z** en el operador de $\mathbf{S}_{ij}$, se encuentra que:

$$S_{ij} = \frac{1}{2}(1 + Z_i Z_j) + \frac{1}{2}(X_i X_j)(1 - Z_i Z_j)$$

Si se define:

$$Y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad i = \sqrt{-1},$$

Se obtiene la forma más compacta:

$$S_{ij} = \frac{1}{2}(1 + X_i X_j + Y_i Y_j + Z_i Z_j)$$

Durante tres cuartos de siglo los físicos han disfrutado agrupar las representaciones matriciales de los tres operadores **X**, **Y** y **Z** en un tri-vector $\vec{\sigma}$ cuyos componentes son matrices de 2x2:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Con lo cual el operador de intercambio se convierte en:[33]

$$S_{ij} = \frac{1}{2}\left(1 + \vec{\sigma}^{(i)} \cdot \vec{\sigma}^{(j)}\right),$$

Donde "." representa el producto escalar de tres dimensiones ordinario:

$$\vec{\sigma}^{(i)} \cdot \vec{\sigma}^{(j)} = \sigma_x^{(i)} \sigma_x^{(j)} + \sigma_y^{(i)} \sigma_y^{(j)} + \sigma_z^{(i)} \sigma_z^{(j)}$$

Los tres componentes de $\vec{\sigma}$ tienen muchas propiedades que se mantienen invariables bajo permutaciones cíclicas de *x*, *y* y *z*. Las tres son Hermitianas[34]. Todas elevadas al cuadrado resultan en la unidad,

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = 1$$

[33] Los físicos disfrutan de la simplicidad de esta derivación "computacional" de la forma del operador de intercambio, comparada con la tradicional derivación cuántico-mecánica, la cual recurre a todo el aparato de la teoría del momento angular.

[34] Los elementos de una matriz Hemitiana A satisfacen la condición de que $A_{ji} = A_{ij}^*$, donde * denota conjugación compleja.

Todas son anti-conmutativas en pares y el producto de dos de ellas está simplemente relacionado a la tercera:

$$\sigma_x\sigma_y = -\sigma_y\sigma_x = i\sigma_z,$$
$$\sigma_y\sigma_z = -\sigma_z\sigma_y = i\sigma_x,$$
$$\sigma_z\sigma_x = -\sigma_x\sigma_z = i\sigma_y$$

Las tres relaciones anteriores difieren solamente por las permutaciones cíclicas de *x*, *y* y *z*.

Las dos relaciones anteriores pueden ser resumidas en una sola identidad. Sean $\vec{a}$ y $\vec{b}$ dos tri-vectores con componentes a_x, a_y, a_z y b_x, b_y, b_z que son números reales ordinarios (también pueden ser números complejos, pero para la mayoría de aplicaciones útiles son reales). Entonces se puede fácilmente confirmar que las dos relaciones anteriores implican y son implicadas por la sola identidad:

$$\left(\vec{a}\cdot\vec{\sigma}\right)\left(\vec{b}\cdot\vec{\sigma}\right) = \left(\vec{a}\cdot\vec{b}\right)1 + i\left(\vec{a}\times\vec{b}\right)\cdot\vec{\sigma}$$

Donde $\vec{a}\times\vec{b}$ denota el producto vectorial (o producto cruz) de $\vec{a}$ y $\vec{b}$:

$$\left(\vec{a}\times\vec{b}\right)_x = a_y b_z - a_z b_y,$$
$$\left(\vec{a}\times\vec{b}\right)_y = a_z b_x - a_x b_z,$$
$$\left(\vec{a}\times\vec{b}\right)_z = a_x b_y - a_y b_x$$

Junto con la matriz unitaria 1, las matrices σ_x, σ_y y σ_z forman la base para el álgebra 4-dimensional de matrices de número complejos bidimensionales: cualquiera de tales matrices es una combinación lineal única de estas cuatro con coeficientes complejos. Dado que las cuatro son Hermitianas, cualquier matriz Hermitiana bidimensional A de números complejos debe ser una combinación lineal de las cuatro y por tanto de la forma:

$$A = a_0 1 + \vec{a}\cdot\vec{\sigma}$$

Donde a_0 y los componente del tri-vector $\vec{a}$ son todos números reales.

Las matrices σ_x, σ_y y σ_z fueron introducidas en los primeros días de la mecánica cuántica por Wolfgang Pauli, para describir el momento angular asociado con el spin de un electrón. Tienen muchos otros propósitos útiles, estando simplemente relacionadas a los cuaterniones inventados por Hamilton para tratar eficientemente la composición de las

rotaciones tridimensionales. Se hace uso intensivo de los operadores de 1 qubit de Pauli en el tema de la corrección de errores cuánticos.

2.2.3 Qubits y sus estados

El estado de un bit es un espécimen poco representativo de un vector bidimensional. Los únicos vectores con un significado clásico en todo el espacio vectorial bidimensional son los vectores orto normales $|0\rangle$ y $|1\rangle$, dado que son los únicos dos estados que un bit puede tener. Afortunadamente, la naturaleza cuenta con sistemas físicos, qubits, que se describen con estados que no sufren de esta limitación. El estado $|\psi\rangle$ asociado con un qubit puede ser cualquier vector unitario en el espacio de vectores bidimensional creado por $|0\rangle$ y $|1\rangle$ sobre los números complejos. El estado general de un qubit es:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

Donde α_0 y α_1 son dos números complejos limitados solo por el requerimiento de que $|\psi\rangle$, tal como $|0\rangle$ y $|1\rangle$, debe ser un vector unitario en el espacio de vectores complejos – es decir, por la condición de normalización:

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

El estado $|\psi\rangle$ se dice que está en una *superposición* de los estados $|0\rangle$ y $|1\rangle$ con amplitudes α_0 y α_1. Si α_0 o α_1 es 0, entonces el otro es 1 – por ejemplo el caso especial en el cual el estado del qubit es uno de los dos estados clásicos $|0\rangle$ o $|1\rangle$ - puede ser conveniente mantener el lenguaje apropiado para bits, refiriéndose a que el qubit "tiene el valor de" 0 o 1. Es más correcto sin embargo decir que el estado del qubit es $|0\rangle$ o $|1\rangle$. Para qubits, en contraste con bits, no se puede decir que "tienen valores". Tienen – o más correctamente, están descritos por, o, mejor aún, están asociados con – estados.

Así como el estado de un solo qubit es una superposición normalizada de los dos posibles estados clásicos, el estado general $|\Psi\rangle$ que la naturaleza permite asociar con dos qubits es una superposición normalizada de los cuatro estados clásicos ortogonales:

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

Con las amplitudes complejas siendo limitadas solamente por la condición de normalización:

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Lo cual generaliza el obvio camino para n qubits, cuyo estado general puede estar en cualquier superposición de 2^n estados clásicos diferentes, con amplitudes cuyas magnitudes al cuadrado suman la unidad:

$$|\Psi\rangle = \sum_{0 \le x < 2^n} \alpha_x |x\rangle_n , \qquad \sum_{0 \le x < 2^n} |\alpha_x|^2 = 1$$

En el contexto de la computación cuántica, el conjunto de 2^n estados clásicos – todos los posibles productos tensores de los estados $|0\rangle$ y $|1\rangle$ de *n* bits individuales – es llamado la *base computacional*. Para la mayoría de propósitos *base clásica* es un término más apropiado. Los estados que caracterizan *n* bits – los estados de la base clásica – son un subconjunto extremadamente limitado de los estados de *n* qubits, los cuales pueden estar en cualquier superposición (normalizada) con coeficientes complejos de estos estados de la base clásica.

Si se tienen dos bits, uno en el estado $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ y el otro en el estado $|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, entonces el estado $|\Psi\rangle$ del par, en una generalización de la regla para estados de múltiples bits, se toma como el producto tensor de los estados individuales:

$$\begin{aligned} |\Psi\rangle = |\psi\rangle \otimes |\phi\rangle &= \left(\alpha_0|0\rangle + \alpha_1|1\rangle\right) \otimes \left(\beta_0|0\rangle + \beta_1|1\rangle\right) \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle \\ &= \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} \end{aligned}$$

Se puede notar que el estado general de dos qubits, es de la forma anterior, si y solo si $\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}$. Dado que las cuatro amplitudes se limitan solo por la condición de normalización, y la condición $\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}$ no siempre se mantiene; el estado general de

dos qubits, a diferencia del estado general de dos bits, no es un producto de los estados de dos qubits. Lo mismo se aplica para el estado de *n* qubits. A diferencia de los bits, cuyo estado general solo puede ser uno de los 2^n productos de $|0\rangle$ y $|1\rangle$, un estado general de *n* qubits es una superposición de estos 2^n estados producto y no puede, en general, ser expresado como un producto de un conjunto de estados de un qubit. Qubits individuales, formando parte de un sistema de múltiples qubits, en contraste a bits individuales, no pueden ser siempre caracterizados como poseedores de estados propios.[35]

Tales estados que no provienen de un producto de dos o más qubits son llamados estados *entrelazados*. El término es una traducción del verschränkt de Schrödinger, el cual es traducido más precisamente como "entrelazado" o "envuelto". Sin embargo el mismo Schrödinger utilizó el término "entrelazado" como palabra inglesa. Cuando el estado de varios qubits es entrelazado, pueden comportarse de forma muy extraña.

2.3.4 Operaciones reversibles sobre qubits

La única operación reversible no trivial que un computador clásico puede realizar sobre un solo bit es la operación NOT. La naturaleza ha sido mucho más versátil en la forma en la que permite trabajar con qubits. Las operaciones reversibles que un computador cuántico permite realizar sobre un qubit se representan por la acción sobre el estado del qubit de cualquier transformación *lineal* que convierte vectores unitarios en vectores unitarios. Tales transformaciones **u** son llamadas *unitarias* y satisfacen la condición:

$$\mathbf{u}\mathbf{u}^t = \mathbf{u}^t\mathbf{u} = \mathbf{1}$$

Dado que cualquier transformación unitaria tiene una inversa unitaria, tales acciones de un computador cuántico sobre un qubit son reversibles. La reversibilidad es vital para el funcionamiento correcto de un computador cuántico. Se puede generalizar la transformación unitaria **u** para *n* qubits como una transformación unitaria 2^n-dimensional **U**, que satisface:

$$\mathbf{U}\mathbf{U}^t = \mathbf{U}^t\mathbf{U} = \mathbf{1}$$

Muchas operaciones unitarias importantes sobre qubits se definen como permutaciones de los estados de la base clásica. El efecto de la operación sobre tales estados

[35] Precisamente, no siempre tienen lo que se llaman *estados puros* de sí mismos. Es a menudo conveniente dar una descripción estadística de un qubit individual (o un grupo de qubits) en términos de lo que se llama una *matriz de densidad* o *estado mixto*.

$\sum \alpha_x |x\rangle_n$ es permutar las amplitudes α_x. Tal permutación preserva el valor de $\sum |\alpha_x|^2$, de manera que U transforma vectores unitarios en vectores unitarios. Preservando la norma y siendo lineal, **U** es en realidad unitario.

Cualquier operación reversible sobre *n* bits puede ser asociada con una operación unitaria **U** sobre n qubits. Dado que la base clásica es una base, **U** puede ser extendida arbitrariamente a estados de *n* qubits siempre y cuando sea lineal. En particular las transformaciones **X**, **S** y **C** sobre bits son inmediatamente definidas de esta forma para qubits. Las transformaciones unitarias para qubits son mucho más generales que simples extensiones de operaciones clásicas, tal es el caso del operador **Z** y las transformaciones Hadamard **H**.

Al diseñar algoritmos cuánticos, la clase de transformaciones unitarias permitidas es casi siempre del tipo que puede ser construida enteramente del producto de transformaciones unitarias que actúan solo sobre un qubit a la vez, llamadas *puertas de 1 qubit*, o que actúan en solo un par de qubits, llamadas *puertas de 2 qubits*. Esta restricción es impuesta por que los problemas técnicos de construir puertas cuánticas de mayor orden son todavía más formidables que los (de por sí) difíciles problemas de construir puertas cuánticas confiables de 1 y 2 qubits.

Resulta ser que esta no es una limitación fundamental, dado que transformaciones unitarias arbitrarias pueden ser aproximadas hasta un grado de precisión arbitrario por una cantidad suficientes de puertas de 1 y 2 qubits. Para un computador clásico reversible, se puede mostrar que al menos una puerta de 3 bits se necesita para construir operaciones lógicas generales. Pero, en un computador cuántico, se encuentra notablemente – e importante para la factibilidad de la computación cuántica práctica – que la extensión cuántica de una puerta de 3 bits puede ser construida a partir de un pequeño número de puertas de 1 y 2 qubits.

2.3 Diagramas de circuitos

Es la costumbre en la ciencia de la computación cuántica representar la acción de una secuencia de puertas actuando sobre *n* qubits mediante un diagrama de circuitos. El estado inicial del qubits aparece a la izquierda, el estado final a la derecha y las puertas en la parte central de la figura.

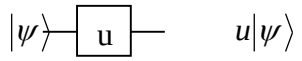


Figura 1.1 Un diagrama de circuito representando la acción sobre un solo qubit de una puerta **u**. Inicialmente el qubit se describe por el estado de entrada $|\psi\rangle$ a la izquierda. La línea delgada (alambre) representa la historia subsecuente del qubit. Luego de emerger de la caja representando a **u**, el qubit se describe a la derecha por el estado final $u|\psi\rangle$.

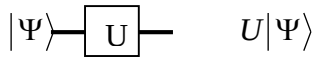
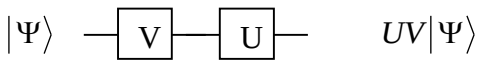


Figura 1.2 Un diagrama de circuito representando la acción sobre un *n* qubits de una puerta **U**. Inicialmente los qubits son descritos por el estado de entrada $|\Psi\rangle$ a la izquierda. La línea gruesa (barra) representa la historia subsecuente de los qubits. Luego de emerger de la caja representando a **U**, los qubits son descritos a la derecha por el estado final $U|\Psi\rangle$.

La siguiente figura revela una característica particular de los diagramas de circuitos de la cual es importante estar al tanto. Los diagramas se leen de izquierda a derecha. La parte (a) representa un circuito que actúa primero con **V** y luego con **U** sobre el estado inicial $|\Psi\rangle$. El resultado es el estado $UV|\Psi\rangle$, porque es la convención, al escribir ecuaciones para operadores lineales sobre espacios vectoriales, que la operación aparezca a la izquierda del estado sobre el cual actúa. Por tanto la secuencia de símbolos $|\Psi\rangle$, **V** y **U** a la izquierda del diagrama de circuitos en (a) es invertida de la secuencia en la cual aparecen en la representación matemática del estado que es producido a la derecha. La parte (b) muestra las consecuencias de ello para la parte del circuito que contienen solamente las puertas: un diagrama en el cual la puerta **V** (a la izquierda) es seguida por la puerta **U** a la derecha describe la transformación unitaria **UV**.



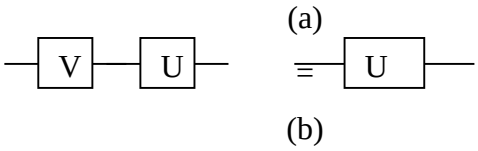


Figura 1.3 Múltiples puertas actúan sobre un estado. El orden de las puertas en el diagrama de circuitos se invierta al pasar a la representación como ecuaciones.

Mientras que algunos de los diagramas más importantes son simétricos, muchos otros no lo son, y se debe tomar en cuenta el traducir las puertas en sentido inverso al pasar de ecuaciones a diagramas de circuitos y viceversa.

Existe poca utilidad para diagramas de circuitos de las formas anteriores, debido a su simplicidad, pero son importantes como los bloques de construcción a partir de los cuales mayores diagramas son concebidos. A medida que el número de operaciones aumenta, el diagrama permite evaluar de una sola vez la acción de una secuencia de puertas unitarias de 1 y 2 qubits sobre una colección de varios qubits en una forma más transparente y fácil de recordar que la correspondiente formulación. En realidad, muchos cálculos que involucran ecuaciones realmente largas pueden ser simplemente llevados a cabo manipulando diagramas de circuitos.

2.4 Puertas de medición

Para dar el estado de un bit solo se necesita una pieza de información: el estado es $|0\rangle$ o $|1\rangle$. Pero para especificar el estado de un solo qubit con suficiente precisión, se necesitan muchas piezas de información, dado que se deben especificar dos números complejos sujetos a la limitante de normalización. Dado que los qubits no solo tienen un conjunto más rico de estados que los bis, sino que pueden estar sujetos a la acción de un correspondiente conjunto más rico de transformaciones, es obvio que un computador cuántico es mucho más poderoso que un computador clásico. Así también existe un gran problema.

El problema radica en que: si se tienen n bits, cada uno representando un 0 o un 1, se puede averiguar el estado de cada uno solamente con revisarlos. No hay nada problemático en conocer el estado de un bit, y por tanto conocer el resultado de cualquier cálculo construido a partir de operaciones sobre esos bits. Incluso – es tomado por sentado en cualquier discusión de computación clásica - el estado de los bits no se altera por el proceso de leerlos. La acción de obtener información de bits no es perturbadora. Se pueden leer los bits en cualquier etapa del proceso computacional sin alterar las etapas posteriores.

En completo contraste, si se tienen *n* qubits en una superposición de estados de base computacional no hay nada que se pueda hacer para extraer de esos qubits la gran cantidad de información contenida en las amplitudes α_x. No se puede leer los valores de esas amplitudes y por tanto no se puede averiguar cuál es el estado. El estado de *n* qubits no está asociado con ninguna propiedad verificable de esos qubits.

Solo existe una manera de extraer información de *n* qubits en un estado dado. Eso se denomina *hacer una medición*. El proceso consiste en llevar a cabo una cierta prueba sobre cada qubit, el resultado de la cual es 0 o 1. La colección particular de ceros y unos producida por la prueba no está en general determinada por el estado $|\Psi\rangle$ de los qubits; el estado determina solo la probabilidad de los posibles resultados, de acuerdo con la siguiente regla: la probabilidad de obtener un resultado en particular – por decir 01100, si se tienen 5 qubits – está dada por la magnitud al cuadrado de la amplitud del estado $|01100\rangle$ en la expansión del estado $|\Psi\rangle$ de los qubits sobre los 2^5 estados básicos computacionales. Más generalmente, si el estado de los *n* qubits es:

$$|\Psi\rangle = \sum_{0 \le x < 2^n} \alpha_x |x\rangle_n$$

Entonces la probabilidad de que ceros y unos resultado de la medición de todos los qubits de la expansión binaria del entero x es:

$$p(x) = |\alpha_x|^2$$

Esta regla básica de cómo la información puede ser extraída de un estado cuántico fue en principio formulada por Max Born, y se conoce como la *regla de Born*. Provee la conexión entre amplitudes y los números que se pueden leer cuando se pone a prueba – mide – los qubits. Las magnitudes al cuadrado de las amplitudes dan las probabilidades de los resultados de las mediciones. La condición de normalización es solo el requerimiento de que las probabilidades para todos los 2^n resultados mutuamente exclusivos sumen 1.

El proceso de medición se lleva a cabo por un dispositivo de hardware con una pantalla digital, conocido como una *puerta de medición de n qubits*. Tal puerta es representada esquemáticamente en la siguiente figura. En contraste a las puertas unitarias, las cuales tienen una única salida para cada entrada, el estado de los qubits que emerge de una puerta de medición está solo estadísticamente determinado por el estado de las qubits de entrada. Para contrastar más con las puertas unitarias, la acción de una puerta de medición no puede ser deshecha: dado el estado final $|x\rangle$, no hay manera de reconstruir el estado inicial $|\Psi\rangle$. La medición es irreversible. Tampoco es la acción de una puerta de medición en algún sentido lineal.

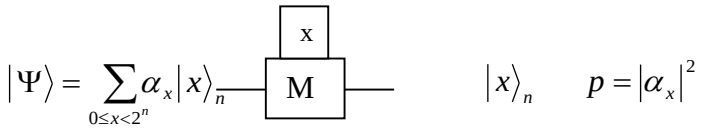


Figura 1.4 Diagrama de circuitos representando la puerta de medición de n qubits.

En la manera en la que sugiere que alguna propiedad preexistente está siendo revelada, "medición" es un término peligrosamente incorrecto. Se debe evitar este engaño, pues en mecánica cuántica "medición" no es igual a medir el peso de alguien, por ejemplo, sino más bien medir su IQ, lo cual no revela una propiedad numérica preexistente, sino solo lo que pasa cuando alguien se somete a una prueba de IQ. Para la computación cuántica la "medición" significa solamente aplicar y leer la pantalla de una puerta apropiada, cuya acción está totalmente gobernada por la regla de Born.

El más simple enunciado de la regla de Born es para un solo qubit. Si el estado del qubit es la superposición de los estados $|0\rangle$ y $|1\rangle$ con amplitudes α_0 y α_1 entonces el resultado de la medición es 0 con probabilidad $|\alpha_0|^2$ o 1 con probabilidad $|\alpha_1|^2$. Como se especificó anteriormente, puertas de medición de *n* qubits pueden ser construidas aplicando puertas de medición de 1 qubit a cada uno de los *n* qubits. El proceso de medición puede por tanto ser reducido a aplicar múltiples copias de *una sola pieza de hardware elemental: la puerta de medición de 1 qubit*.

Junto con mostrar un entero de *n* bits con probabilidades determinadas por las amplitudes, existe un segundo aspecto muy importante acerca de la acción de puertas de medición: si *n* qubits, inicialmente descritos por el estado $|\Psi\rangle$, se envían a través de una puerta de medición de *n* qubits, y la pantalla de la puerta de medición indica el entero x, entonces se debe asociar con los qubits que emergen de la puerta de medición el estado de la base clásica $|x\rangle_n$. Lo cual significa que todo indicio de las amplitudes α_x caracterizando el estado de entrada se ha perdido en el estado de salida.

Este cambio de estado obtenido luego de una medición es a menudo *reducción* o *colapso* del estado. Se dice que el estado pre-medición se *reduce* o *colapsa* al estado post-medición, como consecuencia de la medición. Es importante recordar, en este contexto, que el estado de *n* qubits no es más que una representación abstracta, utilizada, mediante la regla de Born, para calcular las probabilidades del resultado de la medición. No existe una propiedad interna de los qubits que corresponda a sus estados.

Como es posible aprender algo de interés computacional bajo estas condiciones. El arte de la computación cuántica consiste en producir, a través de transformaciones unitarias astutamente construidas, una superposición en la cual la mayoría de las amplitudes α_x son cero o extremadamente cercanas a cero, con la información útil contenida en cualquiera de los calores de *x* que tienen una probabilidad apreciable de ser indicados por la medición. Es importante buscar información que, una vez poseída, pueda ser fácilmente confirmada, tal vez con un computador ordinario (clásico) (por ejemplo los factores de un número), de manera que resultados de baja probabilidad no resulten relevantes.

La regla de Born no implica que antes de la prueba el qubit ya llevaba el valor revelado por la prueba y estaba descrito por el correspondiente estado de la base clásica, dado que, entre otras posibilidades, la acción de la prueba en si podría jugar un rol en sacar

a la luz el resultado. Esto se puede ver con la ayuda de la transformación Hadamard; suponiendo que se aplica **H** a un qubit que esta inicialmente en el estado:

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

Se deduce que el resultado es:

$$\begin{aligned} H|\phi\rangle &= \frac{1}{\sqrt{2}} H\left(|0\rangle + |1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(H|0\rangle + H|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) + \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right) \\ &= \frac{1}{\sqrt{2}}\left(\frac{2}{\sqrt{2}}|0\rangle\right) \\ &= |0\rangle \end{aligned}$$

De manera que de acuerdo a la regla de Born, si se mide el qubit descrito por el estado $H|\phi\rangle$, el resultado será 0 con una probabilidad de 1.

Pero suponiendo que el qubit en el estado $|\phi\rangle$ estuviese en realidad en el estado $|0\rangle$ con probabilidad ½ y en el estado $|1\rangle$ con probabilidad ½. En cualquier caso, de acuerdo a la subsecuente acción de **H** se produciría un estado – $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ o $\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ – que bajo medición resultaría en 0 o 1 con igual probabilidad. Lo cual contradice la demostración anterior y es incorrecto. Es por ello que un qubit en una superposición cuántica no puede ser visto como estando en un estado u otro con ciertas probabilidades, sino que es una forma natural e irreductible como lo son los estados $|0\rangle$ y $|1\rangle$ individualmente.

Si los estados de *n* qubits se restringen a los estados de la base computacional entonces el proceso de medición es exactamente igual al proceso clásico de "mirar el valor de x" sin alterar el estado. Y por tanto un computador cuántico puede ser llevado a simular un computador clásico reversible permitiendo solo estados de la base computacional como entrada, y utilizando solo puertas unitarias que transforman estados de base computacional en otros estados de base computacional.

La regla de Born, relacionando las amplitudes α_x en la expansión $|\Psi\rangle = \sum_{0 \le x < 2^n} \alpha_x |x\rangle_n$ de un estado general de *n* qubits $|\Psi\rangle$ a las probabilidades de medición de *x*, es a menudo

expresa en términos de productos escalares u operadores de proyección. La probabilidad de una medición dando el resultado de x ($0 \le x < 2^n$) es:

$$p_\Psi(x) = |\alpha_x|^2 = |\langle x|\Psi\rangle|^2$$

También puede ser útil expresada en términos de operadores de proyección:

$$p_\Psi(x) = \langle x|\Psi\rangle\langle\Psi|x\rangle = \langle x|P_\Psi|x\rangle$$

O

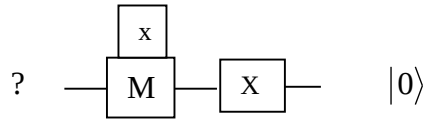
$$p_\Psi(x) = \langle\Psi|x\rangle\langle x|\Psi\rangle = \langle\Psi|P_x|\Psi\rangle$$

Donde $P_\Psi = |\Psi\rangle\langle\Psi|$ es el operador proyección sobre el estado $|\Psi\rangle$, y $P_x = |x\rangle\langle x|$ es el operador proyección sobre el estado $|x\rangle$.

2.5 Preparación de estados

Además de proveer un resultado al final del proceso computacional, las puertas de medición también juegan un rol crucial (no a menudo enfatizado) al inicio. Dado que no hay forma de determinar el estado de una colección dada de qubits; ¿cómo producir un conjunto de qubits en un estado definido para ser transformado por las puertas de un computador cuántico hasta otro estado útil computacionalmente?

La respuesta es a través de la medición. Si se toman *n* qubits arbitrariamente, y se los somete a una puerta de medición de *n* qubits que registra *x*, entonces los qubits que emergen de dicha puerta tienen asignado el estado de la base clásica $|x\rangle_n$ Si se aplica la operación de un solo qubit **X** a cada qubit que registre un 1 en la medición, sin tocar los bits que registran 0, el conjunto resultante de qubits será descrito por el estado $|0\rangle_n$. Es este estado el que la mayoría de algoritmos de computación cuántica toman como su entrada. Tal uso de la puerta de medición se muestra en la siguiente figura:



La acción inicial de las puertas de medición es llamada *preparación de estado*, dado que los qubits que emergen de dicho proceso pueden ser caracterizados por un estado definido. Para las realizaciones físicas particulares de qubits, pueden existir otras formas de producir el estado inicial estándar $|0\rangle_n$. Suponiendo, por ejemplo, que cada qubit es un átomo, el estado $|0\rangle$ es el estado de más baja energía (el estado fundamental) del átomo, y el estado $|1\rangle$ es el estado atómico del siguiente nivel de energía (el primer estado excitado). Entonces se puede producir el estado $|0\rangle_n$ enfriando *n* de tales átomos a una temperatura baja apropiada (determinada por la diferencia energética entre los dos estados – mientras menor es la energía, más baja debe ser la temperatura).

Desde el punto de vista conceptual, la preparación de estados con el uso de puertas de medición es el camino más simple. Un candidato físico aceptable para un qubit debe ser un sistema para el cual las puertas de medición estén inmediatamente disponibles. De otra manera no habría forma de extraer la información del proceso computacional, sin importar que tan bien las puertas unitarias realicen su trabajo. Sin importar cuál sea el método físico

para inicializar los qubits, es suficiente saber que siempre puede ser realizado mediante puertas de medición.

2.5.1 Construcción de estados arbitrarios de 1 y 2 qubits

El arte de la computación cuántica es construir circuitos a partir de puertas de 1 y 2 qubits que producen estados finales capaces de revelar información útil, cuando es medida. La expectativa es que puertas de un qubit sean comparativamente fáciles de construir. Puertas de dos qubits que no son simples productos tensores de puertas de un qubit posiblemente sean substancialmente más difíciles de construir. La atención se ha centrado en fuertemente sobre la puerta cNOT, y las puertas que pueden ser construidas a partir de ella en combinación con unitarias de 1 qubit. Dada la dificultad de hacer puertas cNOT, es considerado deseable que mantener su número tan pequeño como sea posible. Como una ilustración de tal construcción, se puede examinar como asignar estados arbitrarios a uno o dos qubits, a partir del estado estándar de un qubit $|0\rangle$ o el estado estándar de dos qubits $|00\rangle$ (ambos pueden ser producidos con la ayuda de puertas de medición).

La situación para estados de un qubit es bastante simple. Sea $|\psi\rangle$ cualquier estado de un qubit, y sea $|\phi\rangle$ el estado ortogonal, que satisfacen $\langle\psi|\phi\rangle = 0$. Dado que $|0\rangle$ y $|1\rangle$ son linealmente independientes; existe una única transformación lineal que los convierte en $|\psi\rangle$ y $|\phi\rangle$. Pero dado que $|\psi\rangle$ y $|\phi\rangle$ son una par orto normal (como lo son $|0\rangle$ y $|1\rangle$), se verifica fácilmente que esta transformación lineal preserva la norma de estados arbitrarios, de manera que es una transformación unitaria **u**. Por tanto para cualquier $|\psi\rangle$ existe una puerta unitaria de un qubit u que convierte $|0\rangle$ en $|\psi\rangle$:

$$|\psi\rangle = u|0\rangle$$

Las cosas son más complicadas para estados de dos qubits. Un estado de dos qubits no entrelazado, siendo el producto de dos estados de un qubit, puede ser construido a partir de $|00\rangle$ mediante la aplicación de unitarias de un qubit a cada uno de los dos qubits. Pero un estado general de dos qubits está entrelazado, y su producción requiere una puerta de dos qubits la cual no es solo el producto tensor de unitarias de un qubit. Interesantemente, una sola puerta cNOT, combinada con unitarias de un qubit, es suficiente para realizar el truco.

Para probar ello, es de notar que el estado general de dos qubits:

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Es de la forma:

$$|\Psi\rangle = |0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\phi\rangle$$

Donde $|\psi\rangle = \alpha_{00}|0\rangle + \alpha_{01}|1\rangle$ y $|\phi\rangle = \alpha_{10}|0\rangle + \alpha_{11}|1\rangle$. Se aplica $u \otimes 1$ a $|\psi\rangle$, donde **u** es una transformación lineal, cuya acción sobre la base computacional es de la forma:

$$u|0\rangle = a|0\rangle + b|1\rangle, \qquad u|1\rangle = -b^*|0\rangle + a^*|1\rangle; \qquad |a|^2 + |b|^2 = 1$$

La transformación **u** es unitaria dado que preserva la ortogonalidad y normalización de la base $|0\rangle$, $|1\rangle$.

Se obtiene:

$$\begin{aligned}(u \otimes 1)|\Psi\rangle &= \big(a|0\rangle + b|1\rangle\big) \otimes |\psi\rangle + \big(-b^*|0\rangle + a^*|1\rangle\big) \otimes |\phi\rangle \\ &= |0\rangle \otimes |\psi'\rangle + |1\rangle \otimes |\phi'\rangle\end{aligned}$$

Donde

$$|\psi'\rangle = a|\psi\rangle - b^*|\phi\rangle \qquad |\phi'\rangle = b|\psi\rangle + a^*|\phi\rangle$$

Si se escogen los números complejos a y b de manera que $|\psi'\rangle$ y $|\phi'\rangle$ sean ortogonales. El producto escalar $\langle\phi'|\psi'\rangle$ es:

$$\langle\phi'|\psi'\rangle = a^2\langle\phi|\psi\rangle - b^{*2}\langle\psi|\phi\rangle + ab^*\big(\langle\psi|\psi\rangle - \langle\phi|\phi\rangle\big)$$

Si $\langle\phi|\psi\rangle \neq 0$, entonces igualando $\langle\phi'|\psi'\rangle$ a 0 resulta en una ecuación cuadrática para *a*/*b**, la cual tiene dos soluciones complejas. Si *a* es un número complejo diferente de 0, entonces cualquier solución determina *b*, que junto con *a* produce una unitaria de un qubit **u** para la cual:

$$(u \otimes 1)|\Psi\rangle = |0\rangle \otimes |\psi'\rangle + |1\rangle \otimes |\phi'\rangle$$

Donde $|\psi'\rangle$ y $|\phi'\rangle$ son ortogonales. Si $\langle\phi|\psi\rangle = 0$ entonces $|\Psi\rangle = |0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\phi\rangle$ ya es de esta forma con **u** = 1

Se pueden escoger números reales positivos λ y μ de manera que $|\psi''\rangle = |\psi'\rangle/\lambda$ y $|\phi''\rangle = |\phi'\rangle/\mu$ son vectores unitarios, haciendo de $|\psi''\rangle$ y $|\phi''\rangle$ un par orto normal. Ellos están por tanto relacionados a $|0\rangle$ y $|1\rangle$ por una transformación unitaria **v**:

$$|\psi''\rangle = v|0\rangle \qquad |\phi''\rangle = v|1\rangle$$

De manera que la ecuación se transforma en:

$$|\Psi\rangle = (u^t \otimes v)(\lambda|0\rangle \otimes |0\rangle + \mu|1\rangle \otimes |1\rangle)$$

Lo cual se puede reescribir como:

$$|\Psi\rangle = (u^t \otimes v)C_{10}(\lambda|0\rangle + \mu|1\rangle) \otimes |0\rangle$$

Dado que $|\psi\rangle$ es un vector unitario y las transformaciones unitarias preservan los vectores unitarios, se deduce de lo anterior que $\lambda|0\rangle + \mu|1\rangle$ es un vector unitario. Puede por tanto ser obtenido de $|0\rangle$ por una transformación **w**. Finalmente:

$$|\Psi\rangle = (u^t \otimes v)C_{10}(w \otimes 1)(|0\rangle \otimes |0\rangle) = u_1^t v_0 C_{10} w_1 |00\rangle$$

Se ha establecido que el estado general de dos qubits puede ser construido a partir de tres unitarias de un qubit y una sola puerta cNOT, actuando sobre el estado estándar $|00\rangle$.

La puerta cNOT tiene el efecto de entrelazar dos qubits, y para facilitar las cosas, a partir del entrelazamiento de dos qubits, se pueden entrelazar *n* qubits.

2.6. Bits vs Qubits

La tabla siguiente provee una comparación de las propiedades elementales de bits y qubits. La tabla utiliza el término Bits con mayúscula para representar "bits o qubits".

	bits	**qubits**
Estados de n Bits	$\|x\rangle_n$, $0 \le x < 2^n$	$\sum \alpha_x \|x\rangle_n$, $\sum \|\alpha_x\|^2 = 1$
Subconjuntos de n Bits	Siempre tienen estados	Generalmente no tienen estados
Operaciones reversibles sobre estados	Permutaciones	Transformaciones unitarias
Puede el estado ser conocido a partir de Bits	Si	No
Para conocer el estado de Bits	Examinarlos	Conocer la preparación del estado inicial y las puertas que han actuado
Para obtener información de Bits	Mirarlos	Medirlos
Información obtenida	x	x con probabilidad $\|\alpha_x\|^2$
Estado luego de obtener información	El mismo: todavía $\|x\rangle$	Diferente: ahora $\|x\rangle$

Tabla 1.1 Un resumen de las características de qubits, contrastado con las características análogas de bits.

2.7. El proceso computacional cuántico

Un computador cuántico apropiadamente programado debería actuar sobre un número *x* para producir otro número *f(x)* para alguna función especificada *f*. Correctamente interpretado, con una precisión que se incrementa mientras se incrementa *k*, se pueden considerar tales números como enteros no negativos menores que 2^k. Cada entero es representado en el computador cuántico por el correspondiente estado de la base computacional de *k* qubits.

Si se especifican los números *x* como enteros de n bits y los números *f(x)* con enteros de m bits, entonces se necesitan al menos *n + m* qubits: un conjunto de *n* qubits llamado *registro de entrada*, para representar *x*, y otro conjunto de *m* qubits, llamado el *registro de salida*, para representar *f(x)*. La razón para tener registros separados es que si *f(x)* asigna el mismo valor a diferentes valores de *x* entonces el proceso computacional no puede ser invertido, si su único efecto es transformar los contenidos de un solo registro de *x* a *f(x)*. Tener registros separados de entrada y salida es la práctica estándar en la teoría clásica de la computación reversible. Dado que los computadores cuánticos deben operar reversiblemente (a excepción de las puertas de medición), están diseñados para operar con estos dos registros.

El proceso computacional generalmente requerirá muchos qubits además de los *n + m* en los registros de entrada y salida, pero se puede ignorar estos qubits adicionales debido a la reversibilidad del proceso computacional. De manera que el cálculo de *f* consiste solamente en aplicar una transformación unitaria $\mathbf{U}_f$ a los *n + m* qubits. El protocolo cuántico-computacional estándar define la acción de $\mathbf{U}_f$ sobre los estados de la base computacional $|x\rangle_n|y\rangle_m$ de los *n + m* qubits que forman los registros de entrada y salida como:

$$U_f\left(|x\rangle_n|y\rangle_m\right)=|x\rangle_n|y\oplus f(x)\rangle_m$$

Donde $\oplus$ indica la adición módulo 2 (o exclusivo) bit por bit.

Si el valor inicial representado por el registro de salida es *y = 0* entonces se tiene:

$$U_f\left(|x\rangle_n|0\rangle_m\right)=|x\rangle_n|f(x)\rangle_m$$

Se obtiene *f(x)* en el registro de salida. Sin importar el valor inicial de *y*, el registro de entrada se mantiene en su estado inicial $|x\rangle_n$.

La transformación anterior es claramente invertible, en realidad, $\mathbf{U}_f$ es su propia inversa:

$$U_f U_f\left(|x\rangle_n|y\rangle_m\right) = U_f\left(|x\rangle_n|y\oplus f(x)\rangle_m\right)$$
$$= |x\rangle_n|y\oplus f(x)\oplus f(x)\rangle_m = |x\rangle_n|y\rangle_m$$

Dado que $z\oplus z = 0$ para cualquier *z*.

Si se aplica a cada qubit en el estado de dos qubits $|0\rangle|0\rangle$ la transformación Hadamard de 1 qubit **H**, entonces se obtiene:

$$(H\otimes H)(|0\rangle\otimes|0\rangle) = H_1H_0|0\rangle|0\rangle = (H|0\rangle)(H|0\rangle)$$
$$= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$
$$= \frac{1}{2}(|0\rangle|0\rangle+|0\rangle|1\rangle+|1\rangle|0\rangle+|1\rangle|1\rangle)$$
$$= \frac{1}{2}(|0\rangle_2+|1\rangle_2+|2\rangle_2+|3\rangle_2)$$

Lo cual claramente se generaliza al producto tensor de *n* Hadamards, aplicado al estado de *n* qubits $|0\rangle_n$:

$$H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}}\sum_{0\le x<2^n}|x\rangle_n$$

Donde

$$H^{\otimes n}|0\rangle_n = H\otimes H\otimes\cdots\otimes H, \qquad n \text{ veces}$$

De manera que si el estado inicial del registro de entrada es $|0\rangle_n$ y se aplica una transformación Hadamard *n* veces a ese registro, su estado se convierte en una superposición igualmente ponderada de todos los posibles *n* qubits de entrada. Si entonces se aplica $\mathbf{U}_f$ a esa superposición, con 0 inicialmente en el registro de salida, entonces por linealidad se obtiene:

$$U_f\left(H^{\otimes n}\otimes 1_m\right)(|0\rangle_n|0\rangle_m) = \frac{1}{2^{n/2}}\sum_{0\le x<2^n}U_f\left(|x\rangle_n|0\rangle_m\right)$$
$$= \frac{1}{2^{n/2}}\sum_{0\le x<2^n}|x\rangle_n|f(x)\rangle_m$$

El resultado de este proceso computacional se describe por un estado cuya estructura no puede ser explícitamente especificada sin conocer el resultado de todas las 2^n evaluaciones de la función *f*. De manera que si se tienen apenas 100 qubits en el registro de

entrada, inicialmente todos en el estado $|0\rangle_{100}$ (y *m* más en el registro de salida), si un ciento de transformaciones Hadamard actúan sobre el registro de entrada antes de la aplicación de $\mathbf{U}_f$, entonces la forma del estado final contiene los resultados de $2^{100} \approx 10^{30}$ evaluaciones de la función *f*. Un billón de billones de trillones de evaluaciones! Este aparente milagro es lo que se conoce como *paralelismo cuántico*.

Sin embargo, una gran parte del milagro es solo aparente. No se puede decir que el resultado del cálculo son 2^n evaluaciones de *f*; todo lo que se puede decir es que esas evaluaciones caracterizan a la forma del estado que describe el resultado del cómputo. Se sabe cuál es ese estado solo si ya se conocen los valores numéricos de esas 2^n evaluaciones de *f*. Pero cuando se tiene una colección de qubits en un estado definido pero desconocido, no hay manera de averiguar cuál es ese estado. La única manera de extraer alguna medición es someter los qubits a una medición.

Luego de la medición el estado de los registros se reduce a $|x_0\rangle f|(x_0)\rangle$, siendo x_0 un *x* al azar, y no hay manera de conocer algo sobre los valores de *f* para otros valores de *x*. Así que a pesar de que es posible conocer algo sobre el resultado del "cómputo en paralelo", no es nada más de lo que se hubiera podido conocer simplemente iniciando con el estado $|x\rangle$ en el registro de entrada, con el valor de *x* escogido al azar. Lo cual, por supuesto, podría haber sido realizado con un computador clásico.

Algo del milagro queda en el hecho de que para el caso cuántico la selección de *x* es hecha solo después de que el proceso computacional ha sido llevado a cabo.

Si existiera una forma fácil de realizar copias del estado de salida antes de hacer una medición, sin ejecutar todo el proceso de nuevo, entonces se podría, con alta probabilidad, conocer los valores de *f* para varios valores de *x* diferentes (al azar). Pero tal copia se prohíbe por un resultado elemental llamado el "teorema de no clonación", el cual enuncia que no existe tal proceso de duplicación: no hay una transformación unitaria que pueda llevar el estado $|\psi\rangle_n|0\rangle_n$ al estado $|\psi\rangle_n|\psi\rangle_n$ para un $|\psi\rangle_n$ arbitrario.

El teorema de no clonación es una consecuencia inmediata de linealidad si:

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle \qquad \text{y} \qquad U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle$$

Entonces se deduce por linealidad que:

$$U(a|\psi\rangle + b|\phi\rangle)|0\rangle = aU|\psi\rangle|0\rangle + bU|\phi\rangle|0\rangle = a|\psi\rangle|\psi\rangle + b|\phi\rangle|\phi\rangle$$

Pero si U clona entradas arbitrarias, se tendría:

$$U\left(a|\psi\rangle + b|\phi\rangle\right)|0\rangle = \left(a|\psi\rangle + b|\phi\rangle\right)\left(a|\psi\rangle + b|\phi\rangle\right) = a^2|\psi\rangle|\psi\rangle + b^2|\phi\rangle|\phi\rangle + ab|\psi\rangle|\phi\rangle + ab|\phi\rangle|\psi\rangle$$

Las dos equivalencias son diferentes a menos que a y b sean cero. Sorprendentemente, este teorema tan simple no fue probado hasta medio siglo después del descubrimiento de la mecánica cuántica.

Por supuesto, la habilidad de clonar a un razonable grado de aproximación sería bastante útil. Pero esto también es imposible. Suponiendo que **U** aproximadamente clona $|\psi\rangle$ y $|\phi\rangle$:

$$U\left(|\psi\rangle|0\rangle\right) \approx |\psi\rangle|\psi\rangle \qquad \text{y} \qquad U\left(|\phi\rangle|0\rangle\right) \approx |\phi\rangle|\phi\rangle$$

Entonces dado que las transformaciones unitarias preservan los productos escalares, dado que el producto escalar de un producto tensor de estados es el producto ordinario de sus productos escalares, y dado que $\langle 0|0\rangle = 1$ se deduce que:

$$\langle\phi|\psi\rangle \approx \langle\phi|\psi\rangle^2$$

Lo cual requiere que $\langle\phi|\psi\rangle$ sea cercano a 1 o cercano a 0. Por tanto una transformación unitaria puede llegar cerca de la clonación de ambos estados $|\psi\rangle$ y $|\phi\rangle$ solo si los estados son casi los mismos o muy cercanamente a ser ortogonales. En todos los otros casos, al menos uno de los dos estados no se copiará bien.

Si esta fuera toda la historia, solo unos pocos filósofos estarían interesados en la computación cuántica. Sin embargo existe gran interés porque cosas más ingeniosas se pueden hacer. Estas involucran aplicar puertas unitarias adicionales a uno o ambos registros de entrada y salida antes y/o después de aplicar $\mathbf{U}_f$, algunas veces mezclados con puertas de medición intermedias actuando sobre un subconjunto de qubits. Todas estas puertas son cuidadosamente escogidas de manera que cuando finalmente se realiza la medición de todos los qubits, se extrae información útil acerca de la *relaciones* entre los valores de *f* para varios valores diferentes de *x*, lo cual un computador clásico solo podría obtener haciendo varias evaluaciones independientes. El precio que se paga por esta información relacional es perder la posibilidad de conocer el valor de *f(x)* para un *x* específico. Este sacrificio de un tipo de información por otro es típico de la computación cuántica, y típico de la física cuántica en general, donde se llama *principio de incertidumbre*. El mismo principio inicialmente enunciado por Werner Heisenberg en el contexto de la información mecánica – la posición de una partícula contra su momento.

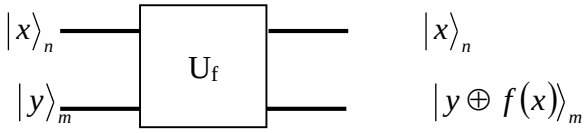


Figura 1.5 Una representación esquemática de la transformación unitaria $\mathbf{U}_f$ para evaluar la función transformando un número $0 \le x < 2^n$ en un número $0 \le f(x) < 2^m$. Para que el proceso computacional sea reversible cuando *f* no es uno a uno, dos registros de múltiples qubits deben ser utilizados.

El proceso computacional generalmente requiere el uso de muchos qubits además de *n* + *m* en los registros de entrada y salida. La acción del computador se describe entonces por la transformación unitaria $\mathbf{W}_f$ que actúa sobre todos los qubits, asumiendo que se utilizan *r* qubits adicionales. En general los registros de entrada y salida llegarán a estar entrelazados con los estados de los *r* qubits adicionales y no se les puede ni siquiera asignar un estado. Pero si la acción del computador sobre los *n* + *m* + *r* qubits es de una forma especial, los registros de entrada y salida pueden en verdad terminar con un estado, relacionado con sus estados iniciales mediante la transformación unitaria deseada $\mathbf{U}_f$. Si los *r* qubits adicionales empiezan en algún estado inicial estándar $|\psi\rangle_r$, entonces el estado inicial del registro de entrada, el registro de salida y los qubits adicionales es:

$$|\Psi\rangle_{n+m+r} = |x\rangle_n |y\rangle_m |\psi\rangle_r$$

A pesar de que los qubits adicionales llegarán a estar entrelazados con los registros de entrada y salida para ser de utilidad, cuando el cálculo termine, el estado final del computador será de la forma:

$$W_f |\Psi\rangle_{n+m+r} = |x\rangle_n |y \oplus f(x)\rangle_m |\phi\rangle_r$$

Donde los qubits adicionales no solo estarán des-entrelazados de los registros de entrada y salida, sino que también tendrán un estado $|\phi\rangle_r$, que es independiente del estado inicial de los registros de entrada y salida. Esta independencia de los estados iniciales puede ser arreglada mediante la inicialización de los *r* qubits adicionales a algún estado inicial estándar, por ejemplo, $|\psi\rangle_r = |0\rangle_r$. Un estado final estándar $|\phi\rangle_r$, el cual es en realidad idéntico a su estado inicial $|\psi\rangle_r$, puede ser producido tomando ventaja del hecho de que las transformaciones unitarias son reversibles, con lo cual la transformación que entrelaza los

registros de entrada y salida a los qubits adicionales puede ser deshecha luego del cálculo aplicando su conjugada adjunta.

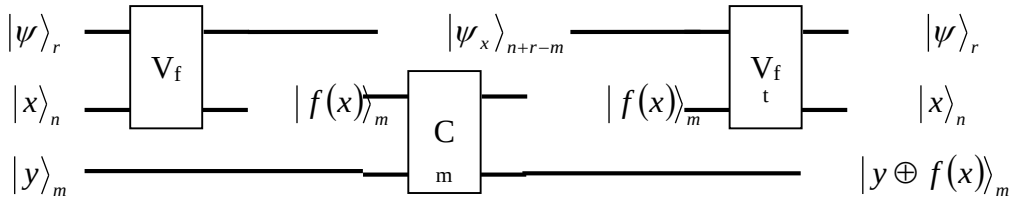


Figura 1.6 Una vista detallada de la transformación unitaria $\mathbf{W}_f$. Algebraicamente $\mathbf{W}_f=\mathbf{V}_f{}^t\mathbf{C}_m\mathbf{V}_f$. Primero una transformación unitaria $\mathbf{V}_f$ actúa sobre el registro de entrada y los qubits adicionales, actuando como la identidad sobre el registro de salida. Esta operación transforma los $n + r$ qubits en un estado en el cual un subset de m qubits representa el resultado de $f(x)$. Luego una transformación cNOT actúa sobre estos m qubits y los m qubits del registro de salida, dejando el primero sin cambios pero cambiando el número representado por el registro de salida de y a $y \oplus f(x)$. Finalmente la inversa $\mathbf{V}_f{}^t$ es aplicada a los $n + r$ qubits para regresarlos a sus estados iniciales (no entrelazados).

2.8. Encontrar el periodo, factorización y criptografía

Un problema difícil, pero muy natural, es encontrar el periodo de una función *f* sobre los enteros que es periódica bajo adición ordinaria, satisfaciendo *f(x)=f(y)* para distintos *x* y *y* si y solo si *x* y *y* difieren por un múltiplo integral de r. Encontrar el periodo de tal función periódica resulta ser la clave para factorizar productos de grandes números primos, un problema natural de las matemáticas con aplicaciones bastante prácticas.

Se podría pensar que encontrar el periodo de tal función periódica debería ser fácil, pero eso es solo porque al pensar en funciones periódicas se tiende a imaginar funciones continuas que varían lentamente (como la función del seno) cuyos valores en un pequeño intervalo de puntos dentro del periodo pueden dar importantes pistas sobre cuál podría ser este periodo. Pero el tipo de función a considerar es una función sobre los enteros cuyos valores dentro de un periodo *r* son virtualmente aleatorios de un entero al siguiente, y por tanto no proporcionan ninguna pista sobre el valor de *r*.

El más conocido de los algoritmos clásicos para encontrar el periodo *r* de tal función toma un tiempo que crece más rápido que cualquier potencia del número *n* de bits de *r* (exponencialmente con $n^{1/3}$). Pero en 1994 Peter Shor descubrió que se puede explotar el poder de un computador cuántico para conocer el periodo *r*, en un tiempo que crece solo un poco más rápido que n^3.

Debido a que la habilidad de encontrar periodos eficientemente, combinada con algunos trucos de la teoría de números, permite factorizar eficientemente el producto de dos números primos de gran magnitud, el descubrimiento de Shor es de considerable interés práctico. Bajo el gran esfuerzo computacional requerido por todas las técnicas de factorización clásica yace la base de la seguridad del ampliamente utilizado método de encriptación RSA[36]. Cualquier computador que pueda eficientemente encontrar periodos sería una gran amenaza a la seguridad de comunicaciones tanto militares como comerciales. Esta es la razón por la cual la investigación sobre la factibilidad de computadores cuánticos es un asunto de considerable interés en los mundos de la guerra y los negocios.

[36] Nombrado en honor a las personas que lo inventaron en 1977, Ronald Rivest, Adi Shamir, y Leonard Adleman. La encriptación RSA fue independientemente inventada por Clifford Cocks cuatro años antes, pero su descubrimiento se clasificó como ultrasecreto por la Inteligencia Británica y no le fue permitido revelar su prioridad hasta 1997.

2.8.1. Teoría de los números elemental

Se dice que *a* es congruente con *b* módulo *q*:

$$a \equiv b(\mathrm{mod}\, q)$$

Si $a - b$ es un múltiplo de *q*. Está condición también puede ser expresada por la notación $q \mid (a-b)$, la cual se lee "q divide a menos b". Un conjunto de todos los enteros congruentes (mod *q*) se llama clase de congruencia (por ejemplo el conjunto de números impares y el conjunto de números pares son clases de congruencia módulo 2). Cada clase puede ser caracterizada por su representativo canónico, un entero $r \in \{0,\ldots,q-1\}$. Se dice:

$$a \bmod q = r$$

Lo cual precisamente significa que *r* es el residuo de *a* (el sobrante de la división entera de *a* para *q*), $a = mq + r$, donde $m \in Z$, $r \in \{0,\ldots,q-1\}$. En la mayoría de casos no es necesario hacer una distinción entre clases de congruencia y sus representativos canónicos, así que el término "residuo" se refiere a ambos. De manera que $7 \bmod 3 = 1$ es la clase de congruencia que contiene 7 y cuyo representante canónico es 1: el conjunto $\{\ldots,-5,-2,1,4,7,\ldots\}$.

Los residuos (clases de congruencia) pueden ser sumados, restados o multiplicados al realizar las correspondientes operaciones sobre los enteros que representan. Por tanto $r = r_1 r_2$ (multiplicación modular) si y solo si $a \equiv a_1 a_2 (\mathrm{mod}\, q)$, donde $a \bmod q = r$, $a_1 \bmod q = r_1$, y $a_2 \bmod q = r_2$. Es importante notar que a_1 y a_2 pueden ser reemplazados por cualquier número congruente (mod *q*), siendo el producto congruente también. De manera que:

$$\text{Si } a_1 \equiv b_1 \text{ y } a_2 \equiv b_2, \text{ entonces } a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\, q)$$

Las operaciones aritméticas de enteros y las operaciones con residuos (mod *q*) forman anillos conmutativos.

Un *anillo* es un conjunto *R* equipado con dos operaciones binarias, "+" y "." (el punto usualmente se suprime al escribir), y dos elementos especiales, 0 y 1, de manera que las siguientes relaciones se mantienen:

$$(a+b)+c = a+(b+c), \qquad a+b = b+a, \qquad a+0 = a,$$

$$(ab)c = a(bc), \qquad 1 \cdot a = a \cdot 1 = a,$$

$$(a+b)c = ac+bc, \qquad c(a+b) = ca+cb$$

Para todo $a \in R$ existe un elemento *v* tal que $a + v = 0$.

Si además, $ab = ba$ para cualquier *a* y *b*, entonces *R* es llamado un *anillo conmutativo*. Todas las siguientes definiciones solo consideran anillos conmutativos.

Se puede notar que el elemento *v* es único. Pues, si otro elemento *v'* satisface $a + v' = 0$, entonces:

$$v' = v' + 0 = v' + (a + v) = (v' + a) + v = (a + v') + v = 0 + v = v + 0 = v$$

Tal *v* se nota como *–a*. Las relaciones en la lista implican otras relaciones bien conocidas, por ejemplo, $a \cdot 0 = 0$.

La diferencia entre dos elementos de un anillo se define como $a - b \overset{def}{=} a + (-b)$. Un anillo se convierte en un grupo Abeliano si se dejan de lado la multiplicación y el 1, pero se conservan + y 0. Este grupo se llama el grupo aditivo del anillo. El anillo de residuos módulo *q* se denota por *Z/qZ*, mientras que el grupo aditivo correspondiente se denota por Z_q (este es precisamente el grupo cíclico de orden *q*).

Una de las diferencias entre el anillo de enteros *Z* y el anillo de residuos *Z/qZ* es que Z es infinito mientras que *Z/qZ* es finito. Otra importante distinción es la siguiente. Para enteros, *xy=0* implica que *x=0* o *y=0*. Esto no es verdad para anillos de residuos (específicamente es falso en el caso donde *q* es un número compuesto). Por ejemplo en el caso de los residuos *Z/10Z*, $r \in \{0,1,2,3,4,5,6,7,8,9\}$, donde cada elemento representa su clase de congruencia, $2 \cdot 5 \equiv 0 (\mathrm{mod}\, 10)$, dado que los elementos del anillo de residuos son cíclicos y 10 es en realidad representado por 0, y se cumple que $2 \cdot 5 - 0 = 10$; a pesar de que tanto 2 como 5 representan elementos diferentes de 0 en *Z/10Z*.

Se dice que un elemento *x* de un anillo *R* es un *divisor de cero* si $\exists y \neq 0 (xy = 0)$. Por ejemplo 0,2,3,4,6,8,9,10 son divisores de cero en *Z/12Z*, mientras que 1,5,7,11 no lo son. Se puede demostrar que *r* es un divisor de cero en *Z/qZ* si y solo si *r* y *q* (considerados como enteros) tiene un divisor común no trivial (que no sea 1).

Existe otro concepto importante al hablar de anillos. Un elemento $x \in R$ es llamado invertible si existe un *y* tal que *xy=1*; en este caso se escribe $y=x^{-1}$. Por ejemplo, $7=4^{-1}$ en *Z/9Z* dado que $7 \cdot 4 \equiv 1 (\mathrm{mod}\, 9)$. Es obvio que si *a* y *b* son invertibles entonces *ab* también lo es y $(ab)^{-1}=a^{-1}b^{-1}$. Por consiguiente elementos invertibles forman un grupo Abeliano con respecto a la multiplicación, el cual se denota *R**. Por ejemplo, $Z^* = \{1,-1\}$ y

$(Z/12Z)^* = \{1,5,7,11\}$. En el último caso, los elementos invertibles son exactamente los elementos que no son divisores de cero, lo cual no es una coincidencia.

Si un elemento $x \in R$ es invertible, entonces *x* no es un divisor de cero. En el caso donde *R* es finito, lo opuesto también es cierto. Suponiendo que *xy=0*, entonces:

$$y = (x^{-1}x)y = x^{-1}(xy) = x^{-1} \cdot 0 = 0$$

Ahora asumiendo que *x* no es un divisor de cero, y que *R* es finito. Entonces algunos elementos en la secuencia $x, x^2, x^3, \ldots$ deben repetirse, de manera que existe algún $n > m \geq 0$ tal que $x^n = x^m$. Por tanto $x^m(x^{n-m} - 1) = 0$. Esto implica que $x^{m-1}(x^{n-m} - 1) = 0$ dado que *x* no es un divisor de cero. Iterando el argumento se obtiene $x^{n-m} - 1 = 0$, luego $x^{n-m} = 1$ y finalmente $x^{n-m-1} = x^{-1}$.

Si p es un número primo, entonces cada elemento diferente de cero del anillo *Z/pZ* es invertible. Un anillo con esta propiedad se llama *campo*. El campo *Z/9Z* también se denota por F_p.

2.8.2. Utilizar un grupo con respecto a la multiplicación

Sea G_N el conjunto de todos los enteros positivos menores que *N* (incluyendo 1) que no tienen factores en común con *N*. Dado que su factorización en primos es única, el producto de dos número en G_N (sea el producto ordinario o el producto módulo N) tampoco tiene factores en común con N, de manera que G_N es cerrado con respecto a la multiplicación módulo *N*. Si *a*, *b* y *c* están en G_N bajo la condición $ab \equiv ac \pmod N$, entonces $a(b-c)$ es un múltiplo de N, y dado que *a* no tiene factores en común con *N*, entonces *b-c* debe ser un múltiplo de *N*, de manera que $b \equiv c \pmod N$. De manera que la operación de multiplicación módulo *N* por un miembro fijo a de G_N convierte miembros distintos de G_N en miembros distintos, es decir que la operación permuta los miembros del conjunto finito G_N. Dado que 1 es un miembro de G_N, debe existir algún *d* en G_N que satisface $ad \equiv 1 - a$ debe tener un inverso multiplicativo en G_N. Por tanto G_N satisface las condiciones para ser un grupo módulo N con respecto a la multiplicación, es decir representa $(Z/NZ)^*$.

Cada miembro *a* de un grupo finito *G* se caracteriza por su *orden k*, el entero más pequeño para el cual (en el caso de G_N):

$$a^k \equiv 1 \pmod N$$

Gracias al teorema de Lagrange (el orden de cualquiera de los subgrupos divide el orden del grupo), el orden de cada miembro de *G* es un divisor del número de miembros de *G* (el orden de *G*). Si *p* es un número primo, el grupo G_p (equivalente al campo F_p) contiene *p - 1* números, dado que ningún entero positivo menor que *p* tiene factores en común con *p*. Entonces *p - 1* es múltiplo del orden *k* de cualquier *a* en G_p, y se deduce de la equivalencia anterior que cualquier entero *a* menor que *p* satisface:

$$a^{p-1} \equiv 1 (\text{mod } p)$$

Esta relación, conocida como el *pequeño teorema de Fermat*, se extiende a enteros arbitrarios *a* no divisibles por *p*, dado que tal *a* es de la forma $a = mp + a'$ siendo *m* un entero y *a'* menor que *p*.

La encriptación RSA explota una extensión del pequeño teorema de Fermat al caso caracterizado por dos números primos distintos, *p* y *q*. Si un entero *a* no es divisible ni por *p* ni por *q*, entonces ninguna potencia de *a* lo es. Entonces, en particular, a^{q-1} no es divisible por *p*, y aplicando el pequeño teorema de Fermat se obtiene:

$$\left[a^{q-1}\right]^{p-1} \equiv 1 (\text{mod } p)$$

Por la misma razón se obtiene:

$$\left[a^{p-1}\right]^{q-1} \equiv 1 (\text{mod } q)$$

Estas dos relaciones concluyen que $a^{(q-1)(p-1)} - 1$ es un múltiplo tanto de *p* como de *q*. Dado que *p* y *q* son números primos distintos, debe por tanto ser un múltiplo *pq*, y por consiguiente:

$$a^{(q-1)(p-1)} \equiv 1 (\text{mod } pq)$$

Si, por ejemplo p=3 y q=5 entonces se requiere que 2^8 - 1 sea divisible por 15, y en verdad, 255 = 17 x 15.

Como una derivación alternativa de la equivalencia anterior, se puede notar que dado que *a* no es divisible ni por *p* ni por *q*, no tiene factores en común con *pq* y se encuentra por tanto en G_{pq}. El número de elementos de G_{pq} es $pq - 1 - (p-1) - (q-1) = (p-1)(q-1)$, dado que existen *pq – 1* enteros menores que *pq*, de los cuales *p – 1* son múltiplos de *q* y distintos *q – 1* son múltiplos de *p*. De lo cual también se deduce la equivalencia anterior pues el orden $(p-1)(q-1)$ de G_{pq} debe ser un múltiplo del orden de *a*.

La versión de esta equivalencia que es la base de la encriptación RSA se obtiene tomando una potencia entera *s* de $a^{(q-1)(p-1)} \equiv 1 (\text{mod } pq)$ y multiplicando ambos lados por *a*:

$$a^{1+s(q-1)(p-1)} \equiv a(\text{mod } pq)$$

Esta relación se mantiene incluso para enteros *a* que son divisibles por *p* o *q*.

Se puede notar finalmente que no tiene factores en común con $(p-1)(q-1)$, entonces c se encuentra en $G_{(p-1)(q-1)}$ y por tanto tiene una inversa en $G_{(p-1)(q-1)}$, es decir existe un *d* en $G_{(p-1)(q-1)}$ que satisface:

$$cd \equiv 1(\text{mod}(p-1)(q-1))$$

De manera que para algún entero *s*:

$$cd = 1 + s(p-1)(q-1)$$

A la vista de las dos equivalencias anteriores, cualquier entero *a* debe satisfacer:

$$a^{cd} \equiv a(\text{mod } pq)$$

De forma que si

$$b \equiv a^c (\text{mod } pq)$$

Entonces

$$b^d \equiv a(\text{mod } pq)$$

Los hechos matemáticos elementales resumidos en estas últimas equivalencias constituyen toda la base de la encriptación RSA.

2.8.3. Encriptación RSA

Bob quiere recibir un mensaje de Alice codificado de tal manera que solo él pueda leerlo. Para hacerlo escoge dos grandes (200 dígitos) números primos *p* y *q*. Le da a Alice su producto *N* = *pq* y un gran número codificador *c* que ha escogido de manera que no tenga factores en común con $(p-1)(q-1)$[37]. El no revela, sin embargo, los valores separados de *p* y *q* y, dada la imposibilidad práctica de factorizar un número de 400 dígitos con los computadores actualmente disponibles, está bastante confiado en que ni Alice ni alguna espía Eve puedan calcular *p* y *q* conociendo solo su producto *N*. Bob, sin embargo, dado que conoce *p* y *q*, y por tanto $(p-1)(q-1)$, puede encontrar la inversa multiplicativa *d* de *c*

[37] La probabilidad de que dos grandes números aleatorios no tengan factores en común es mayor a ½, de manera que tales *c* son fácilmente encontrados. Si dos números tienen factores en común, esto puede ser determinado por el algoritmo de Euclides y fácilmente ejecutado por Bob en un computador clásico.

módulo $(p-1)(q-1)$, la cual satisface $cd \equiv 1(\text{mod}(p-1)(q-1))$. El guarda *d* estrictamente para sí mismo para utilizarla en la decodificación.

Alice codifica un mensaje representándolo como una cadena de menos de 400 dígitos utilizando, por ejemplo, alguna versión de codificación ASCII. Si su mensaje requiere más de 400 dígitos lo corta en piezas más pequeñas. Ella interpreta tales cadenas como un número *a* menor que *N*. Utilizando el número codificador *c* y el valor de *N* que recibe de Bob calcula $b \equiv a^c \pmod{pq}$ y lo envía a mediante un canal público. Con *c* siendo típicamente un número de 200 dígitos, se podría pensar que esto mismo sería requeriría grandes recursos computacionales, pero no es así, lo cual se muestra posteriormente. Cuando recibe *b*, Bob explota su conocimiento privado de *d* para calcular $b^d \pmod{pq}$, lo cual es el mensaje *a* original del Alice.

Si la espía Eve pudiese encontrar los factores *p* y *q* de *N*, podría calcular $(p-1)(q-1)$ y encontrar el entero decodificador *d* a partir del entero codificador públicamente disponible *c*, en la misma forma que Bob lo hizo. Pero factorizar un número tan grande como *N* está muy por encima de su capacidad computacional clásica. La búsqueda eficiente del periodo es de interés en este escenario criptográfico no solo porque lleva directamente a factorización eficiente, sino porque puede llevar a Eve directamente a una forma alternativa de decodificar el mensaje de Alice *b* sin tener que calcular los factores *p* y *q*.

2.8.4. Búsqueda cuántica del periodo

Todo se reduce a encontrar el periodo *r* de la función periódica conocida:

$$f(x) = b^x \pmod{N}$$

Esto parece ser una tarea simple, especialmente dado que las funciones periódicas de esta forma tienen la característica de que $f(x+s) = f(x)$ solo si *s* es un múltiplo del periodo *r*. Pero $b^x \pmod{N}$ es precisamente el tipo de función cuyos valores dentro de un periodo brincan tan irregularmente que no ofrecen pistas obvias acerca del periodo. Se podría intentar evaluar $f(x)$ para un *x* aleatorio hasta que se encuentren dos valores de *x* diferentes para los cuales *f* sea la misma. Esos valores difieren por un múltiplo del periodo, lo cual proveería información útil acerca del periodo en sí. Pero es una manera ineficiente de proceder, incluso clásicamente.

Sea n_0 el número de bits en $N = pq$, de manera que 2^{n0} es la potencia de 2 más pequeña que excede *N*. Si N es un número de 500 dígitos – un tamaño típico para aplicaciones criptográficas - n_0 tendría alrededor de 1700. Esto también marca la escala para el número típico de bits de los otros números relevantes *a*, *b* y su periodo *r* módulo *N*. Para tener una probabilidad apreciable de encontrar *r* mediante búsqueda aleatoria se requiere un número de evaluaciones de *f* que es exponencial en n_0. Existen métodos clásicos que mejoran la búsqueda aleatoria, utilizando, por ejemplo, el análisis de Fourier, pero no se conoce ningún enfoque clásico que no requiera un tiempo que crece más rápido que alguna potencia de n_0. Con un computador cuántico, sin embargo, el paralelismo cuántico lleva tentadoramente cerca de resolver el problema con una sola aplicación de $\mathbf{U}_f$, y permite resolverlo completamente con una probabilidad arbitrariamente cerca de la unidad en un tiempo que crece solo como un polinomio de bajo orden en n_0.

Para tratar con los valores de *x* y $f(x) = b^x \pmod N$ entre 0 y N, tanto el registro de entrada como el de salida deben contener al menos n_0 qubits. Por razones que emergerán posteriormente, para encontrar el periodo *r* eficientemente el registro de entrada debe tener realmente $n=2\,n_0$ qubits. Doblar el número de qubits en el registro de entrada asegura que el rango de valores de *x* para los cuales $f(x)$ es calculada contiene al menos *N* periodos completos de *f*. Esta redundancia resulta ser esencial para una determinación exitosa del periodo con el método de Shor.

El algoritmo de búsqueda del periodo empieza utilizando el computador cuántico en la forma familiar para construir el estado:

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n \, |f(x)\rangle_{n_0}$$

Con una sola aplicación de $\mathbf{U}_f$. Una vez que el estado de los registros se encuentra en esta forma, se puede realizar una medición sobre los *n* qubits del registro de salida. Si la medición produce el valor f_0, entonces la regla de Born predice que el estado de los *n* qubits del registro de salida puede considerarse como:

$$|\Psi\rangle_n = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n$$

Aquí x_0 es el menor valor de *x* $(0 \le x < r)$ para el cual $f(x_0) = f_0$, y *m* es el entero más pequeño para el cual $mr + x_0 \ge 2^n$, así:

$$m = \left\lfloor \frac{2^n}{r} \right\rfloor \qquad \text{o} \qquad m = \left\lfloor \frac{2^n}{r} \right\rfloor + 1$$

Dependiendo del valor de x_0 (donde $\lfloor x \rfloor$ es la parte entera de x – el entero más grande menor o igual que x). Si se pudiera producir un pequeño número de copias idénticas del estado anterior, el trabajo estaría listo, ya que una medición sobre la base computacional resultaría en uno de los valores de $x_0 + kr$ aleatorio y la diferencia entre los resultados de pares de medidas sobre tales copias idénticas daría una colección de múltiplos aleatorios de *r* de los cuales *r* en sí puede ser directamente extraído. Pero esta posibilidad es descartada por el teorema de no clonación. Todo lo que se puede extraer es un solo valor $x_0 + kr$ para un x_0 aleatorio desconocido, lo cual es inútil para determinar *r*. Y por supuesto si se ejecuta todo el algoritmo una vez más, se terminaría con un estado de la misma forma para otro valor aleatorio de x_0, lo cual no permite comparación útil con lo que se obtuvo en la primera ejecución.

Sin embargo, se puede hacer algo más ingenioso al estado $|\Psi\rangle_n = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n$ antes de realizar la medición final. El problema es el desplazamiento por el desconocido y aleatorio x_0, lo cual evita que cualquier información acerca de *r* sea extraída en una sola medición. Es necesaria una transformación unitaria que convierta la dependencia de x_0 en un factor de fase universal inofensivo. Esto se logra con la *transformada de Fourier cuántica*.

2.8.5. La transformada de Fourier Cuántica

El corazón del algoritmo de Shor es una súper rápida transformada de Fourier cuántica, la cual puede ser llevada a cabo por un circuito cuántico espectacularmente eficiente construido enteramente de puertas de 1 y 2 qubits. La transformada de Fourier cuántica para n qubits se define como la transformación unitaria $\mathbf{U}_{\text{FT}}$ cuya acción sobre la base computacional se da por:

$$U_{FT}|x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} |y\rangle_n$$

El producto *xy* aquí es multiplicación ordinaria. Se puede verificar fácilmente que $\mathbf{U}_{\text{FT}}$ es normalizada a la unidad y que $U_{FT}|x\rangle_n$ es ortogonal a $U_{FT}|x'\rangle_n$ a menos que x=x',

de manera que $\mathbf{U}_{FT}$ es unitaria. La unitariedad también emerge del análisis siguiente que explícitamente construye $\mathbf{U}_{FT}$ a partir de puertas unitarias de 1 y 2 qubits. La unitaria $\mathbf{U}_{FT}$ es útil porque aplicada a una superposición de estados $|x\rangle$ con amplitudes complejas $\gamma(x)$, produce otra superposición con amplitudes que están relacionadas a $\gamma(x)$ mediante la apropiada transformada de Fourier discreta:

$$U_{FT}\left(\sum_{x=0}^{2^n-1}\gamma(x)|x\rangle\right)=\sum_{x=0}^{2^n-1}\tilde{\gamma}(x)|x\rangle$$

Donde

$$\tilde{\gamma}(x)=\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}e^{2\pi ixy/2^n}\gamma(y)$$

La celebrada rápida transformada de Fourier clásica (FFT por sus siglas en inglés) es un algoritmo que requiere un tiempo que crece con el número de bits de forma $n2^n$ (en lugar de $(2n)^2$ como el obvio enfoque directo requeriría) para evaluar $\tilde{\gamma}$. Pero existe un algoritmo para ejecutar la transformación unitaria $\mathbf{U}_{FT}$ exponencialmente más rápido, en un tiempo que crece solo tanto como n^2. El truco, como siempre, es que se termina sin conocer el conjunto completo de coeficientes de Fourier, a diferencia de cuando se aplica FFT. De todas formas, como se ha notado repetidamente, luego de la aplicación de $\mathbf{U}_{FT}$ se tienen n qubits descritos por el estado de la ecuación, pero no se puede conocer cuál es ese estado, así que no hay manera de extraer todos los coeficientes $\tilde{\gamma}$. Pero si γ es una función periódica con un periodo no mayor a 2n/2, entonces un registro en ese estado puede dar importantes pistas acerca del valor preciso del periodo *r*, incluso si *r* tiene una longitud de varios cientos de dígitos.

Es destacable el parecido de la transformada de Fourier con la transformación Hadamard de orden n. Dado que $-1=e^{\pi i}$, la transformación Hadamard asume la forma:

$$H^{\otimes n}|x\rangle_n=\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}e^{\pi ix\cdot y}|y\rangle_n$$

Además de las diferentes potencias de 2 que aparecen en la transformada de Fourier – así los factores de módulo 1 en la superposición no son solo 1 y -1 – la única otra diferencia entre las dos transformaciones es que *xy* es multiplicación ordinaria en la transformada de Fourier, mientras que *x.y* es el producto escalar bit a bit en la transformación Hadamard. Debido a que el producto aritmético *xy* es una función más elaborada, la transformación de

Fourier cuántica no puede ser construida completamente de puertas unitarias de 1 qubit. Pero, notablemente, puede ser construida en su totalidad de puertas de 1 y 2 qubits. Y más destacable aún, cuando el procedimiento se utiliza para encontrar el periodo, todas las puertas de 2 qubits pueden ser reemplazadas por puertas de medición de 1 qubit seguidas por adicionales puertas unitarias de 1 qubit cuya aplicación es contingente sobre los resultados de la medición.

Para construir un circuito que ejecute la transformada de Fourier $\mathbf{U}_{FT}$, es conveniente introducir el operador unitario de n qubits Z, diagonal en la base computacional:

$$Z|y\rangle_n = e^{2\pi i y/2^n}|y\rangle_n$$

Esto puede ser visto como una generalización a n qubits del operador de 1 qubit **Z**, al cual se reduce cuando n=1. Utilizando la relación familiar:

$$H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}|y\rangle_n$$

Se puede expresar la definición de $\mathbf{U}_{FT}$ como:

$$U_{FT}|x\rangle_n = Z^x H^{\otimes n}|0\rangle_n$$

Esto resulta en $U_{FT}|x\rangle_n$ como un operador dependiente de x actuando sobre el estado $|0\rangle$.

Ahora se expresa nuevamente el lado derecho de la última equivalencia como un operador lineal independiente de x actuando sobre el estado $|x\rangle_n$. Dado que los estados de la base computacional $|x\rangle_n$ son una base, esto dará una expresión alternativa para $\mathbf{U}_{FT}$ en sí. La construcción de esta forma alternativa se hace más transparente especializándola al caso de 4 qubits. La estructura que emerge en el caso n=4 tiene una obvia extensión a un *n* general. Tratar con el caso de *n* desde el inicio solo obscurece las cosas.

Cuando n=4 el objetivo es encontrar una forma apropiada para:

$$U_{FT}|x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle = Z^x H_3 H_2 H_1 H_0 |0\rangle|0\rangle|0\rangle|0\rangle$$

Si $|y\rangle_4 = |y_3\rangle|y_2\rangle|y_1\rangle|y_0\rangle$ en la definición de Z, de manera que $y = 8y_3 + 4y_2 + 2y_1 + y_0$, entonces el operador Z puede ser construido a partir de operadores numéricos de un solo qubit:

$$Z = \exp\left(\frac{i\pi}{8}\left(8n_3 + 4n_2 + 2n_1 + n_0\right)\right)$$

El operador Z^x entonces se convierte en:

$$Z^x = \exp\left(\frac{i\pi}{8}(8x_3 + 4x_2 + 2x_1 + x_0)(8n_3 + 4n_2 + 2n_1 + n_0)\right)$$

Dado que el operador de 1 qubit $\exp(2\pi i n)$ actúa como la identidad sobre cualquiera de los estados de un qubit $|0\rangle$ y $|1\rangle$, y dado que cualquier estado de un qubit es una superposición de estos dos, **n** obedece al operador identidad:

$$\exp(2\pi i n) = 1$$

Y por tanto al multiplicar los términos que aparecen en el exponente, se pueden eliminar todos los productos $x_i\boldsymbol{n}_j$ cuyos coeficientes son una potencia de 2 mayor a 8, obteniendo:

$$Z^x = \exp\left[i\pi\left(x_0 n_3 + \left(x_1 + \frac{1}{2}x_0\right)n_2 + \left(x_2 + \frac{1}{2}x_1 + \frac{1}{4}x_0\right)n_1 + \left(x_3 + \frac{1}{2}x_2 + \frac{1}{4}x_1 + \frac{1}{8}x_0\right)n_0\right)\right]$$

A continuación se puede notar que los operadores numéricos y Hadamard para un solo qubit obedecen la relación:

$$\exp(i\pi x n)H|0\rangle = H|x\rangle$$

El efecto de los cuatro términos en el exponente que no contienen factores 1/2, 1/4 o 1/8 es producir la generalización de la expresión anterior a varios qubits:

$$\begin{aligned}
&\exp[i\pi(x_0 n_3 + x_1 n_2 + x_2 n_1 + x_3 n_0)]H_3 H_2 H_1 H_0 |0\rangle|0\rangle|0\rangle|0\rangle \\
&= [\exp(i\pi x_0 n_3)H_3][\exp(i\pi x_1 n_2)H_2][\exp(i\pi x_2 n_1)H_1][\exp(i\pi x_3 n_0)H_0]|0\rangle|0\rangle|0\rangle|0\rangle \\
&= H_3 H_2 H_1 H_0 |x_0\rangle|x_1\rangle|x_2\rangle|x_3\rangle
\end{aligned}$$

Los seis términos restantes en el exponente (que contienen coeficientes fraccionarios) convierten $\mathbf{U}_{\mathrm{FT}}$ a la forma:

$$\begin{aligned}
&U_{FT}|x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle = \\
&\exp\left[i\pi\left(\frac{1}{2}x_0 n_2 + \left(\frac{1}{2}x_1 + \frac{1}{4}x_0\right)n_1 + \left(\frac{1}{2}x_2 + \frac{1}{4}x_1 + \frac{1}{8}x_0\right)n_0\right)\right]H_3 H_2 H_1 H_0 |x_0\rangle|x_1\rangle|x_2\rangle|x_3\rangle
\end{aligned}$$

El estado $|x_0\rangle|x_1\rangle|x_2\rangle|x_3\rangle$ es un estado propio de los operadores numéricos $\mathbf{n}_3$, $\mathbf{n}_2$, $\mathbf{n}_1$, $\mathbf{n}_0$ con los respectivos valores propios x_0, x_1, x_2, x_3. Por tanto es posible reemplazar cada x_i por el operador numérico $\mathbf{n}_{3\text{-}i}$ de cuál es el valor propio para obtener:

$$U_{FT}|x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle = H_3 \exp\left[i\pi\frac{1}{2}n_2n_3\right]H_2 \exp\left[i\pi n_1\left(\frac{1}{2}n_2+\frac{1}{4}n_3\right)\right]$$
$$\times H_1 \exp\left[i\pi n_0\left(\frac{1}{2}n_1+\frac{1}{4}n_2+\frac{1}{8}n_3\right)\right]$$
$$\times H_0|x_0\rangle|x_1\rangle|x_2\rangle|x_3\rangle$$

Si se define el operador unitario de 2 qubits:

$$V_{ij} = \exp\left(i\pi n_i n_j / 2^{|i-j|}\right)$$

Entonces $\mathbf{U}_{FT}$ asume la forma más legible:

$$U_{FT}|x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle = H_3(V_{32}H_2)(V_{31}V_{21}H_1)(V_{30}V_{20}V_{10}H_0)|x_0\rangle|x_1\rangle|x_2\rangle|x_3\rangle$$

Los paréntesis solamente se utilizan para guiar al ojo hacia la estructura, cuya generalización para más de 4 bits es obvia.

Si se define el operador unitario **P** de manera que retorne la permutación de los estados de la base computacional:

$$P|x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle = |x_0\rangle|x_1\rangle|x_2\rangle|x_3\rangle$$

Entonces $\mathbf{U}_{FT}$ se convierte en:

$$U_{FT}|x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle = H_3(V_{32}H_2)(V_{31}V_{21}H_1)(V_{30}V_{20}V_{10}H_0)P|x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle$$

Esta forma expresa $\mathbf{U}_{FT}$ como un producto de operadores unitarios, estableciendo por tanto independientemente que $\mathbf{U}_{FT}$ es unitaria. Más importante, provee una construcción explícita de $\mathbf{U}_{FT}$ a partir de puertas unitarias de 1 y 2 qubits, cuyo número crece solo cuadráticamente con el número *n* de qubits. (La permutación P puede ser construida a partir de puertas cNOT y un qubit adicional, inicialmente en el estado $|0\rangle$).

2.8.6. Encontrar el periodo

El periodo *r* de *f* aparece en el estado $|\Psi\rangle_n = \frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}|x_0+kr\rangle_n$ de los qubits del registro de entrada producido por una sola aplicación de $\mathbf{U}_f$. Para obtener información útil sobre *r* se aplica la transformación de Fourier cuántica $U_{FT}|x\rangle_n = \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}e^{2\pi ixy/2^n}|y\rangle_n$ al registro de entrada:

$$U_{FT}\frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}\left|x_0+kr\right\rangle=\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}\frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}e^{2\pi i(x_0+kr)y/2^n}\left|y\right\rangle_n$$

$$=\sum_{y=0}^{2^n-1}e^{2\pi i x_0 y/2^n}\frac{1}{\sqrt{2^n m}}\left(\sum_{k=0}^{m-1}e^{2\pi i kry/2^n}\right)\left|y\right\rangle_n$$

Si ahora se realiza una medición, la probabilidad $p(y)$ de obtener el resultado *y* es precisamente la magnitud al cuadrado del coeficiente de $\left|y\right\rangle$. El factor $e^{2\pi i x_0 y/2^n}$, en el cual el anteriormente problemático x_0 ocurre explícitamente se retira de esta probabilidad y todo lo que queda es:

$$\frac{1}{2^n m}\left|\sum_{k=0}^{m-1}e^{2\pi i kry/2^n}\right|^2$$

Esto completa la parte cuántica del proceso, excepto que, como se notó anteriormente, se podría tener que repetir el proceso una pequeña cantidad de veces (en el orden de 10 aproximadamente) para obtener una alta probabilidad de conocer el periodo *r*. Para ver porque la forma de $p(y)$ hace que esto sea posible se requiere mayor análisis puramente matemático, lo cual en un cierto punto explotará otra rama la teoría numérica elemental. En realidad la probabilidad es al menos 0.4 de que el valor medido de *y* sea tan cercano cómo es posible a – con diferencia de 0.5 – a un múltiplo entero de $2^n/r$.

2.8.7. Calculo de la función periódica

Se ha asumido la existencia de una subrutina eficiente que calcule $b^x \bmod(N)$. Se puede pensar que calcular $f(x)=b^x \bmod(N)$ para valores arbitrarios de *x* menores que, por ejemplo, $2^n=10^{800}$ requeriría un número astronómico de multiplicaciones, pero no es así. Simplemente se eleva al cuadrado $b \bmod(N)$, se eleva al cuadrado el resultado $\bmod(N)$, se eleva al cuadrado eso, etc., calculando el comparativamente menor número de potencias $b^{2^j} \bmod(N)$ con j<n. La expansión binaria de $x = x_{n-1}x_{n-2}\ldots x_1x_0$ dicta cuáles de ellos deben ser multiplicados para obtener $b^x = \prod_j \left(b^{2^j}\right)^{x_j}$.

De manera que si se empieza con x en registro de entrada, 1 (000…001) en el registro de salida y b en un registro de trabajo adicional, se puede proceder de la manera siguiente:

(a) Multiplicar el registro de salida por el registro de trabajo si y solo si x_0=1;

(b) Reemplazar el contenido del registro de trabajo por su cuadrado módulo N;

(a') repetir (a) con la multiplicación ahora condicional sobre x_1=1;

(b') repetir (b);

(a´´) repetir (a) con la multiplicación ahora condicional sobre x_2=1; etc.

Al final de este proceso todavía se tendrá *x* en el registro de entrada (el cual sirve solamente como registro de control para las *n* multiplicaciones controladas), y se tendrá $b^x \bmod(N)$ en el registro de salida. El registro de trabajo contendrá b^{2n} sin importar el valor de *x* en el registro de entrada, y por tanto no estará entrelazado con los registros de entrada y salida.

Es destacable la diferencia entre los estilos de programación clásico y cuántico. En un computador clásico se tendría una tabla de búsqueda de todos los *n* módulo N múltiplos cuadrados de *b*, dado que los bits son baratos y estables y de otra forma obtener todos los $b^x \bmod(N)$ para todos los valores necesarios de *x* requeriría recalcular los sucesivos cuadrados tantas veces que se volvería ridículamente ineficiente. Pero la situación es bastante opuesta con un computador cuántico, dado que los qubits son caros y frágiles y el paralelismo cuántico hace posible producir el estado $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n|f(x)\rangle_{n_0}$ con una sola ejecución del procedimiento que realiza los sucesivos cuadrados.

Como es usual, el truco es que una medición inmediata sobre los qubits en dicho estado puede revelar solo el valor de una de las potencias módulo *N* de *b*. Pero al aplicar $\mathbf{U}_{FT}$ al registro de entrada del estado y solo entonces realizar la medición, se puede obtener importante información colectiva acerca de los valores módulo N de b^x – en este caso un divisor del crucial periodo *r* – a costa del precio de perder toda la información de los valores individuales de b^x.

2.8.8. Búsqueda del Periodo y Factorización

Si se cuenta con una manera de determinar periodos (como el algoritmo de Shor) y se desea encontrar los factores primos de $N = pq$, se debe escoger un número aleatorio *a* coprimo(su m.c.d. es 1) con *N*. La probabilidad de que un número aleatorio *a* sea un múltiplo de *p* o de *q* es minúscula cuando *p* y *q* son muy grandes. Si ese fuera el caso, el algoritmo de Euclides aplicado a *a* y *N* obtendría *p* y *q* directamente.

Utilizando la rutina de búsqueda de periodo, se encuentra el orden de *a* en G_{pq}: el menor entero *r* para el cual:

$$a^r \equiv 1 (\text{mod } pq)$$

Se puede encontrar esta información para factorizar *N* si la elección de *a* fue acertada en dos formas.

Primero se debe obtener un r que es par. Con lo cual se puede calcular:

$$x = a^{r/2} (\text{mod } pq)$$

Y se puede notar que:

$$0 \equiv x^2 - 1 \equiv (x-1)(x+1) (\text{mod } pq)$$

Ahora $x-1 = a^{r/2} - 1$ no es congruente con 0 módulo pq, dado que *r* es la potencia de *a* más pequeña congruente con 1. Suponiendo que a fue tan acertado que:

$$x+1 = a^{r/2} + 1 \neq 0 (\text{mod } pq)$$

En tal caso ni $x-1$ ni $x+1$ son divisibles por $N = pq$, pero su producto si lo es. Dado que *p* y *q* son primos, esto es posible solo si uno de ellos, por ejemplo *p*, divide $x-1$ y el otro, *q*, divide $x+1$. Dado que los únicos divisores de N son *p* y *q*, se deduce que p es el máximo común divisor de *N* y $x-1$, y que q es el máximo común divisor de *N* y $x+1$. Es posible encontrar entonces *p* y *q* por una aplicación directa del algoritmo de Euclides.
De manera que todo se resume a la suerte. La probabilidad es la menos 0.5 de que un número aleatorio *a* en G_{pq} tenga un orden *r* par con $a^{r/2} \neq -1 (\text{mod } pq)$. Así que no se debe repetir el procedimiento una gran cantidad de veces para alcanzar una alta probabilidad de éxito.

2.8.9. Ejemplo de aplicación del Algoritmo de Shor

Dado el número 21 el objetivo es obtener sus factores mediante el Algoritmo de Shor.

(1) Se toma una base aleatoria menor al número a factorizar y mayor a 1. Para el efecto del ejemplo se utilizará como base el número 2.

(2) Ahora se empiezan a obtener los exponentes de la base utilizando la función:

$$f(x) \equiv 2^x \text{ mod}(21)$$

exp	$f(x)$
0	1
1	2
2	4
3	8
4	16
5	11
6	1

(3) Al obtener un valor de función iguala a 1 o un valor de función previamente obtenido (repetido), se detiene el cálculo de la función.

(4) En el caso de que el exponente sea un múltiplo de 2, se procede a factorizar la función. De lo contrario se repiten los pasos (1) a (4) hasta agotar las bases u obtener los factores.

$$2^6 \equiv 1 \bmod(21)$$
$$2^6 - 1 \equiv 0 \bmod(21)$$
$$\left(2^3\right)^2 - 1^2 \equiv 0 \bmod(21)$$
$$\left(2^3 - 1\right)\left(2^3 + 1\right) \equiv 0 \bmod(21)$$
$$\left(2^3 - 1\right) \equiv 0 \bmod(21) \quad \left(2^3 + 1\right) \equiv 0 \bmod(21)$$
$$(8 - 1) \equiv 0 \bmod(21) \quad (8 + 1) \equiv 0 \bmod(21)$$
$$7 \equiv 0 \bmod(21) \quad 9 \equiv 0 \bmod(21)$$

(5) Para cada uno de los números obtenidos se calcula el Máximo Común Divisor entre el factor y el número a factorizar.

MCD(7, 21) = 7

MCD(9, 21) = 3

(6) De esta manera se obtiene los factores, en caso de obtener un MCD trivial como la unidad (1) o el mismo número a factorizar (21) se procede a ejecutar el algoritmo con una nueva base.

2.9. Decoherencia

En un computador cuántico los sistemas físicos que codifican los bits lógicos individuales no deben tener interacciones físicas fuera del completo control del programa. Cualquier otra interacción, por irrelevante que pudiera parecer en un computador clásico, introduce trastornos potencialmente catastróficos en la operación de un computador cuántico. Tales encuentros pueden incluir interacciones con el ambiente externo, como moléculas de aire rebotando contra los sistemas físicos que representan los bits, o la absorción de diminutas cantidades de energía térmica radiante en el ambiente. Pueden incluso existir interacciones destructivas entre las características relevantes para el proceso computacional de los sistemas físicos que representan los bits y otras características de los mismos sistemas asociadas con aspectos irrelevantes de su estructura interna. Tales interacciones destructivas entre lo que importa para el proceso computacional y lo que no, resultan en decoherencia, la cual es fatal para un computador cuántico.

Para evitar la decoherencia, bits individuales no pueden en general estar codificados en sistemas físicos de tamaño macroscópico, ya que tales sistemas (excepto bajo circunstancias muy especiales) no pueden ser aislados de sus propias propiedades internas irrelevantes. Tal aislamiento puede ser alcanzado si los bits se codifican con un pequeño número de estados de un sistema de tamaño atómico, donde las características internas extra no sean relevantes, sea porque no existen o porque requieren grandes energías no disponibles para entrar en juego. Tales sistemas de escala atómica, deben ser desacoplados de su entorno excepto por las interacciones completamente controladas que se asocian con el proceso computacional en sí.

Dos cosas evitan que la situación no tenga salida. Primero, la separación entre los niveles de energía discreta de un sistema en escala atómica puede ser mucho mayor que la separación entre los niveles de un sistema más grande, el aislamiento dinámico de un sistema atómico es más fácil de alcanzar. Se necesita de un golpe substancial para sacar a un átomo de su estado de más baja energía. La segunda razón se debe al descubrimiento de que los errores inducidos por interacciones externas pueden ser corregidos si ocurren a una tasa suficientemente baja. Mientras que la corrección de errores es rutinaria para bits representados por sistemas clásicos, la corrección de errores cuánticos está sujeta al formidable requerimiento de que debe ser realizada sin conocer el estado original o el estado

corrupto de los sistemas físicos que representan los bits. Contradiciendo a la lógica, esto resulta ser posible.

2.9.1 Corrección de errores cuánticos

Ya que la implementación de la más simple puerta lógica es experimentalmente difícil, pronto fue reconocido que las técnicas de corrección de error podrían jugar un rol importante en un computador cuántico funcional. Prometedores estudios realizados por Shor[38] y Steane[39] sugirieron una metodología, y una teoría de corrección de errores cuánticos fue pronto puesta en marcha. Todos estos algoritmos se basan en el problema de la decoherencia.

La realización física de un computador cuántico es un problema por demás interesante, pero difícil. Solo hace unos pocos años atrás, varias dudas fueron expresadas acerca de la capacidad de llevarlo a cabo. El problema es que una transformación unitaria arbitraria solo puede ser realizada con una cierta precisión. Además de ello, un sistema de spines o un sistema cuántico similar no pueden ser completamente protegidos de los disturbios en el ambiente que los rodea. Todo esto lleva a errores que se acumulan en el proceso computacional. En $L \approx \delta^{-1}$ pasos (donde δ es la precisión de cada transformación unitaria) la probabilidad de un error estará en el orden de 1, lo cual hace al proceso inútil. En parte esta dificultad puede ser resuelta utilizados códigos de corrección de errores cuánticos. El resultado final de ellos es que existe un valor límite δ_0 tal que para una precisión $\delta < \delta_0$ cálculos computaciones cuánticos arbitrariamente grandes son posibles. Sin embargo para $\delta > \delta_0$ los errores se acumulan más rápido de lo que pueden ser corregidos exitosamente. De acuerdo a varios estimados, δ_0 está en el intervalo entre 10^{-6} y 10^{-2} (el valor exacto depende del carácter de los disturbios y el circuito que es utilizado para la corrección del error).

38 "Esquema para reducir la decoherencia en la memoria de computadores cuánticos" por Peter Shor.
39 "Códigos de corrección de error en la teoría cuántica" por A. M. Steane

CAPÍTULO III

3. SIMULADOR

3.1. Teoría del caos aplicada al desarrollo de software

3.1.1 Conceptos de teoría del caos

La teoría del caos es una de las ciencias más jóvenes, sus orígenes se sitúan en la década de los setentas, y desde entonces se ha transformado en uno de los campos de investigación más fascinantes de hoy en día.

Entre sus aplicaciones se encuentran el control de arritmias en los marcapasos, la compresión de imagen y sonido, la dinámica de fluidos y la física de estado sólido.[40]

Contrario a lo que se pueda suponer, en el corazón de la teoría del caos se encuentra la esencia del orden. A pesar de que un concepto fundamental de la teoría es que diminutos cambios a un sistema producen resultados gigantescos, es posible modelar su conducta global aun cuando no se pueda predecir exactamente el estado futuro del sistema.

Cualquier sistema que no sea perfectamente aleatorio, puede ser caótico. Técnicas como la iteración y la recursión son fundamentales para la teoría del caos, de forma que sin un computador sería imposible explorar conductas propias de esta teoría.

A pesar de la creencia de que el universo funciona con la exactitud de un reloj y que las pequeñas turbulencias dentro de él son efectos secundarios solamente, las investigaciones en biología y física demuestran que gran parte de los sistemas son discontinuos, no homogéneos e irregulares. De manera que en realidad es más común encontrar fases pequeñas y aisladas de orden en medio del caos que viceversa.

El caos es efectivamente una conducta impredecible a largo plazo que surge de un sistema dinámico determinista. Aunque estos sistemas son perfectamente predecibles en el corto plazo dado un conocimiento perfecto de las condiciones iniciales, la impredictibilidad a corto plazo radica en la sensibilidad del problema a las condiciones iniciales.[41]

De manera que para que un sistema se considere caótico debe tener un gran conjunto de condiciones iniciales, altamente inestables, las cuales sin importar con que precisión sean

[40] J. Marcoff, Elements of Chaos in Computer Behavior, New York Times, 1988.
[41] M. Berry, Dynamical Chaos, Princeton University Press, 1987

medidas causarán que la predicción de su futuro sea radicalmente errónea luego de poco tiempo. Es decir, existe un *Horizonte de Predictibilidad* en el problema sin importar el conocimiento de las condiciones iniciales.

Los requerimientos que debe tener un sistema para ser aplicable a la teoría del caos son:

- Constituir un sistema, es decir un conjunto de entidades integradas entre sí para cumplir una función concreta.
- Ser un sistema no lineal, aquel que exhibe una desviación de toda correspondencia funcional de proporcionalidad directa.
- Ser un sistema complejo, aquel compuesto por muchas partes.
- Ser un sistema dinámico, implica un cambio de estado en el sistema causado por la influencia de fuerzas, generalmente ajenas al mismo.

3.1.2 Conceptos de desarrollo de software aplicables

Los siguientes conceptos propios de la teoría del caos son aplicables al desarrollo de software y forman la parte constituyente de esta metodología de desarrollo:

(1) Utilización de iteraciones y recursividad para la solución de problemas y la evolución del sistema.

(2) Un proyecto consiste de muchos niveles interrelacionados de resolución de problemas, el comportamiento de un sistema complejo emerge de la interacción de estos pequeños bloques de construcción.

(3) Al igual que un fractal, todas las fases del ciclo de desarrollo de software ocurren dentro de cada fase en sí, por ejemplo dentro de la fase de implementación se encuentra una pequeña fase de diseño donde el desarrollador considera el nombre apropiado de las variables y las validaciones adecuadas, así como pequeñas pruebas unitarias por cada método.

(4) Una regla dentro de la teoría del caos es resolver el problema más importante en el momento actual primero, una práctica muy común en desarrollo ágil de sistemas en la actualidad.

(5) Pequeñas variaciones en los requerimientos pueden impactar el tiempo de desarrollo del sistema de forma considerable.

(6) En un proyecto complejo de software es imposible determinar con exactitud resultados como el tiempo preciso de desarrollo y la calidad del producto obtenido, de manera que iterativamente se va creando un producto y en cada fase se realizan ajustes y evaluaciones de tareas a completar en la siguiente fase, un principio común de la metodología Scrum.

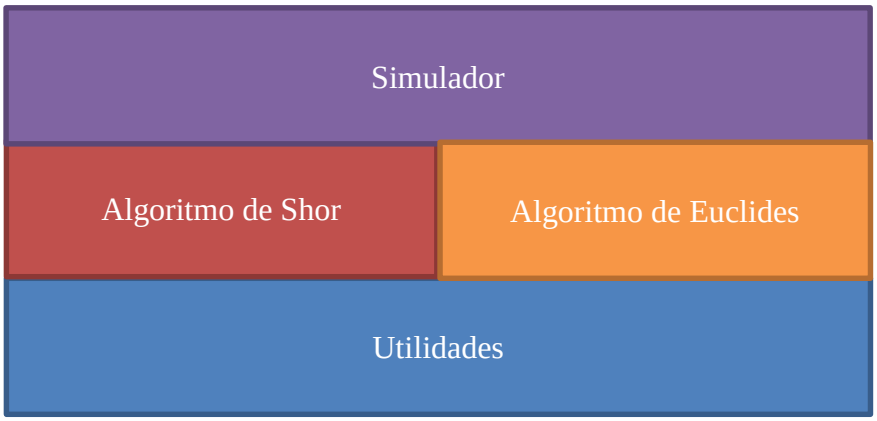
3.2. Desarrollo del simulador

3.2.1 Diseño

Se aplica el principio (2) de la metodología empleada, dividiendo el sistema en pequeños componentes, los cuales interactúan entre sí para producir el resultado deseado.

Los componentes a desarrollar y su funcionalidad es la siguiente:

- Algoritmo de Shor: principal componente de la solución, representa los valores sobre los cuales se va a calcular y el estado actual de dicho proceso.
- Algoritmo de Euclides: es un algoritmo secundario utilizado por el Algoritmo de Shor para obtener el Máximo Común Divisor de dos números.
- Utilidades: métodos y clases auxiliares que proporcionan valores o funcionalidad común a los demás componentes.
- Simulador: Componente gráfico que maneja la interacción con el usuario y realiza las llamadas a los componentes correspondientes a fin de obtener el resultado del procesamiento.



El resultado es un diagrama de componentes a implementar.

3.2.2 Implementación

Se aplican los principios (1), (3) y (4) de la metodología empleada, empezando por el componente más importante y añadiendo poco a poco las funcionalidades necesarias para el procesamiento de los datos, en cada componente se realiza un pequeño diseño y ajuste de la funcionalidad, se utiliza iteraciones y recursividad cuando es necesario.

Los siguientes son los pasos en orden ejecutados durante la implementación de la solución:

- Creación de la solución
- Creación del proyecto Windows Form correspondiente al simulador
    - Incluir los controles para ingresar el número a procesar
- Creación del proyecto Class Library del Algoritmo de Shor
    - Creación de las propiedades para almacenar el número a procesar y la lista de bases
- Creación del proyecto Class Library para las Utilidades
    - Creación de la función para obtener una lista de bases aleatoria
- Pruebas para verificar el método que obtiene la lista aleatoria de bases
- Creación del método para validar si existen bases a procesar
- Llamar a los métodos de validación de bases desde el Simulador
- Incluir validaciones del rango de números a procesar en el Simulador
    - Creación del mensaje de error
- Creación del método para procesar cada base utilizando iteraciones
- Creación del método para escribir los resultados del proceso en una caja de texto
    - Incluir el control correspondiente en el Simulador
- Creación del método para generar la tabla base en el Algoritmo de Shor
    - Creación de las propiedades para almacenar la tabla y el periodo
    - Utilizar iteraciones para procesar la función hasta obtener una condición de parada de acuerdo al algoritmo
    - Calcular el periodo en base a la última ocurrencia
    - Escribir la tabla a la caja de texto
    - Prueba para verificar la generación de la tabla y el periodo

- Validación del periodo en el Simulador
    - Escribir los mensajes correspondientes en caso de no encontrar un periodo válido.
- Creación del método para obtener las raíces en el Algoritmo de Shor
    - Creación de las propiedades para almacenar las raíces
    - Escribir las raíces
    - Pruebas para verificar la generación de las raíces
- Creación del método para obtener el MCD para cada raíz
- Creación del proyecto Class Library del Algoritmo de Euclides
    - Creación de las propiedades para almacenar del número a procesar y del MCD
    - Creación de la propiedad para almacenar los pasos del algoritmo como texto
    - Método recursivo para el cálculo del MCD
- Creación de las propiedades en el Algoritmo de Shor para almacenar el MCD
    - Llamar al Algoritmo de Euclides para generar al MCD y almacenar el resultado en la propiedades creadas
- Validación en el Simulador de los factores obtenidos, al menos uno de los factores no debe ser trivial de acuerdo al algoritmo.
    - Imprimir los resultados
- Pruebas integrales de funcionamiento del Simulador
- Corrección de errores
    - Error en condición de para del método recursivo del Algoritmo de Euclides para obtener el MCD
- Reestructurar la función de escritura a la cada de texto
- Crear varias cajas de texto para organizar los datos obtenidos por el algoritmo
- Ejecutar de manera asíncrona el procesamiento de cada base
    - Pruebas para verificar el funcionamiento correcto
- Incluir un delay en el procesamiento de cada base para mejor visualización
    - Crear el control de intervalo de espera en el Simulador
- Reestructuración del proyecto en carpetas dentro del Sistema Operativo
- Creación de la pantalla de presentación (Splashscreen)

- Diseño gráfico del Simulador
    - Reorganización de las cajas de texto
    - Inclusión de las secciones del simulador en grupos con título
    - Pruebas para determinar la fuente adecuada y el tamaño del formulario
    - Marcar las cajas de texto como solo lectura
- Pruebas finales

3.2.3 Pruebas

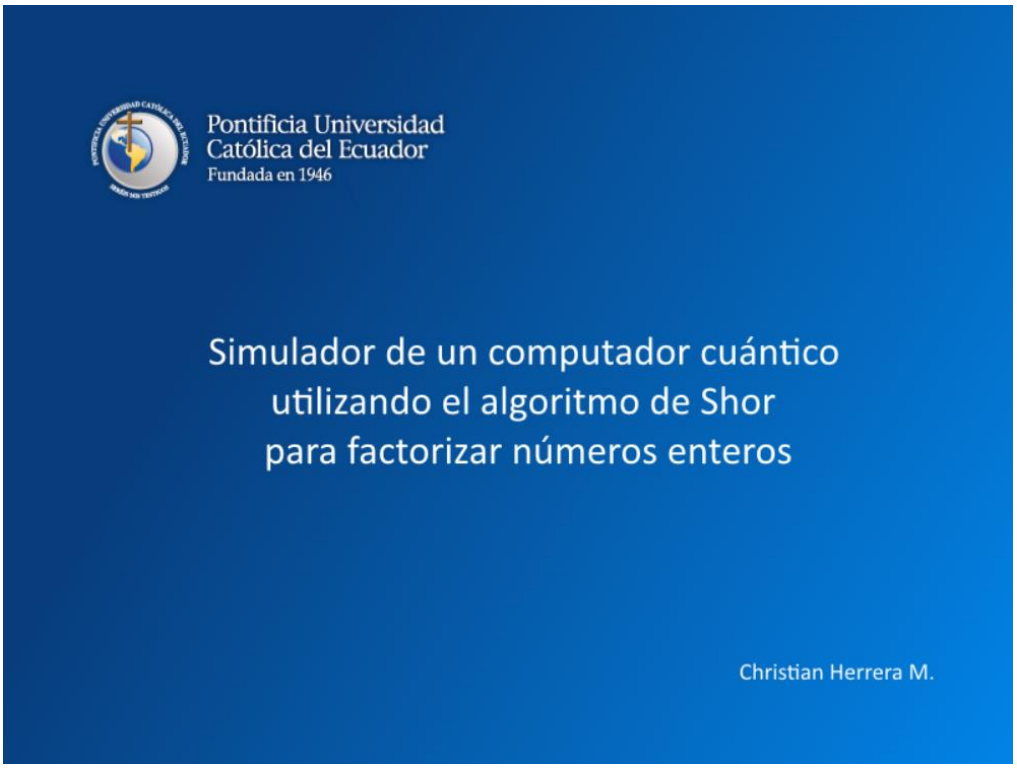
A lo largo de la implementación se ejecutaron las siguientes pruebas:

- Verificación del número mínimo y máximo a procesar
- Verificación de utilizar un número entero
- Verificación de funcionamiento asíncrono
- Verificación de delay entre ejecuciones de procesamiento por cada base
- Verificación de resultados obtenidos por el algoritmo
- Verificación de valores correctos en la tabla
- Ejecución paso a paso del simulador
- Procesamiento con varios casos de prueba
    - Número mínimo a procesar
    - Número primo
    - Producto de dos primos
    - Productos de más de dos factores

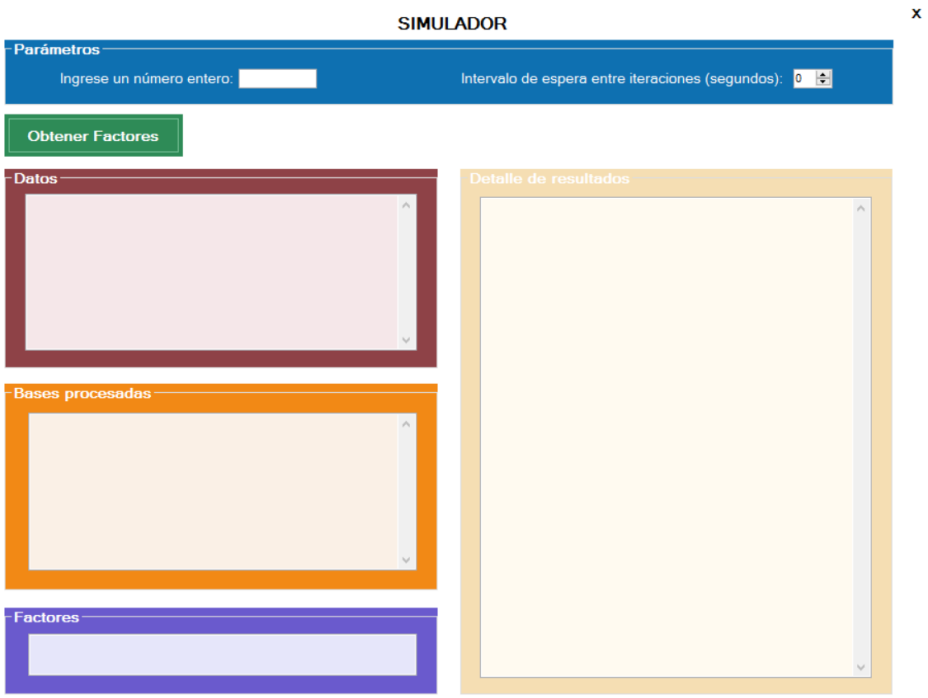
3.3. Manual de usuario

Para ejecutar el Simulador se debe ejecutar el archivo: Simulador.exe

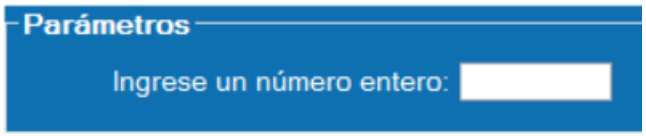
Se mostrará la pantalla de presentación:



Luego de un corto periodo de tiempo se mostrará la pantalla principal del Simulador:

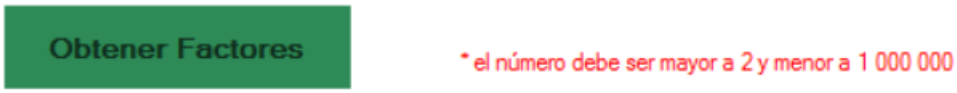


El usuario debe ingresa un número entero del cual se desean obtener los factores:



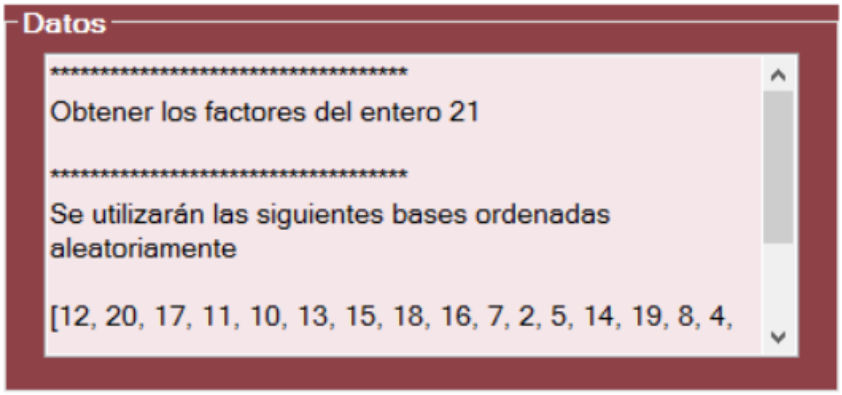
Para procesar se debe hacer click sobre el botón de Obtener Factores:

En caso de presentarse un error, este se mostrará junto al botón anterior:



Los resultados se muestran en las cajas de texto correspondientes

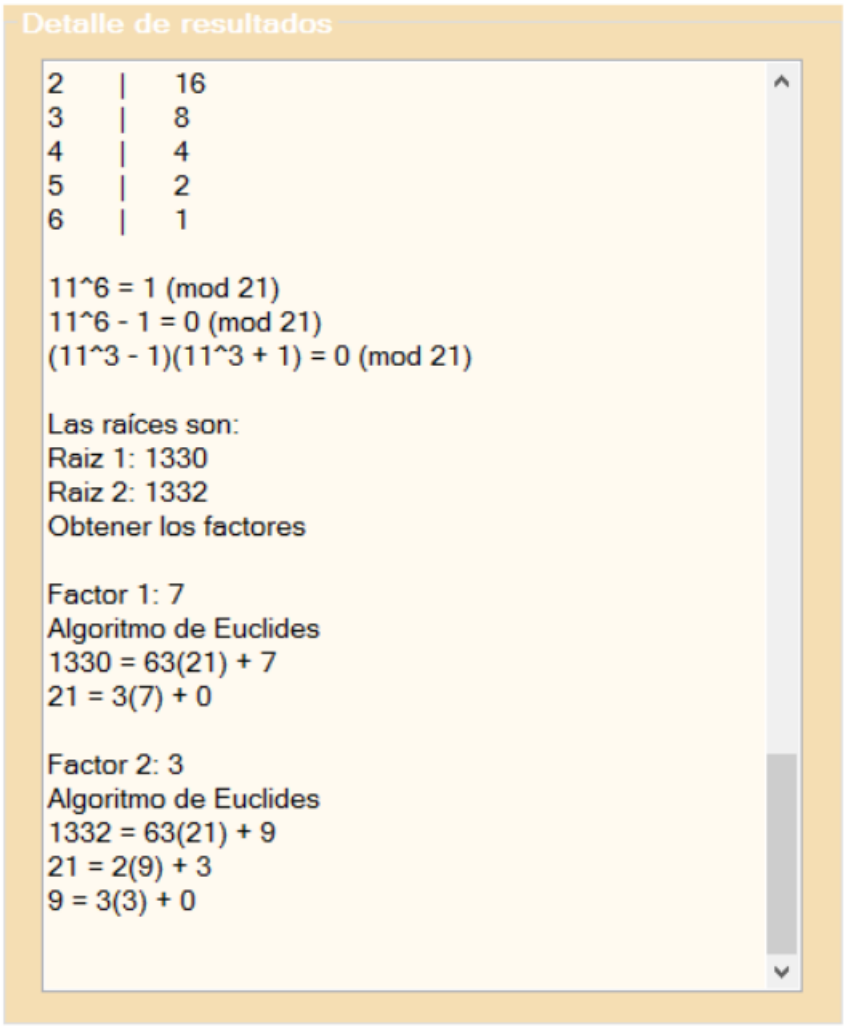
En la sección de Datos se muestra el número a procesar y la lista de bases en el orden aleatorio que se utilizarán al ejecutar el Algoritmo de Shor:



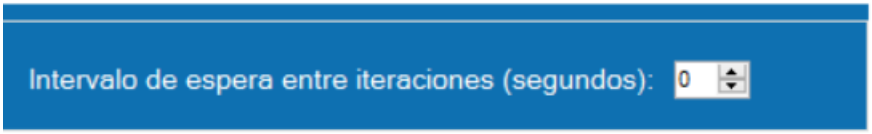
En la sección de Bases Procesadas se muestra cada base en el orden en el que fue procesada, este control se actualiza de manera asíncrona cada vez que una nueva base es procesada:

En la sección de Factores se muestra el resultado de la ejecución del Algoritmo de Shor, en caso de que no se encuentren factores, también se mostrará el mensaje correspondiente:

En la sección de Detalle de Resultados se muestran los pasos completos de la ejecución del Algoritmo de Shor por cada base procesada:



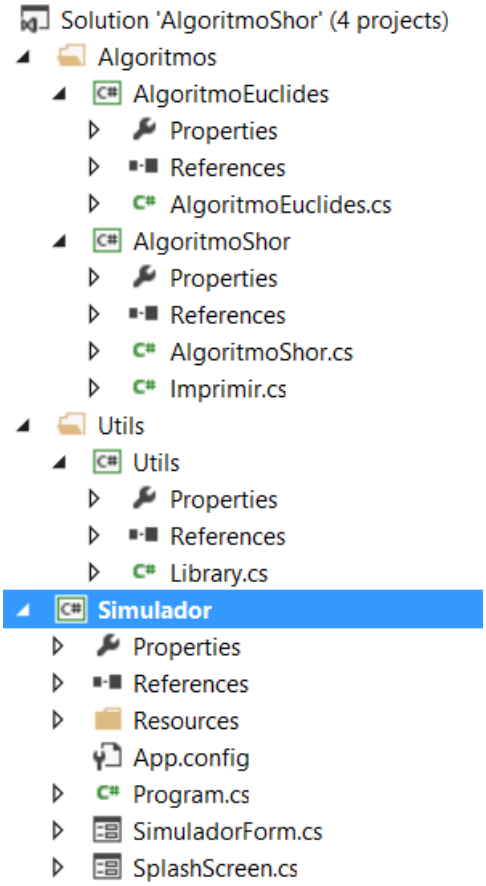
Ya que cada base se procesa de manera asíncrona, es posible introducir un intervalo de entre 0 y 5 segundos de espera de manera que se puedan observar los resultados con mayor detenimiento:



Para salir del programa se debe hacer click en el ícono correspondiente en la esquina superior derecha:

3.3. Manual técnico

La solución está organizada en 4 proyectos, donde los Algoritmos están agrupados en la carpeta correspondiente:



El proyecto de inicio es la aplicación Windows Forms llamada Simulador, la cual contiene dos formularios, el de presentación y el simulador como tal.

El Simulador consta de los siguientes métodos:

- Evento para el botón de Obtener Factores, el cual valida el número entero a procesar
- ProcesarNumero se encarga de validar el rango del entero, crear el objeto correspondiente al Algoritmo de Shor y llamar al siguiente método
- BuscarFactores se encarga de procesar cada una de las base iterativamente llamando al siguiente método asíncronamente

- ProcesarBase se encarga de ejecutar en un hilo diferente los métodos del Algoritmo de Shor para generar la tabla base, obtener las raíces y el mcd de cada una de ellas.
- Métodos de escritura para enviar los resultados a las cajas de texto correspondientes para la visualización del usuario.

El Algoritmo de Shor consta de los siguientes métodos:

- ExisteBase para validar si hay una base actual generada sobre la cual trabajar
- GenerarTablaBase se encarga de obtener los valores de la función del algoritmo y almacenarlos en una tabla local y de obtener el periodo
- ObtenerRaices se encarga de calcular la raíces en base al periodo
- ObtenerMCD se encarga de llamar al Algoritmo de Shor para obtener el MCD de cada raíz

El Algoritmo de Euclides consta de los siguientes métodos:

- ObtenerMCD se encarga de llamar al método recursivo para obtener el MCD
- RecursivoMCD es el método que obtiene el MCD de manera recursiva

Las Utilidades constan de los siguientes métodos:

- ObtenerListaDesordenada se encarga de generar una lista de valores aleatorios menores al parámetro enviado.

CAPÍTULO IV

4. CONCLUSIONES

Es posible desarrollar un simulador de un computador cuántico que utilice el Algoritmo de Shor para factorizar número enteros de manera eficiente, haciendo uso de los conceptos matemáticos en los cuales se basa dicho algoritmo y principalmente buscando la obtención del periodo mediante aritmética modular. Las complicaciones para realizar cálculos con enteros de grandes dimensiones que requiere el algoritmo son reducidas debido a la implementación en lenguajes de alto nivel de clases que representan números enteros con varios dígitos, limitados solamente por la memoria del computador.

El Algoritmo de Shor fue la motivación principal para emprender la construcción de un computador cuántico funcional más allá de la teoría matemática, su importancia en este nuevo campo de la ciencia es vital ya que de llegar a desarrollarse un computador cuántico, las implicaciones de ejecutar el algoritmo y obtener resultados como romper claves RSA de criptografía tendrían eco en la vida diaria de miles de personas. Se afectaría directamente al comercio electrónico y la comunicación privada lo cual llevaría al mundo a buscar nuevas formas de mantener las transacciones seguras.

A pesar de la gran cantidad de recursos invertidos por varias corporaciones relacionadas con la tecnología como Microsoft y Google, el campo de la computación cuántica todavía se mantiene como uno de los más innovadores y con gran potencial para la investigación y el desarrollo. Grupos de científicos tienen como objetivo desarrollar software que permita simular el procesamiento cuántico como del nuevo lenguaje LIQUi|>, sin embargo la simulación se limita por el momento a números de pocos dígitos, el avance es lento pero constante. De la misma forma existe investigación a nivel de hardware para implementar un computador cuántico, a pesar de que la comunidad se mantiene escéptica con respecto a tecnologías como D-Wave, otros prospectos están encontrando mercado y se abren paso hacia los bienes de consumo como televisores para el caso de puntos cuánticos.

Un computador cuántico es un dispositivo especializado en resolver cierta clase de problemas que tomarían demasiado tiempo en un computador clásico. Es por ello que un computador cuántico no podría reemplazar a un computador clásico, por ejemplo operaciones como el procesamiento de texto no se beneficiarían de las capacidades cuánticas. Sin embargo tal vez el procesamiento gráfico si podría considerarse una aplicación

en un futuro lejano. Lo cierto es que los computadores clásicos no van perder su preponderancia durante varios años, a pesar de que la constante miniaturización de componentes está dejando de obedecer la famosa Ley de Moore.

Las ventajas que provee la computación cuántica no abarcan solamente el procesamiento de complejos algoritmos matemáticos, sino también la capacidad de obtener una criptografía que en verdad no pueda ser violada. El principio de incertidumbre de Heisenberg determina que cualquier interacción con un sistema afecta el estado del sistema, por lo cual la aplicación a la criptografía es también un campo de investigación muy activo. Cabe destacar que constantemente los científicos buscan nuevos algoritmos que sean aplicables a la computación cuántica.

CAPÍTULO V

5. RECOMENDACIONES

Se podría utilizar el recientemente liberado lenguaje de simulación cuántica LIQUi|> de Microsoft para implementar el Algoritmo de Shor, con la limitación de que simular qubits en un computador clásico requiere manejar 2^n estados concurrentes, lo cual limita la capacidad de factorizar números de más allá de unos cuantos bits. Adicionalmente existe la complejidad de manejar miles de compuertas cuánticas y posiblemente mejoras al algoritmo que utilizan matemática avanzada.

También es posible simular al algoritmo de Grover para búsqueda cuántica con la consecuente complejidad matemática y de implementación utilizando un computador clásico.

Una opción más simple sería simular el algoritmo de Simon, que es similar al algoritmo de Shor pero con menor complejidad y posiblemente mejores resultados y rendimiento si se utilizan lenguajes como LIQUi|>.

Es recomendable también simular el procesamiento del computador cuántico D-Wave para resolver el problema para el cual ha sido optimizado, demostrando que un computador clásico puede rivalizar en tiempos de procesamiento.

CAPÍTULO VI

6. BIBLIOGRAFÍA

Benioff Paul, The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines, Journal of Statistical Physics, Volumen 22 - Issue 5, 1980

Deutsch David, Quantum Theory: The Church-Turing Principle and the Universal Quantum Computer, The Royal Society, Volumen 400 - Issue 1818, 1985

Deutsch David, Quantum Computational Networks, Proc. Royal Society London, Volumen 425, 1989

Dirac Paul, The Principles of Quantum Mechanics, Londres, Oxford University Press, 4ta Edición, 1982

Feynman Richard, The Feynman Lectures on Physics, New York, Addison Wesley, 1970

Karkare Manasi, Applied Physics II, Nueva Delhi, I.K. International Publishing House, 2008

Kitaev Yu y otros, Classical and Quantum Computation, Estados Unidos, American Mathematical Society, 2002

Mermin David, Quantum Computer Science: An Introduction, New York, CAMBRIDGE UNIVERSITY PRESS, 2007

Monroy César, Teoría del Caos, México, Alfaomega Grupo Editor S.A., 1997

Nelson Sue y Holligan Richard, Cómo Clonar a la Rubia Perfecta, España, Ediciones Nowtilus, 2004

Pittenger Arthur, An Introduction to Quantum Computing Algorithms, Boston, Birkhauser, 2da edición, 2001

Shor Peter, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal of Computing, No 26, 1997

Varios, Proceedings of the International Conference on Inter Disciplinary Research in Engineering and Technology, Association of Scientists Developers and Faculties, 2da edición, 2015

INTERNET

Deutsch David y Ekert Artur, Machines, Logic and Quantum Physics, http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=9052179&fileId=S1079898600006387, Acceso: 13/12/2015

Gershenfeld Neil y Chuang Isaac L., Quantum Computing with Molecules, http://cba.mit.edu/docs/papers/98.06.sciqc.pdf, Acceso: 13/12/2015

Hassan Mehedi, Microsoft releases its quantum simulator, Liquid, http://microsoft-news.com/microsoft-releases-its-quantum-simulator-liquid/, Acceso: 13/12/2015

Jones Nicola, Google and NASA snap up quantum computer, http://www.nature.com/news/google-and-nasa-snap-up-quantum-computer-1.12999, Acceso: 13/12/2015

Moynihan Tim, What Are Quantum Dots, and Why Do I Want Them in My TV?, http://www.wired.com/2015/01/primer-quantum-dot/, Acceso: 13/12/2015

Simonite Tom, Google Says It Has Proved Its Controversial Quantum Computer Really Works, http://www.technologyreview.com/news/544276/google-says-it-has-proved-its-controversial-quantum-computer-really-works/, Acceso: 13/12/2015

Thompson Clive, The Revolutionary Quantum Computer That May Not Be Quantum at All, http://www.wired.com/2014/05/quantum-computing/, Acceso: 13/12/2015

Varios, A Modern Sequel, http://www.computerhistory.org/babbage/modernsequel/, Acceso: 13/12/2015

Varios, Quantum Dots, http://www.sigmaaldrich.com/materials-science/nanomaterials/quantum-dots.html, Acceso: 13/12/2015

Varios, Language-Integrated Quantum Operations: LIQUi|>, http://research.microsoft.com/en-us/projects/liquid/, Acceso: 13/12/2015

ANEXOS

MECÁNICA CUÁNTICA

La Luz

Las partículas más pequeñas de luz conocidas son los fotones que, a su vez, pueden ser descritas gracias a sus propiedades o estados cuánticos. Entre ellas cabe destacar la forma en que gira o la dirección en que vibra una partícula.

A inicios del siglo XX, los hombres de ciencia sabían muchas cosas acerca de la luz. 200 años antes, Sir Isaac Newton utilizó un prisma de cristal para demostrar que la luz blanca podría descomponerse en distintos colores, así como las gotas de lluvia descomponen la luz y permiten contemplar los siete colores del arco iris.

En aquel entonces había varias teorías acerca de la naturaleza de la luz. Había dos grupos fundamentales, aquellos como Christian Huygens y Robert Hooke pensaban que la luz era una onda y los que, como Newton, creían que la luz estaba compuesta de partículas. En 1801, el erudito inglés Thomas Young realizó un experimento que convenció a la mayor parte de la gente de que, en vez de estar compuesta de partículas, la luz era una onda.

Thomas Young aprendió a leer con dos años y ya en su adolescencia hablaba una docena de lenguas distintas. Fue médico y físico y ayudó a los egiptólogos a descifrar la piedra Rosetta, lo cual permitió que el mundo moderno pudiera descifrar los jeroglíficos.

Sin embargo probablemente se conoce mejor a Young por el siguiente experimento. Proyectó un rayo de luz a través de dos estrechas rendijas produciendo lo que habitualmente se conoce como patrón característico de interferencia, que consiste en una serie de barras de luz y oscuridad proyectadas sobre una pantalla. Al parecer, utilizó dos patos para que le ayudaran a comprender por qué la luz se comportaba de aquella forma. Supuestamente, Young estaba mirando como nadaban los patos cuando cayó en cuenta de que en el momento en que las ondas que producía cada ave se solapaban, creaban una ola más grande, o bien una superficie de agua en calma. Luego aplicó el mismo concepto a la luz, imaginando que la luz viajaba en el aire en forma de ondas.

Cuando los picos de dos ondas de luz coinciden, se combinan para crear un pico más grande, esto es lo que se suele denominar interferencia constructiva. Entonces la onda

luminosa combinada tiene una mayor cantidad de energía y produce una iluminación más brillante. Cuando picos opuestos se cancelan entre sí, la energía queda neutralizada y se produce la oscuridad. Esto es lo que se denomina interferencia destructiva. Parecía que no había otra explicación posible para entender por qué se producía el patrón característico de barras de luz y oscuridad. Por tanto la luz tenía que ser una onda.

Los Cuantos de Plank

Los primeros indicios de que la luz tenía otras propiedades aparecieron cuando el físico alemán Max Plank introdujo el concepto de unidades de energía – denominados cuantos – en 1900. Plank creó los cuantos para poder explicar algo que, en teoría, se suponía que no ocurría.

Al calentar algo, el color de la radiación que emite cambia con la temperatura. Esta es la razón por la cual un atizador en el fuego cambia de color a medida que se calienta. Cuando los científicos trazaron gráficos mostrando la intensidad de la radiación emitida por un cuerpo caliente como una función de su longitud de onda, siempre obtenían una forma similar: una curva que comienza con una intensidad mínima y luego alcanza un pico característico antes de volverse a apagar. De la misma manera, la posición del pico puede desplazarse dependiendo de la temperatura del cuerpo caliente.

La temperatura del sol es de aproximadamente 5800 grados centígrados, y el pico de su curva de radiación a esta temperatura es la parte amarilla del espectro visible. Si el sol se calentara aún más, su pico de radiación se desplazaría teniendo una longitud de onda más corta.

En la física clásica se pensaba que un cuerpo caliente que absorbiera radiación tendría a su vez que irradiar dicha energía (fenómeno conocido como radiación térmica o radiación de cuerpo opaco) a una tasa infinita y de forma equivalente en relación con todas las longitudes de onda. Por tanto la curva clásica para el mismo gráfico comenzaba en un punto muy alto con el punto de máxima radiación situado siempre en la misma región del espectro luminoso: las longitudes de onda ultravioleta. Esta predicción no guardaba relación alguna con la realidad: un atizador al fuego no emite rayos ultravioleta cuando se caliente excesivamente. La incompatibilidad de la teoría con lo que realmente ocurría supuso un gran dilema para los científicos, al punto que la anomalía recibió el nombre de la “catástrofe ultravioleta”.

El físico alemán Max Plank intentaba explicar el misterio de la catástrofe ultravioleta mediante fórmulas matemáticas y sus ecuaciones le permitieron hallar la respuesta correcta, al suponer que la radiación estaba compuesta de pequeñas cantidades de energía o cuantos. En otras palabras, la energía no tenía el carácter fluido y continuo que se creía antiguamente sino que estaba dividida en pequeños paquetes o pedazos. Dichas cantidades debían ser siempre un múltiplo de un cuanto y nunca cantidades intermedias.

Se trataba de una solución de carácter radical y, aún cuando sus idea fueron adoptadas por otros científicos, el mismo Plank nunca se encontró cómodo con la misma. Plank se mostraba reticente a aceptar que los cuantos eran algo más que una herramienta matemática de carácter teórico, pero su fórmula funcionaba y la constante matemática que requería para hacerlo pronto se bautizó como "la constante de Plank" (conocida con la letra H pues la P ya era utilizada).

Cinco años más tarde, en 1905, un científico novato llamando Albert Einstein, descubrió que la misma idea de los cuantos podría explicar el efecto fotoeléctrico. Se trataba de otro rompecabezas científico que no podía explicarse utilizando las leyes clásicas de la física. No obstante el propio Einstein nunca llegó a aceptar del todo las implicaciones últimas de la teoría cuántica.

Si se iluminan con una cierta clase de luz determinados metales, como es el caso del zinc, en un medio en el que se haya practicado el vacío, partículas cargadas negativamente (electrones) saltan de la superficie metálica y se genera una corriente eléctrica. Esto es lo que se denomina efecto fotoeléctrico.

Heinrick Hertz y Aleksandr Stoletov descubrieron conjuntamente este fenómeno a finales del siglo XIX, pero en aquel entonces nadie podía explicar que era lo que estaba ocurriendo. Al parecer el efecto no ocurría con la luz blanca - independientemente de su nivel de intensidad – mientras que la física clásica predecía que si se incrementaba el brillo, o energía, de una onda luminosa, debería incrementarse el nivel de energía de los electrones, lo cual provocaría escape de un mayor número de los mismos.

Por si no resultaba suficientemente extraño, los electrones solo saldrían disparados si la luz que incidía sobre la superficie metálica estaba situada por encima de un determinado umbral de frecuencia, habitualmente situado en el rango ultravioleta. Es más, si la luz ultravioleta se hacía más brillante se obtenían más electrones, pero no resultaban tan rápido ni tenían tanta energía como cuando se atenuaba el nivel de luz ultravioleta.

Albert Einstein, tomando la idea de los cuantos de Plank consideró que la luz estaba formada por partículas individuales, conocidas más tarde como fotones. Si una partícula luminosa choca con un metal, la luz transfiere su energía a un electrón y dicho electrón la absorbe. Si la energía resulta suficiente para superar la energía potencial que mantiene al electrón unido al metal, entonces éste sale despedido. Un electrón solo puede recibir energía procedente de un fotón, lo que explica porque el incremento de intensidad de la luz no producía ninguna diferencia, ya que si no está situada en el rango correcto no se produce efecto alguno.

La explicación del efecto fotoeléctrico y su contribución a la física teórica permitieron que Albert Einstein ganara el premio Nobel en 1921. Si bien la introducción del concepto de los cuantos de Plank no significó el final de la física clásica puso de manifiesto que dicho conocimiento estaba empezando a perder su posición de privilegio como fundamento de todo el conocimiento científico. Así, la física clásica no podía explicarlo todo, particularmente, carecía de respuestas a nivel atómico. Como resultado de todo ello nació una nueva rama de la física que requería una forma de pensamiento totalmente novedosa: la mecánica cuántica.

El átomo en mecánica cuántica

El conocimiento del átomo se ha ido forjando en los últimos cien años. Su nombre deriva de la antigua palabra griega atomon, que significa “aquello que no puede dividirse”, ya que se consideraba que un átomo era el trozo de materia más pequeña que existía, una partícula fundamental que conformaba toda la realidad física circundante. Hubo que esperar hasta 1909 para que los científicos descubrieran que el propio átomo estaba constituido por partículas aún más pequeñas. Luego de que Rutherford propuso su modelo atómico, en el cual fundamentalmente el átomo estaba constituido de espacio vacío y su masa se concentraba en un núcleo central; Niels Bohr decidió combinar la mecánica cuántica y la idea de la energía cuántica de Plank en un modelo en el cual cada electrón tenía una velocidad de rotación que a su vez estaba relacionada con un nivel específico de energía. Dichos electrones necesitaban absorber o emitir una cantidad exacta de energía para escapar de una órbita y saltar a otra.

Si un electrón saltaba de una órbita a otra de menor energía, emitía un fotón y, por el contrario, si un electrón absorbía un fotón que tuviera la cantidad de energía necesaria para

pasar a un nivel de energía superior, entonces lo haría. Bohr fue uno de los científicos responsables de la interpretación de Copenhague acerca de la mecánica cuántica y mantuvo discusiones científicas de alto nivel con Albert Einstein. Fue el propio Bohr quien afirmó lo siguiente: "Todo aquel cuyo primer encuentro con los cuantos no le haya producido una sensación de vértigo, es que no ha entendido ni una sola palabra".

Hoy en día se conoce que dentro del núcleo se encuentran protones y neutrones, fuera del núcleo se hallan los electrones en un estado de movimiento constante. La idea de un átomo indivisible hace mucho tiempo que pasó a la historia. Los electrones tienen un carácter fundamental o indivisible y pertenecen a una familia de partículas llamadas leptones, que también tienen carácter fundamental. No obstante los protones y los neutrones pertenecen a una familia llamada hadrones. Esta clase partículas está a su vez compuesta por partículas más pequeñas llamadas quarks. Existen seis clases de quarks y siempre aparecen en parejas: "up and down" (arriba y abajo), "top and bottom" (cima y fondo) y "strange and charm" (extraño y encantador). El mundo subatómico es un sitio muy curioso y la propia palabra quark tuvo un orígen bastante extravagante. Se trata de una palabra que no tiene sentido alguno inventada por James Joyce y utilizada en su novela Finnegan's Wake.

La naturaleza de la luz

Bohr propuso la idea de que la luz era al mismo tiempo una onda y una partícula y que toda la materia compartía esta misma estructura dual onda-particula. Posteriormente, el científico y aristócrata francés, Louis Victor de Broglie, presentó una fórmula que vinculaba a las partículas con las ondas. Esta ecuación es sorprendentemente simple, como suele ocurrir con las mejores, y relaciona el momento de una partícula (su masa y velocidad) con la longitud de onda asociada a dicha partícula.

Tres años después de esta propuesta, un experimento realizado por el físico americano Arthur Compton confirmó que una partícula individual, el electrón, en realidad tenía propiedades propias de una onda, lo cual constituyó una prueba de que la radiación electromagnética tenía tanto propiedades de onda como de partícula. De manera que tanto Isaac Newton como Thomas Young estaban en lo cierto. La luz es una partícula y una onda.

En 1926, un científico austriaco, Edwin Schrödinger, proporcionó el equivalente matemático del punto de vista enunciado por Bohr: se trataba de un sistema para describir una partícula como una onda. Schrödinger, formuló una ecuación explicando el tipo de onda

que describe el movimiento de una partícula – cualquier partícula – incluyendo el caso de los fotones. Se trata de la llamada función de onda de la partícula y comprendía el estado cuántico de la misma. Y puesto que siempre hay un grado de incertidumbre implicado, esta descripción incluye la probabilidad. Se trata de la probabilidad ya que, de acuerdo con la teoría cuántica, no es posible decir con exactitud donde estará una partícula, sino solamente donde es probable que esté.

La ecuación de ondas de Schrödinger subrayó dos aspectos extraordinarios de la teoría cuántica. La primera, era la noción de incertidumbre, una idea que impresionó enormemente a muchos científicos, entre los cuales estaba Einstein:

"La mecánica cuántica ciertamente se impone" afirmó, "pero una voz interior me dice que no es del todo exacta. La teoría dice mucho pero ciertamente no nos acerca más al conocimiento de lo primigenio. En cualquier caso estoy convencido, de que Dios no juega a los dados".

Asimismo la ecuación de Schrödinger puso de manifiesto una condición poco usual conocida como superposición, según la cual las partículas pueden tener diferentes estados al mismo tiempo. En la misma época en que Schrödinger formuló sus ideas, un físico alemán llamado Werner Heisenberg llegó a conclusiones matemáticas similares. En 1927 el principio de incertidumbre de Heisenberg afirmaba que resulta imposible determinar la velocidad y la posición de una partícula al mismo tiempo. El razonamiento que subyacía a esta conclusión es que al acercarse demasiado a la partícula que se intenta medir, el hecho de la cercanía influye en su comportamiento. Así, la partícula estaría situada en una posición distinta a la que ocupada originalmente o, debido a la interacción del observador, viajaría a una velocidad diferente.

La introducción de la probabilidad, la incertidumbre y la posibilidad de que algo esté en varios sitios de forma simultánea otorga a la teoría cuántica ese aspecto de algo mágico propio de un relato de ciencia ficción. Sin embargo la teoría cuántica ha sido comprobada experimentalmente y hasta el momento, funciona. En cualquier caso para comprenderla basta citar al científico Richard Feynman:

"Pienso que con toda probabilidad nadie entiende la mecánica cuántica. No sigas preguntándote en caso de que puedas ¿Cómo es posible que funcione de esta manera? Ya que te vas a meter en un callejón sin salida del cual nadie a logrado escapar. Nadie sabe como funciona".

El gato de Schrödinger

Schrödinger concibió un famoso experimento mental para demostrar hasta que punto podían resultar extrañas las conclusiones de su ecuación. La idea de Schrödinger era una especie de "mecanismo": un contenedor de gas venenoso, que solo liberaba el gas si un material radioactivo empezaba a caer y producía una radiación. El potencial gas "matagatos" estaba situado en una caja desprovista de orificios que contenía un gato y todo lo que el gato necesitaba para sobrevivir.

La vida del gato dependía de si se liberaba o no un átomo desde el material radioactivo. La teoría cuántica afirma que si no se observa qué es lo que está ocurriendo existe un rango de resultados probables. A esta posibilidad los científicos la llamaron superposición de dos posibilidades o superposición de estados. Esto implica que el átomo puede haber sido liberado, puede haber sido no liberado o bien puede haber sido liberado y no liberado al mismo tiempo. Puesto que la vida del gato depende de este átomo, Schrödinger extendió el concepto al propio gato: si la caja se abre existe un 50% de posibilidades de que el gato esté muerto, un 50% de que esté vivo, pero si la caja permanece cerrada el estado del gato resulta indeterminado. Esta vivo y al mismo tiempo está muerto.

Obviamente, un gato nunca puede estar vivo y muerto en la vida real y esta es la razón por la cual Schrödinger presentó este experimento mental. Las implicaciones de dicho experimento resultaban tan patentemente absurdas que demostraban claramente las falencias lógicas de esta nueva ciencia.

La paradoja EPR

Schrödinger no fue el único científico en poner de manifiesto los resultados aparentemente ilógicos que implicaba la aplicación de la teoría cuántica a las partículas. En 1935, Albert Einstein intentó demostrar que la mecánica cuántica tenía una serie de fallos. Para ello, escribió un artículo junto con Boris Podolsky y Nathan Rosen, intentando encontrar una serie de defectos en la teoría. La clave de la disconformidad de los autores se encuentra en el título ¿Acaso al descripción de Mecánico-Cuántica de la física puede considerarse realmente completa? En su opinión la respuesta era definitivamente no. E intentaron convencer a otros científicos de que estaban en lo cierto.

Einstein, Podolsky y Rosen propusieron un experimento mental basado en la teoría cuántica que, en su opinión, probaba que la teoría cuántica era incorrecta. Afirmaban que si se separaban dos partículas descritas por la misma función de onda, entonces cabía efectuar medidas individuales en relación con cada partícula sin que esto perturbara a la otra. Bajo estas condiciones, el hecho de conocer datos acerca de una partícula, permitiría conocer automáticamente datos acerca de la segunda partícula.

Así por ejemplo, cuando una partícula está en movimiento tiene la propiedad conocida como momento, el cual depende de su masa y su velocidad. Una partícula estacionaría carece de momento, pero si otra partícula choca con ella, entonces se produce una transferencia de momento. Tras la colisión, la cantidad total de momento compartida entre ambas partículas sería igual al momento que tenía la partícula en movimiento antes de la colisión, de acuerdo al principio de conservación del momento. Si se conoce el momento de las dos partículas, luego de separarlas y medir el momento de una partícula, se podrían efectuar los cálculos necesarios para averiguar el momento de la otra.

En otras palabras, el hecho de tomar medidas acerca de una partícula en un sitio dado, proporcionaría información acerca de otra partícula situada en otro sitio. Así, ambas partículas estarían conectadas de alguna manera. Esto va contra el sentido común y, puesto que este fenómeno no ocurre en el mundo real, comenzó a ser conocido como la paradoja EPR. Einstein y sus colegas concluyeron que la existencia teórica de una conexión de esta clase implicaba que la teoría estaba incompleta y debían existir “variables ocultas” que permitirían completarla.

El artículo proporcionó una descripción matemática de dos partículas vinculadas mediante propiedades específicas: posición y momento. Esta condición de conexión se denominó más tarde estado “entrelazado” o par EPR, utilizado las iniciales de Einstein, Podolsky y Rosen. Irónicamente, a pesar de que afirmaban que el entrelazamiento no podía producirse, más tarde se demostró no solo que existía, sino que terminó constituyendo la base de los primeros experimentos de teletransporte.

En la década de los 50 un científico americano, David Bohm, escribió una versión simplificada de artículo de Einstein utilizando el estado del spin en lugar de la posición y el momento. Más tarde, en 1964, un físico irlandés llamado John Bell, logró un gran avance con la paradoja EPR: no se trataba de ninguna paradoja. Bell demostró a través de lo que hoy se conoce como el teorema de Bell, que la no localidad podía ocurrir y que la teoría cuántica estaba en lo cierto. Hasta la década de los 80, nadie pareció dar mucha importancia

al asunto. No obstante en ese momento el científico francés Alain Aspect demostró experimentalmente que, cuando se trata de estas partículas especiales correlacionadas, la mano izquierda sabe exactamente lo que está haciendo la derecha.

En teoría, un par entrelazado de partículas podría crearse y enviarse de forma individual al espacio. Si las propiedades de una partícula fueran medidas posteriormente, la otra partícula quedaría afectada de forma instantánea, de tal manera que adquiriría las propiedades complementarias. Si esto ocurre cuando las partículas están separadas millones de kilómetros, las instrucciones para que esto ocurriera deberían viajar más rápido que la velocidad de la luz y, como decretó Einstein años antes en su teoría de la relatividad especial, nada puede viajar más rápido que la velocidad de la luz.

Teletransportación cuántica

En 1993, seis científicos internacionales, Charles Bennett de IBM, Pilles Brassard y Richard Jozsa de la Universidad de Montreal, Claude Crepeau de la Escuela Normal Superior de Paris, Asher Peres de Instituto Technion de Israel y William Wooters del Williams College de Massachussets, publicaron un artículo describiendo una forma de lograr la teletransportación cuántica sin violar las leyes científicas.

El artículo apareció en Physical Review Letters, la misma revista en la que se había publicado el artículo EPR original casi 60 años antes. Suponiendo que una persona llamada Alice desea enviar a su amigo Bob ciertos datos acerca del estado cuántico de una partícula, Alice tendría una partícula entrelazada y Bob la otra. Si Alice intenta medir alguna característica acerca de su partícula y luego decide compartir esta característica con Bob, éste solo recibiría una copia imperfecta de la partícula original, pues el principio de incertidumbre no permite que cada fragmento de información de la partícula sea medido correctamente. Es más, al momento de realizar la medida, Alice habría alterado el estado de su partícula y la copia de Bob siempre resultaría inexacta.

Para que el teletransporte funcione Alice y Bob deben tener cada uno una partícula entrelazada. Luego Alice entrelaza su partícula – aquella cuyas propiedades quiere transportar – con la partícula previamente entrelazada que comparte con Bob. Entonces Alice ya no puede distinguir entre las dos partículas que tiene, lo cual resulta importante, pues cualquier medición sobre ambas partículas no alterará el estado de su partícula original. La partícula entrelazada de Alice complementará cualquier propiedad de su partícula original.

Y ya que la partícula de Bob debe complementar a la partícula entrelazada de Alice, adquirirá la misma propiedad de la partícula que Alice deseaba transportar.

Alice debe medir sus dos partículas y enviar el resultado a Bob. Este envío se realiza de forma clásica, de manera que el teletransporte no resulta instantáneo y no habría excedido la velocidad de la luz. Pero lo más importante es que el emisor no necesita conocer la localización del receptor. Este concepto provocó una simpática convención entre los científicos que trabajan sobre el campo. A partir de entonces, el emisor de la partícula que debe transportarse siempre se ha llamado Alice y el receptor Bob.

En diciembre de 1997, dos grupos de investigación de la Universidad de Innsbruck en Austria (dirigidos por Antón Zeilinger) y la Universidad de Roma en Italia (dirigidos por Francesco de Martini), informaron acerca de los primeros pasos en el teletransporte, dichos equipos lograron transportar la polarización de de un fotón (la dirección en la que viaja la luz, puede ser horizontal, vertical o un ángulo intermedio).

Los científicos crearon un par entrelazado haciendo pasar un fotón de radiación ultravioleta a través de un cristal no lineal. Esto produjo dos fotones entrelazados de baja energía. Uno de ello fue enviado a Alice, mientras que el otro fue enviado a Bob. El fotón de Alice y uno de los fotones entrelazados fueron posteriormente enviados a un divisor de rayos de tal manera que llegaron ahí al mismo tiempo. El divisor de rayos es el nombre con el cual se denomina a un espejo semiplateado que puede reflejar o transmitir ambos fotones con probabilidad del 50% hacia uno de los dos detectores.

El fotón de Alice no pudo ser identificado, al estar entrelazado con uno de los fotones previamente entrelazados, por tanto, las medidas realizadas en aquel lado no pusieron en cuestión el principio de indeterminación de Heisenberg. El resultado de esta medida se envió a Bob por el conducto clásico así como también a través de la teletransportación cuántica. Todo lo que se sabía acerca de los dos fotones de Alice es que debían tener una polarización complementaria (así por ejemplo, si uno es horizontal, el otro debía ser vertical). Pero esta misma conexión se aplica al fotón que estaba entrelazado con el fotón de Bob, lo cual hizo que el fotón de Bob tuviera la misma polarización que tenía el fotón original de Alice.

En 1998, un equipo compuesto por Akira Furusawa, Chris Fuchs y Jeff Kimble del Instituto de Tecnología de California, Jean Sorensen y Eugene Polzik de la Universidad Aarhus de Dinamarca y Samuel Braunstein de Universidad Wales de Bangor lograron efectuar un teletransporte cuántico de cientos de fotones con varios estados cuánticos utilizando el mismo método de entrelazamiento con la diferencia de que utilizaron dos

cristales. El primero, al pasar un rayo láser, dividía cada fotón entrante en dos fotones con el doble de frecuencia; este nuevo rayo de luz fue conducido a través de un segundo cristal, que redujo a la mitad las frecuencias, produciendo lo que se denominó "luz exprimida". Ciertamente lograron luz con la misma frecuencia que tenían al comienzo pero ahora los rayos estaban entrelazados.

En 2001, Eugene Polzik y su equipo de la Universidad Aarhus de Dinamarca, logró entrelazar trillones de átomos en dos halos de cesio.

Aún queda un enorme salto tecnológico entre el teletransporte de partículas luminosas y el teletransporte de los átomos que conforman el cuerpo humano, considerando que hay aproximadamente 10.000.000.000.000.000.000.000.000.000 de átomos en el cuerpo y por el momento nadie ha sido capaz de teletransportar un solo átomo.

Sin embargo existe un importante elemento filosófico a tener en cuenta. El teletransporte con éxito implica la producción de una copia exacta, pero una vez que se ha completado la duplicación, el original siempre se destruye, de manera que la copia se convertiría en el nuevo original. Se supone que el nuevo cerebro original contendrá todos los años de recuerdos, aprendizaje y experiencia, pero ¿qué sucede con el alma?, suponiendo que exista. El problema es que nadie ha probado que el alma realmente exista y si el alma no puede ser explicada mediante medios físicos ¿Cómo saber si es posible teletransportarla? Es posible que una máquina de teletransportación pudiera probar si el alma existe o no.

Una vez Einstein dijo "cuanto más éxito alcanza la teoría cuántica, más estúpida parece".