74

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

HACIA UNA COMPUTADORA CUANTICA

T E S I S
QUE PARA OBTENER EL TITULO DE:
INGENIERO MECANICO ELECTRICISTA
P R E S E N T A:

JORGE OLEA FLORES

ASESOR: DR. ZBIGNIEW OZIEWICZ KWASS

CUAUTITLAN IZCALLI, EDO. DE MEX. 2001

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

U. N. A. M.
FACULTAD DE ESTUDIOS
DEPARTAMENTO DE EXAMENES PROFESIONALES

ASUNTO: VOTOS APROBATORIOS

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos la TESIS:

"Hacia una Computadora Cuántica"

que presenta el pasante: Jorge Olea Flores
con número de cuenta: 09312514-1 para obtener el título de:
Ingeniero Mecánico Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 5 de Noviembre de 2001

PRESIDENTE	Ing. Fernando Guerra Parra	
VOCAL	Fís. José de Jesús Cruz Guzmán	
SECRETARIO	Dr. Zbigniew Oziewicz Kwass	Zbigniew Oziewicz
PRIMER SUPLENTE	Ing. Nicolas Calva Tapia	
SEGUNDO SUPLENTE	Ing. Ramón Osorio Galicia	

Esta Tesis es parte de un temario más amplio de investigaciones.

- Cátedra: Álgebra y Lógica en la Ciencia Computacional, clave 2.04, Nivel III.
- Proyecto 27670-E, Métodos diagramáticos en modelos algebráicos en teoría de campos y en lógicas, apoyado por el CONACyT.
- Proyecto IN-109599, Lógicas no-clásicas y aplicaciones en ciencias de la computación, apoyado por DGAPA.

El autor del presente documento fue becario en el proyecto IN-109599.


PERSONAL
TEX
INC

Agradecimientos

*El que tiene imaginación sin instrucción, tiene alas, más no cuerpo.**

*Leonardo da Vinci (1452-1519)

Tan solo soy el escriba del fruto de mis padres.[†]

[†]Jorge Olea Flores, "*ricKter*"

Logros de la Tesis:

- Dar una razón más por la que el ser humano aún tiene mucho que develar.
- Haber consultado más de setenta referencias para la elaboración del presente escrito.
- Haber adecuado un tema propio del Doctorado al nivel Licenciatura.
- Haber creado un punto de partida a futuras investigaciones, tanto teóricas como experimentales.
- Presentar el texto como el primero en Español al Cómputo Cuántico.
- Presenciar la creación y diligencia en el desarrollo de una nueva tecnología.
- Que la tesis contenga el potencial suficiente para ser publicada como libro, en opinón del asesor.
- Haber pasado del incognositivo y robusto mundo experimental a la fragilidad de lo abstracto en la Teoría Cuántica.
- Haber ampliado mi capacidad de síntesis.
- Haber aprendido a utilizar el programa PCTEX32.
- Haber practicado la comprensión de resultados teóricos y prácticos en Inglés.
- Haberle dejado a la Universidad Nacional una pequeña parte de mí.

Contenido

Capítulo 1

Introducción

1.1 Presentación

La presentación de la computación y computadora cuánticas en las siguientes páginas está basada ampliamente en varios puntos de vista, físicos y teóricos. Sin embargo, mi designio es presentar el desarrollo de la computadora cuántica desde el punto de vista de la ingeniería, dominio absoluto de los principios físicos y la ciencia de los materiales cuya necesidad es desarrollar el hardware cuántico.

Inicio con las palabras del investigador en teoría compleja Lance Fortnow [2000 pg. 4]:

> Puede alguien estudiar computación cuántica sin antecedentes profundos en mecánica cuántica? Sí. Manejo un auto sin saber lo que hace un carburador. Puedo programar una computadora clásica e investigar sobre la complejidad computacional de estas máquinas aun sin tener un comprendimiento real de como trabaja un transistor. Frecuentemente investigo modelos de computación teórica tales como no deterministas que no tienen contraparte física en lo absoluto. Dado un modelo de una computadora cuántica, científicos en computación pueden estudiar las habilidades computacionales sin mucho conocimiento de las propiedades físicas de ese modelo.
>
> Los físicos generalmente utilizan la notación de bra-ket de Dirac para representar estados cuánticos base. Cuando los científicos

en computación ven esta notación, que parece completamente extraña asumen que la complejidad de la notación refleja principios profundos en mecánica cuántica. Nada podría estar más alejado de la verdad que la notación bra-ket que representa nada más que vectores.

La notación $|010\rangle$ es llamada "ket" y representa a la cadena 010. En general $|x\rangle$ con $x \in \{0,1\}^k$ representa a la cadena x, concatenación es concatenación: $|x\rangle|y\rangle = |xy\rangle$. La cadena de longitud k forma la base de un vector de espacio de dimensión 2^k

También hay un "bra" y varias reglas que se aplican cuando los bras y kets están juntos, los cuales raramente se usan en computación cuántica.

Por qué la notación que parece tan simple causa tanta confusión? Esta notación no conforma con las convenciones de los científicos en computación, particularmente la de la simetría. Cuando consideramos vectores u otros objetos agrupados, ellos siempre usan corchetes simétricos tales como $\langle 8,3,4\rangle$, $[0\ldots1]$, $(a+b)^*$ y $|x|$. Cuando ven un caracter como "$\rangle$" o "$|$" que no tiene una contraparte, ellos los consideran como operadores relacionales, haciendo a las ecuaciones como

$$|\psi_1(y)\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{\delta_{x,y}} |x\rangle = |\psi_0\rangle - \frac{2}{\sqrt{2^n}} |y\rangle \qquad (1.1)$$

imposible de analizar.

Como este documento lo sugiere, uno no tiene que conocer la notación de Dirac para comprender lo básico de la computación cuántica. Desafortunadamente estamos forzados a aprenderla para seguir la comunicación en el campo.

Alguien puede desarrollar fácilmente una notación más natural para los científicos en computación pero ya hemos perdido la batalla. Eventualmente la notación se vuelve más fácil de analizar y seguir a las fórmulas de la ecuación (1.1) parece casi normal. Es penoso que no vayan a charlas sobre computación cuántica no por la complejidad del asunto sino por la notación anormal.

1.2 Epítome

Varias han sido las piedras milenarias en la historia de la tecnología que involucran el descubrimiento de nuevas formas de controlar a la naturaleza para fructuosos beneficios, explotando muchos recursos físicos tales como materiales, fuerzas, y fuentes de energía. En el siglo veinte, la información entró a esta lista cuando la invención de las computadoras permitió el procesamiento de información compleja no sólo en el cerebro humano. La historia de la tecnología computacional ha involucrado una secuencia de evoluciones, de un tipo de realización física a otra, de engranes a relevadores, de válvulas a transistores, a circuitos integrados y así sucesivamente. Actualmente, las avanzadas técnicas litográficas pueden grabar compuertas lógicas y cables menores a una micra por toda la superficie de silicón que forma al circuito [Deutsch y Ekert, 1998 pg. 1]. Dada la actual tendencia de miniaturización tecnológica, los componentes electrónicos serán más pequeños, hasta el punto donde las compuertas lógicas sean tan pequeñas, que consistirán sólo de moléculas, núcleos y hasta átomos. Esto nos guía hacia el dominio cuántico, pues las nociones clásicas, para la creación y análisis de nuevos dispositivos, aquí ya no son válidas.

Esto implica que la nueva tecnología *cuántica* debe remplazar o suplir a lo que tenemos ahora; pero resulta que dicha tecnología puede ofrecer mucho más que procesadores más rápidos y más pequeños, presenta modos enteramente nuevos de computación, realización de tareas que ninguna computadora clásica podría realizar.

La investigación teórica y experimental sobre computación cuántica han venido creciendo en los últimos diecisiete años. La idea de que la naturaleza puede ser manipulada y controlada a niveles cuánticos es un poderoso estímulo a la imaginación de físicos e ingenieros. Los avances son constantes en el desarrollo de tecnologías más prometedoras para la realización de una computadora cuántica.

En marzo del año dosmil, investigadores del Departamento de Energía del Laboratorio Nacional de Los Alamos y del Instituto Tecnológico de Massachussets (MIT), crearon una computadora cuántica formada con siete bits cuánticos o "qubits" [Laflamme, 2000]. En agosto del mismo año se presenta otra más, desarrollada entre el Centro de Investigaciones IBM, la Universidad de Stanford y la Universidad de Calgary, siendo ésta de cinco qubits [Chuang, 2000 pg. 1].

El camino para llegar a una satisfactoria implementación de una computadora cuántica aún es largo. La construcción de los cimientos para el desarrollo tecnológico de ésta nueva tecnología continuan.

De esta forma, aquí se presenta, sin ilimitación del alcance ingenieril, las ideas requeridas para la implementación de la computadora cuántica, conjuntando ideas tales como Teoría de la Computación, Física Cuántica y Teoría de la información.

Iniciando con los conceptos básicos y fundamentales para la interpretación de todo el material, no es importante, para la ingeniería hasta cierto punto, la demostración rigurosa del formalismo matemático aquí mostrado.

1.3 Antecedentes Históricos

> "No ha sido el pilar de las civilizaciones, sino un entrañable vínculo entre la delicadeza del pensamiento abstracto, lo robusto de una demostración física y la aplicación de ambos."*

El ser humano busca hacer preguntas y encontrar respuestas precisas a cuestiones básicas sobre por qué la naturaleza es como es. Históricamente, los principios fundamentales de la física han tenido relación con preguntas tales como "¿De qué están hechas las cosas?" y "¿Por qué los objetos se mueven de esa manera?" En su *Principia*, Newton dió respuestas muy generales a preguntas de este tipo. Demostrando que las mismas ecuaciones matemáticas pueden describir el movimiento de los objetos que vemos y de los planetas, el mostró que todo objeto cotidiano tal como una tetera está hecha esencialmente de *la misma materia* que un planeta: los movimientos de ambos son descritos en términos de su masa y las fuerzas que actúan sobre ellos. Hoy en día diríamos que se mueven de tal manera que conservan su energía y momentum. De esta forma la Física nos permite extraer conceptos de la naturaleza como el de energía y momentum los cuales siempre obedecen ecuaciones fijas, aunque la misma energía pueda ser expresada en diferentes maneras.

*ricKter

Algo más que puede ser expresado en diferentes maneras es la información. Históricamente, el concepto de información no tiene un origen claro. Podríamos seguir un inicio importante a partir de la paradoja del demonio de Maxwell [Steane, 1997 pg. 5] de 1871 (fig 1a). Recordando que el demonio de Maxwell es una criatura que abre y cierra una puerta entre los dos compartimientos de una cámara que contiene gas, y que persigue la subversiva política de sólo abrir la puerta cuando las moléculas más rápidas se aproximan desde la derecha, o las lentas desde la izquierda.

De esta manera el demonio establece una diferencia de temperatura entre los dos compartimientos sin realizar ningún trabajo, violando la segunda ley de la termodinámica, y consecuentemente permitiendo una multitud de contradicciones.

Un gran número de intentos se hicieron para exorcizar al demonio de Maxwell, como: el demonio no puede reunir información sin realizar trabajo o sin excitar (y calentar) al gas, ambos no son ciertos. Algunos intentaron proponer que ciertamente la segunda ley de la termodinámica era violada por las acciones de un "ser inteligente". Fue hasta 1929 que Leo Szilard redujo el problemas hasta sus componentes básicos, en los cuales el demonio necesita simplemente identificar si la molécula está a la izquierda o derecha de una partición, y su acción permite el calentamiento de un simple motor, llamado el motor de Sziliard. Pero esto aún no era claro, ya que el demonio debe aprender donde está la molécula, incrementando la entropía.

No se dió ninguna respuesta en los siguientes cincuenta años. En los años intermedios las computadoras digitales fueron desarrolladas, y las implicaciones físicas sobre la acumulación y procesamiento de la información fueron cuidadosamente consideradas. El costo termodinámico de la manipulación de información elemental fue analizado por Landauer en 1961 y otros durante la década de los sesentas como, Keyes y Landauer en 1970), y aquellos de computación general por Bennet, Fredkin, Toffoli y otros durante los setentas (Bennet 1973, Toffoli 1980, Fredkin y Toffoli 1982). Se encontró que todo en principio puede hacerse de una manera reversible, es decir, sin costo de entropía en lo absoluto (Bennet y Landauer 1985). Bennet en 1982 relacionó explícitamente este trabajo y la paradoja de Maxwell proponiendo que el demonio sí aprende donde está la molécula en el motor de Szilard sin realizar trabajo o incrementar la entropía en el ambiente y así obtener trabajo útil durante una rotación del motor. Sin ambargo, la información sobre el lugar de la molécula entonces debe estar presente en la memoria del demonio

(fig 1a). Entre más y más rotaciones se hagan, más información es reunida en la memoria del demonio. Hasta completar un ciclo termodinámico, el demonio debe *borrar* su memoria, y es durante este proceso de borrado que identificamos un incremento en la entropía del ambiente, como lo requiere la segunda ley de la termodinámica. Esto completa la física esencial del demonio de Maxwell.

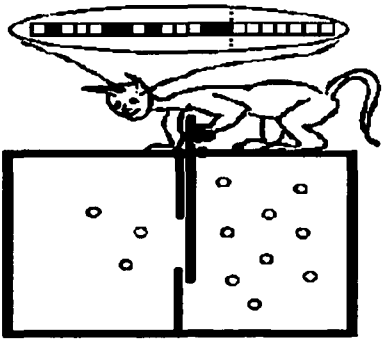


Fig. 1a. El demonio de Maxwell. En esta ilustración el demonio establece una diferencia de presión al levantar la parte divisoria cuando hay más moléculas de gas aproximándose desde la izquierda que desde la derecha. Esto puede hacerse de manera totalmente reversible, mientras la memoria del demonio almacena los resultados aleatorios de sus observaciones de las moléculas. De esta forma la memoria del demonio se calienta. El paso irreversible no es la adquisición de información, sino la perdida de información si el demonio limpia su memoria más tarde.

La teoría de la información clásica esta fundada sobre la definición de información. La teoría trata de capturar lo mayor posible del término información. 'Información' para nosotros será un término abstracto, definido en detalle en la Sección 3.1. Los antecedentes de la teoría de la información nos remontan hasta el trabajo de Shannon en la década de los cuarenta. La observación de que la información puede ser traducida de una forma a otra está encapsulada y cuantificada en el teorema de codificación sin ruido de Shannon (1948), el cual cuantifica las fuentes necesarias para almacenar o transmitir una cierta cantidad de información relacionada con la velocidad

de transmisión. Este teorema es el resultado central de la teoría de la información clásica.

Los fundamentos de la ciencia de la computación fueron formulados al mismo tiempo que la teoría de la información de Shannon. El padre de la ciencia computacional es, a discutir, Alan Turing (1912-1954), y su profeta es Charles Babbage (1791-1871). Babbage concibió la mayoría de los elementos eseciales de una computadora moderna, aunque en sus días no existía la tecnología para implementar sus ideas. Un siglo después, antes que el Motor Analítico de Babbage fuera mejorado Turing describe La máquina Universal de Turing a mediados de los treintas, Turing intenta aclarar exactamente lo que era capaz de hacer una máquina de cálculos y enfatizar el rol de la programación, es decir, el software, aún más de lo que Babbage había hecho.

Las computadoras actuales no son máquinas de Turing ni motores de Babbage, aunque estén basadas en principios generales muy similares, y su potencia computacional sea equivalente, en un sentido técnico. Su único desarrollo, al través de los años, ha sido una mejora en tamaño y velocidad pero no involucra ningún cambio en la idea esencial de lo que es una computadora, o como opera. La mecánica cuántica da la posibilidad de tal cambio.

La mecánica cuántica es la estructura matemática que abarca, en principio, la totalidad de la Física. No corresponde, directamente, con la gravedad, altas velocidades, o partículas exóticas elementales, será suficiente con tratar a la mecánica cuántica no-relativista. La característica importante de la teoría para nuestro propósito no son los detalles en las ecuaciones del movimiento, sino el hecho de que tratan las amplitudes cuánticas de probabilidades, o vectores de espacio en un espacio de Hilbert ($\mathbb{C}$-espacio), en lugar de variables clásicas, pues esto es lo que permite nuevos tipos de información y computación.

Hay cierta similitud entre las preguntas de David Hilbert (1862-1943) sobre las matemáticas y las preguntas que se buscan proponer en la teoría de la información. Antes de Hilbert, casi todos los trabajos matemáticos estaban interesados en establecer o refutar hipótesis particulares, pero Hilbert quiso preguntar que tipo general de hipótesis era más tratable para una prueba matemática. Similarmente, la mayoría de las investigaciones en mecánica cuántica han estado interesadas en el estudio de la evolución de sistemas físicos específicos, pero queremos preguntar que tipo general de evolución es

más concebible bajo las reglas cuánticas.

La primera visión en la teoría de la información cuántica llegó con el análisis de Bell en 1964 sobre el paradójico experimento mental propuesto por Einstein, Podolsky y Rosen (EPR) en 1935. La desigualdad de Bell llamó la atención por la importancia de las *correlaciones* entre sistemas cuánticos separados que han interactuado (directa o indirectamente) en el pasado, pero que ya no influencían el uno con el otro. En esencia su argumento mostró que el grado de correlación que puede estar presente en esos sistemas excede a aquel que pudiera ser predicho sobre las bases de cualquier ley de la física la cual describe partículas en términos de variables clásicas en lugar de estados cuánticos.

El siguiente vínculo entre la mecánica cuántica y la teoría de la información llega cuando se descubre que las simples propiedades de los sistemas cuánticos, tales como la inevitable perturbación involucrada en las mediciones, podría ser puesta en práctica en la *criptografía cuántica*, ésta cubre varias ideas, de las cuales la más firmemente establecida es la distribución clave cuántica. Este es un ingenioso método en el cual los estados cuánticos transmitidos ejecutan una tarea de comunicación muy particular: establecer en dos localidades separadas un par de secuecias binarias idénticas, pero de otra manera aleatoria, de dígitos binarios, evitando que una tercera parte conozca la secuencia. Esto es muy útil porque dicha secuencia aleatoria puede ser usada como una clave criptográfica que permita una comunicación segura.

Mientras la criptografía cuántica estaba siendo analizada y demostrada, la computadora cuántica estaba pasando por sus etapas prematuras. Ya que la mecánica cuántica subraya el comportamiento de todos los sistemas, incluyendo a aquellos que llamamos clásicos, no era obvio como concebir una distintiva computadora mecánica cuántica, es decir, una que no reprodujera la simple acción de una máquina clásica de Turing. Obviamente no es suficiente con identificar un sistema cuántico cuya evolución pudiera ser interpretada como un cálculo; uno debe probar un resultado más fuerte que esto. Conversando, sabemos que las computadoras clásicas pueden simular, con sus cálculos, la evolución de cualquier sistema cuántico ... con una restricción: ningún proceso clásico le permitirá preparar sistemas separados cuyas correlaciones rompan la desigualdad de Bell.

Para pensar en la computación desde un punto de vista cuántico, las

primeras ideas involucraron la conversión de la acción de una máquina de Turing en un proceso equivalente reversible, y después inventar un Hamiltoniano el cual causaría que un sistema cuántico evolucionara en una forma que imitara a una máquina reversible de Turing.

Richard Feynman (1982, 1986) toma un acercamiento diferente, considera la posibilidad, no de una computación universal, sino de una *simulación* universal, esto es, un sistema cuántico construido que pudiera simular el *comportamiento físico* de cualquier otro. Claramente, dicho simulador sería también una computadora universal, ya que cualquier computadora debe ser un sistema físico. Feynman dió argumentos los cuales sugirieron que la evolución cuántica podría ser usada para calcular ciertos problemas más eficientemente que cualquier computadora clásica, pero este dispositivo no estaba lo suficientemente especificado para ser llamado un computador, puesto que él asumió que cualquier interacción entre sistemas de dos estados adyacentes pudieran ser 'ordenados', sin decir como.

En 1985 un paso muy importante fue dado por David Deutsch [Deutsch, 1985 pg. 3]. La proposición de Deutsch es ampliamente considerada para representar el primer plano para una computadora cuántica. El sistema de Deutsch es esencialmente una línea de sistemas de dos estados, y se asemeja más a una máquina registradora que a una máquina de Turing (ambas son máquinas de computación universales clásicas). Deutsch probó que si el sistema de dos estados pudiera hacerse que evolucionara por medio de un pequeño conjunto específico de operaciones simples, entonces, *cualquier* evolución unitaria podría ser producida, y a consecuencia la evolución podría hacerse que simulara aquella de cualquier sistema físico. Él también discutió como producir comportamiento parecido al de Turing usando las mismas ideas.

Las operaciones simples de Deutsch ahora son llamadas 'compuertas' cuánticas, ya que son análogas a aquellas compuertas de lógica binaria de las computadoras clásicas. Varios autores han investigado la clase mínima de compuertas que son suficientes para la computación cuántica [Barenco et. al. 1995 pg. 10].

Los dos aspectos cuestionables de la proposición de Deutsch son su eficiencia y realización. La pregunta sobre la eficiencia es absolutamente fundamental en la ciencia de la computación, y sobre ella gira el concepto de 'universal'. Una computadora *universal* es aquella que no solamente puede

reproducir (simular) la acción de cualquier otra, y además lo hace sin correr tan lentamente. La 'lentitud' está definida en términos del número de pasos computacionales requeridos: este número no debe incrementarse exponencialmente con el tamaño de la entrada (el significado preciso será explicado en la sección 4.1). El simulador de Deutsch no es universal en este estricto sentido , aunque Lloyd (1996) probó que es eficiente para la simulación de varios sistemas cuánticos. Sin embargo, el trabajo de Deutsch ha establecido los conceptos de redes (Deutsch 1989) y compuertas lógicas cuánticas, las cuales son extremadamente importantes en cuanto que nos permiten pensar claramente en la computación cuántica.

A principios de los noventas varios investigadores entre ellos, Deutsch y Jozsa en 1992, Berthiaume y Brassard en 1992, Bernstein y Vazirani en 1993, buscaron tareas computacionales que pudieran ser resueltas por una computadora cuántica más eficientemente que cualquier computadora clásica. Tal algoritmo tomaría un rol conceptual similar al de la desigualdad de Bell, al definir algo de la naturaleza esencial de la mecánica cuántica. Un avance importante fue hecho por Simon (1994), quien describe un algoritmo cuántico eficiente para un problema (de alguna manera abstracto) para el cual ninguna solución eficente era posible en sistemas clásicos, aun por métodos de probabilidad. Esto inspira a Shor (1994) quien asombra a la comunidad al describir un algoritmo que no solo era eficiente en una computadora cuántica, sino que también direccionaba un problema central en la ciencia computacional: la factorización de números enteros grandes.

Shor discute la factorización y los logaritmos discretos en [Shor, 1995], haciendo uso del método de la transformada cuántica de Fourier descubierto por Coppersmith (1994) y Deutsch. Más adelante algunos algoritmos cuánticos importantes fueron descubiertos por Grover (1997) y Kitaev (1995).

Al igual que la computación clásica y la teoría de la información, una vez que las ideas teóricas de la computación habían sido un poco olvidadas, se hizo un esfuerzo por establecer la naturaleza esencial de la información cuántica -la tarea análoga al trabajo de Shannon. Aquí la dificultad puede ser vista al considerar el sistema cuántico más simple, un sistema de dos estados tal como una partícula de medio espín en un campo magnético. El estado cuántico de un espín es una cantidad continua definida por dos números reales, así que en principio puede almacenar una cantidad infinita de información clásica. Sin embargo, la medición de un espín dará sólo una

respuesta de dos valores (espín abajo, espín arriba)- aquí no hay manera de obtener acceso a la información infinita que aparenta estar ahí, por tanto es incorrecto considerar el contenido de información en esos términos. Schumacher y Jozsa (1994) demuestran que el sistema de dos estados juega el rol, en la teoría de la información cuántica, análogo al del bit en la teoría de la información clásica en que el contenido de la información cuántica de cualquier sistema cuántico puede ser significativamente medido como un número mínimo de sistemas de dos estados, ahora conocidos como bits cuánticos, los cuales serían necesarios para transmitir el estado del sistema con gran precisión.

Regresando a la pregunta de la realización de la computadora cuántica. Es elemental, pero fundamentalmente importante, la observación de que los efectos de la interferencia cuántica sólo permiten que los algoritmos como el de Shor sean extremadamente frágiles: la computadora cuántica es ultra sensitiva al ruido y a cualquier influencia experimentales. Armada con el algoritmo de Shor, parece que tal significado fundamental se ha establecido, con el siguiente argumento: ya sea que la naturaleza en verdad permite un dispositivo que corra con la suficiente precisión para ejecutar el algoritmo de Shor para grandes enteros (digamos, más grandes que 10^{10}), o existen límites fundamentales naturales que dan la precisión en los sistemas reales. Ambas eventualidades representan una visión importante en las leyes de la naturaleza.

En este punto, las ideas de la información y computación cuánticas se unen. Para una computadora cuántica se puede hacer que sea menos sensitiva al ruido por medio de una nueva idea, que se forma a partir de la unión de la mecánica cuántica con la teoría de la información clásica, nombrada *corrección de errores cuánticos* explicada en [Gottesman, 2000]. Un desarrollo importante fue la demostración de Shor en 1996) y Kitaev también en 1996, en que la corrección puede ser alcanzada aun cuando las operaciones correctoras sean en ellas mismas imperfectas. Tal método conduce al concepto general computación 'tolerante a fallas'[Leung, 2000 pg. 52].

Al parecer, la computación cuántica sólo trabajará en conjunción con la corrección de errores cuánticos, y que hay una estrecha relación entre la teoría cuántica de la información y las computadoras cuánticas. La corrección de errores no garantiza en ella misma cálculos precisos, puesto que no puede combatir a todos los tipos de ruido, pero el hecho de que es posible en lo absoluto es un desarrollo significativo.

Una computadora que solo exista en papel no resolverá nada. Con este fin, un número de autores propusieron diseños de computadoras basados en la idea de Deutsch pero con los detalles físicos más elaborados, entre ellos: Teich en 1988, Lloyd en 1993, Berman en 1994 y DiVicenzo en 1995. El gran reto es encontrar un sistema lo suficientemente complejo cuya evolución sea coherente (esto es unitaria) y controlable. No es suficiente que sólo algunos aspectos deberían ser cuánticos, como en los 'puntos cuánticos' de estado sólido, o que hay una asunción implícita de precisión no posible o enfriamiento, la cual es el caso cuando se utilizan componentes de estado sólido. Cirac y Zoller (1995) propusieron el uso de una trampa lineal de iones que demostró avances muy rápidos. Más recientemente, Gershenfeld y Chuang (1997) y Cory (1996, 1997) han demostrado que las técnicas de resonancia magnética nuclear (NMR) pueden ser adaptadas para llenar los requerimientos de la computadora cuántica. Siendo esta última técnica la que construyera la computadora de siete qubits.

Como siguen las cosas, ninguna computadora cuántica ha sido construida, basándonos en términos del algoritmo de Shor. Sin embargo, si buscamos un dispositivo en el cual las ideas de la información cuánticas puedan ser exploradas, entonces sólo necesitamos algunos qubits [Steane, 1997 pg. 10].

Bibliografía

[1] Barenco Adriano, Charles H. Bennett, Richard Cleve, David P. DiVicenzo, Norman Margolus, Peter Shor, Tycho Sleator, John Smolin y Harald Weinfurter, *Elementary gates for quantum computation.* Enviado a Physical Review A, 22 de marzo de 1995 (AC5710). e-print.

[2] Chuang Isaac L, *Team uses quantum computer to solve problem*; Artículo de 'HPCwire', agosto de 2000.

[3] Deutsch David and Artur Ekert, *Quantum Computation*; Artículo de 'Physics World', número de marzo de 1998.

[4] Deutsch David, *Quantum theory. The Church-Turing principle and the universal quantum computer*; Proceedings of the Royal Society of London A 400. pg. 97, 11 de julio 1985.

[5] Fortnow Lance, *One Complexity Theorist's view of Quantum Computing*; Basado en una charla presentada en el Segundo Taller sobre Algoritmos en el Procesamiento de Información Cuántica en la Universidad DePaul, Chicago, enero de 1999. Instituto de Investigaciones NEC, Marzo de 2000. El Real audio de la charla está disponible en www.cs.depaul.edu/aqip99.

[6] Gottesman Daniel, *An introduction to Quantum Error Correction*; Simposio de Matemáticas Aplicadas, e-print: quant-ph\0004072

[7] Laflamme Raymond, *Quantum Leap*; Tomado de la sección 'Prototype' de la revista 'Poptronics', mayo de 2000.

[8] Leung Debbie W., *Towards robust quantum computation*; Disertación enviada al Departamento de Física y al Comité de Estudios de Grado de la Universidad de Stanford en cumplimiento parcial de los requerimientos para el grado de Doctor en Filosofía. Julio de 2000.

[9] Shor Peter W., *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*; en Proc. 35th Annual Symp. on Foundations of Computer Science, Santa Fe, IEEE Computer Society Press; preprint quant-ph\9508027.

[10] Steane Andrew, *Quantum computing*; Universidad de Oxford, Inglaterra. Julio de 1997. e-print: quant-ph\9708022

Capítulo 2

Nociones Precedentes

2.1 Categorías

Por qué teoría de categorías? Es una rama de las matemáticas relativamente jóven, refrenando la topología algebráica, y diseñada a describir varios conceptos estructurales de diferentes campos de la matemática en una forma uniforme. Esta teoría provee una bolsa de conceptos (y teoremas sobre estos conceptos) que forman una abstracción de varios conceptos concretos en las diversas ramas de las matemáticas, incluyendo a la ciencia de la computación [Fokkinga, 1994].

Definición
Es una colección de cosas llamadas *Objetos*, y una colección de cosas llamadas *morfismos*, algunas veces nombradas *flechas*, éstos últimos, son los que relacionan a objetos.

2.2 Categoría de espacios vectoriales

Definición:
Un **$\mathbb{C}$-espacio vectorial** V es un grupo conmutativo (abeliano) con la acción de números $\mathbb{C}$ sobre V, esto es, $\mathbb{C} \otimes V \rightarrow V$. En donde diferentes acciones producen diferentes $\mathbb{C}$-espacios.

Siendo $\vec{u}, \vec{v}, \vec{w}$ elementos de V; una operación binaria de un grupo cumple con las propiedades:

1. asociativa
   $\vec{u} + (\vec{v} + \vec{w}) = (\vec{u} + \vec{v}) + \vec{w}$

2. Elemento neutro
   $\vec{u} + \vec{0} = \vec{u}$

3. Inverso
   $\vec{u} + (-\vec{v}) = \vec{0}$

Además cumplen con la propiedad distributiva para cualquier escalar.

Ejemplos de $\mathbb{R}$- o $\mathbb{C}$-espacios vectoriales son: Conjunto de Matrices, Conjunto de funciones, el anillo de los números complejos.

Definición:
Vector es un elemento de cualquier espacio vectorial con características conocidas.

Dimensión del espacio vectorial

La dimensión de un espacio vectorial es el número de elementos que conforman su base.

$\mathbf{dim}_{\mathbb{R}}\ V = 0$ Si sólo tiene un elemento $e = 0$.

$\mathbf{dim}_{\mathbb{R}}\ V = 1 \Rightarrow \forall\, \vec{a} \in V\ ; \forall\, e \neq 0\ ; \exists\, r \in \mathbb{R}\ ,\ \vec{a} = re \therefore\ e$ es elemento único de la base.

$\mathbf{dim}_{\mathbb{R}}\ V = 2 \Rightarrow \forall\, \vec{a} \in V\ ,\ \exists\, r_1, r_2 \in \mathbb{R},\ \vec{a} = r_1 e_1 + r_2 e_2,$

$\mathbf{dim}_{\mathbb{C}}\ \mathbb{C} = 1$

$\mathbf{dim}_{\mathbb{R}}\ \mathbb{C} = 2$

2.3 Funtores

Al igual que las funciones son relaciones entre elementos de dos conjuntos, $f(x, y)$, el funtor es la parte análoga de la función, pues la función aplica sólamente a conjuntos, así, el funtor aplica a categorías.

La categoría de $\mathbb{C}$-espacios vectoriales tiene dos endofuntores unarios (con una sola variable), dualidad '*' $V \overset{*}{\mapsto} V^*$ y complejo conjugado '-' $V \overset{-}{\mapsto} \bar{V}$; y dos binarios (con dos variables), la *suma directa* denotada por: $\oplus$; y el *producto tensorial* expresado con: $\otimes$. Ahora, siendo $\mathbb{C}$-cat $= \{V, W, \dots\}$

y $\mathbb{C}$-vect $= \{V, W, \dots\}$ ambas categorías de espacios vectoriales con sus objetos $V, W, \dots$, los endofuntores binarios los relacionan:

$$\bigoplus : V, W \xrightarrow{\oplus} V \oplus W \in \text{cat}$$

$$\bigotimes : V, W \xrightarrow{\otimes} V \otimes W$$

Las operaciones realizadas por la suma directa son

$$W \oplus V = \begin{cases} (\vec{w}, \vec{v}) + (\vec{a}, \vec{b}) = (\vec{w} + \vec{a}, \vec{v} + \vec{b}) \\ r(w, v) = (rw, rv), \qquad \forall\, r \in \mathbb{C} \end{cases}$$

Al resultado del funtor -como suma directa- el cual para nuestro caso, opera con espacios vectoriales, es otro espacio vectorial en la misma categoría.

2.3.1 Tensor

Ahora bien, el tensor t es un elemento del resultado del funtor como producto tensorial y es conocido como tensor de grado uno:

$$t \in V \otimes W$$

Éste se puede interpretar como una interacción física, èg. Si V es un $\mathbb{C}$-espacio de los estados de un electrón y, W es un $\mathbb{C}$-espacio de otros estados de otro electrón esto implica que $V \otimes W$ es un $\mathbb{C}$-espacio de los estados de un sistema de *dos* electrones.

Ejemplos:

Sean V, W $\mathbb{C}$-espacios vectoriales

1.-
$\dim_{\mathbb{C}} V = 2$
$\dim_{\mathbb{C}} W = 3$

$$\dim_{\mathbb{C}} (V \oplus W) = 5$$
$$\dim_{\mathbb{C}} (V \otimes W) = 6$$

2.-
$\dim_{\mathbb{R}} \mathbb{R} = 1$

$$\dim_{\mathbb{R}} (\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}) = 3$$
$$\dim_{\mathbb{R}} (\mathbb{R} \otimes \mathbb{R} \otimes \mathbb{R}) = 1$$

2.3.2 Tipo de tensor

Sean V, W $\mathbb{R}$-espacios vectoriales con $\dim_{\mathbb{R}} V = 3$ y $\dim_{\mathbb{R}} W = 2$, cuyas bases serán (e_1, e_2, e_3) y (f_1, f_2), respectivamente.

Un tensor cualquiera, $t \in V \otimes W$ con $\dim_{\mathbb{R}}(V \otimes W) = 6$, puede representarse en forma general como:

$$t = a_1 e_1 \otimes f_1 + a_2 e_1 \otimes f_2 + a_3 e_2 \otimes f_1 + a_4 e_2 \otimes f_2 + a_5 e_3 \otimes f_1 + a_6 e_3 \otimes f_2 \quad (2.1)$$

Sean $\vec{u} \in V$ y $\vec{w} \in W$, además por lo menos un vector es desigual a cero lo que conlleva a, la existencia del tensor tipo 1, esto es, $0 \neq \vec{u} \in V$.

Multiplicando las bases de V y W por los escalares: x, y, z, v, w para obtener los vectores $\vec{u}$ y $\vec{w}$,

$$\vec{u} = xe_1 + ye_2 + ze_3 \quad \in \quad W$$

$$\vec{w} = wf_1 + vf_2 \quad \in \quad V$$

Haciendo las operaciones para $u \otimes w$, teniendo en cuenta que u, w siguen siendo vectores a menos que se especifique lo contrario,

$$\begin{aligned} u \otimes w &= (xe_1 + ye_2 + ze_3) \otimes (wf_1 + vf_2) && (2.2) \\ &= xe_1 \otimes wf_1 + xe_1 \otimes vf_2 + ye_2 \otimes wf_1 + ye_2 \otimes vf_2 + ze_3 \otimes wf_1 + ze_3 \otimes vf_2 \\ &= xwe_1 \otimes f_1 + xve_1 \otimes f_2 + ywe_2 \otimes f_1 + yve_2 \otimes f_2 + zwe_3 \otimes f_1 + zve_3 \otimes f_2 && (2.3) \end{aligned}$$

Definición

$$\text{Si} \quad t \equiv u \otimes w \quad \Rightarrow \quad \text{tipo } t = 1 \quad (2.4)$$

$$\text{Si} \quad t \equiv u_1 \otimes w_1 + u_2 \otimes w_2 \quad \Rightarrow \quad \text{tipo } t \equiv 2 \quad (2.5)$$

$$\text{Si} \quad t = u_1 \otimes w_1 + u_2 \otimes w_2 + u_3 \otimes w_3 \quad \Rightarrow \quad \text{tipo } t = 3 \quad (2.6)$$

$$\vdots$$

En todas estas ecuaciones t es dado como en (2.1), y se buscan los valores de las variables $u, w, u_1, w_1, \ldots$.

Las expresiones (2.4) y (2.1) describen a un tensor tipo 1, las cuales denotan a cualquier tensor de tipo $\leqslant 6$. El principal problema es encontrar

si los tensores de tipo dos, tres, cuatro y cinco existen, además de probar hasta qué tipo es posible.

Por el momento se ejemplificará encontrando a un tensor de tipo 1; tomando a la ecuación 2.1 de donde,

$$\begin{aligned} a_1 &= xw \\ a_2 &= xv \\ a_3 &= yw \\ a_4 &= yv \\ a_5 &= zw \\ a_6 &= zv \end{aligned}$$

habiendo cinco variables desconocidas, x, y, z, w y v. Tenemos que demostrar que la ecuación tiene solución, de ser así, el tensor será de tipo uno. Propiamente, una de las condiciones que cumple con esto es:

$$\text{Si } a_1 a_6 \neq a_2 a_5 \quad \Rightarrow \quad t \text{ no es de tipo uno, el tipo es } t \geqslant 2.$$

Problema: Demostrar que todos los tensores en $V \otimes W$ son de tipo 2.

De manera similar se encontraría:

$$t = u \otimes w + v \otimes p$$

En donde hay cuatro vectores desconocidos, $u, v \in V$ y $w, p \in W$, pero sólo es una hipótesis.

Esto es una tarea muy casi intratable. Las pruebas para tensores mayores que el tipo 2, necesitarán otro tipo de algoritmo para su resolución.

2.4 Bra-kets

La notación de Dirac: $\langle b|$ llamado bra y $|a\rangle$ llamado ket. En esta notación $\langle b|$ y $|a\rangle$ son covectores y vectores respectivamente. $\langle b|a\rangle \in \mathbb{C}$ es la evaluación de $|a\rangle$ con $\langle b|$, por lo que es un escalar, y en mecánica cuántica ordinaria es un número complejo. Se puede pensar en que es la amplitud para que el estado inicie en a y termine en b. Esto es, hay un proceso que puede mediar a la transición del estado a hacia el estado b. Excepto por el hecho que las amplitudes son evaluadas en los complejos, obedecen las leyes usuales de la probabilidad [Kauffman, 2001 pg. 2].

Bibliografía

[1] Fokkinga Maarten M., *A Gentle Introduction to Category Theory*; Universidad de Twente, Países Bajos, 6 de junio de 1994.

[2] Kauffman Louis H., *Quantum Computing and the Jones polynomial*; Departamento de Matemáticas, Estadística y Ciencia de la Computación. Universidad de Illinois en Chicago, Mayo de 2001. e-print: quant-ph\0105255.

Capítulo 3

Teoría de la Información

No veremos los temas principales de este apartado. Solamente se expondrán las ideas principales.

La información puede ser expresada en diferentes maneras -como ya se había puntualizado-. Por ejemplo, las dos oraciones "the quantum computer is very interesting" y "l'ordinateur quantique est très intéressant" tienen algo en común, aunque no tomen parte las mismas palabras. Lo que tienen en común es su contenido de *información*. Esencialmente la misma información podría ser expresada en otras formas; de la misma manera que las magnitudes de un vector en diferentes sistemas de unidades, un ejemplo más básico es, sustituyendo los números por letras en un esquema tal que $a \rightarrow 97$, $b \rightarrow 98$, $c \rightarrow 99$ y así sucesivamente, en cuyo caso, la versión en Inglés se expresa como 116, 104, 101, 32, 113, 117, 97, 110, 116, 117, 109 .... Es de suma importancia tener en cuenta que la información puede expresarse en varias formas sin perder su naturaleza esencial, ya que esto nos conduce a la posibilidad de la manipulación automática de la información: una máquina sólo necesita ser capaz de manipular objetos mucho muy simples como enteros con el fin de realizar el procesamiento de información de manera sorprendente y eficaz, así como, desde el procesamiento de textos hasta el cálculo diferencial, aún la traducción entre lenguajes humanos.

Sin embargo, hay algo que todas las formas de expresión de la información deben tener en común: todas ellas usan objetos físicos reales para hacer el trabajo. Las palabras habladas son transmitidas por medio de fluctuaciones de presión en el aire, las escritas por arreglos de moléculas de tinta sobre el papel, aún los pensamientos dependen de las neuronas. A concluir,

sólo en este punto, "no hay información sin representación física" y sin ésta la ingeniería no tiene nada que ver.

El programa para re-investigar los principios fudamentales de la Física desde el punto de vista de la Teoría de la Información todavía está en su infancia; no obstante, ha sido suficiente para construir todo dispositivo de comunicación que ahora tenemos .

3.1 El bit e Información Clásicos

El problema más básico en la teoría de la información clásica es obtener una medida de la información, es decir, una cantidad de información. Supongamos que nos dicen el valor de un número X. Cúanta información hemos ganado? Eso dependerá de lo que realmente conozcamos sobre X. Por ejemplo, si ya sabíamos que X era igual a 2, no aprenderíamos nada, no se obtiene nada de información, a partir de esta declaración. Por el otro lado, si previamente nuestro único conocimiento era que X resultó de la tirada de unos dados, entonces, para obtener su valor estamos obteniendo información. Llegamos aquí a una propiedad paradójica básica la cual es que la *información* es usualmente una medida de la *ignorancia*: el contenido de la información (o 'auto-información') de X se define a ser la información que obtendríamos si conocemos el valor de X.

Si X es una variable aleatoria la cual tienen un valor x con probabilidad $p(x)$, entonces el contenido de información de X está definido a ser [Steane, 1997 pg. 12]

$$S(\{p(x)\}) = -\sum_x p(x)\log_2 p(x). \tag{3.1}$$

nótese que el logaritmo es base 2, y que S es siempre positivo porque las probabilidades están limitadas por $p(x) \leqslant 1$. S es una función de la *distribución de probabilidad* de los valores de X. Es importante recordar esto, ya que en lo siguiente adoptaremos la práctica estándar del uso de la notación $S(X)$ por $S(\{p(x)\})$. Se comprende que $S(X)$ no denota una función de X, sino el contenido de información de la variable X. La cantidad $S(X)$ también se refiere a la entropía [Lomonaco Jr., 2000 pg. 43].

Si nosotros ya sabemos que $X = 2$, entonces $p(2) = 1$ y no hay otros términos en la suma, produciendo $S = 0$, de esta manera X no contiene in-

formación. Si, por el otro lado, X es dado por el lanzamiento de los dados, entonces $p(x) = 1/6$ para $x \in \{1, 2, 3, 4, 5, 6\}$ así $S = -\log_2(1/6) \simeq 2.58$. Si X puede tomar N diferentes valores, entonces el contenido de información (o entropía) de X es maximizada cuando la distribución de probabilidad p es simple, con cada $p(x) = 1/N$. Esto es consistente con el requerimiento de que la información (que obtendríamos al saber el valor de X) es máxima cuando nuestro conocimiento anterior de X es mínimo.

De esta manera, la máxima información que podría ser almacenada, en principio, por una variable que pueda tomar N diferentes valores es $\log_2(N)$. Los logaritmos se tomaron de base dos en lugar de otra base por convención. La elección dicta que la unidad de información: $S(X) = 1$ cuando X puede tomar dos valores con igual probabilidad. Una variable de dos valores o binaria puede contener una unidad de información. Esta unidad es el *bit*, de aquí en adelante llamado el bit clásico, o *cbit*. El cbit es un elemento del campo $\mathbb{Z}_2 = \{0, 1\}$ con dos elementos $|\mathbb{Z}_2| = 2$ los cuales son sus valores. Estos son representados, en general con la ausencia o presencia de voltaje, respectivamente.

En el caso de la variable binaria, se puede definir p para que sea la probabilidad cuando $X = 1$, y la probabilidad $1 - p$ cuando $X = 0$ y la información puede ser escrita como una función de p sólamente:

$$H(p) = -p\log_2 p - (1-p)\log_2(1-p) \tag{3.2}$$

Esta función es conocida como la *función entropía*, $0 \leq H(p) \leq 1$.

Lo siguiente, dentro de este tema, sería probar que la ecuación 3.1 es una buena medida de la información, la mejor compresión de datos posible (El teorema de la codificación de datos de Shannon), y un método práctico para comprimirlos (código Huffman); así como los errores que puede haber en un canal binario para transmitir la información, más el propósito no es tal.

3.2 El bit e Información Cuánticos

La conclusión obtenida es que "la información es física" y es instructivo considerar las diferentes maneras en las que ésta puede presentarse ante nosotros. Pero fundamentalmente, el universo es mecánico cuántico.

Debió haber sido claro en los inicios de la teoría cuántica que las ideas clásicas acerca de la información necesitarían otra revisión con la nueva física. Por ejemplo, los sonidos registrados en un detector que monitorea una fuente radioactiva están descritos por un proceso *vedaderamente aleatorio* de Poisson. En contraste, no hay lugar para este tipo de proceso en la dinámica clásica determinista (aunque es claro que un sistema clásico complejo -caótico- pueda exhibir un comportamiento que en práctica sea indistiguible de lo aleatorio).

Además, debido al principio de incertidumbre, de los observables no conmutables que no pueden ser medidos simultáneamente, el acto de adquirir información de un sistema físico inevitablemente perturba el estado del sistema. No hay contraparte de esta limitación en la física clásica.

El trueque entre adquirir información y la creación de una perturbación está relacionada con la aleatoriedad cuántica. Esto es porque el resultado de una medición tienen un elemento aleatorio el cual somos incapaces de inferir el estado inicial del sistema del resultado de la medición.

Que el adquirir información ocasiona una perturbación también esta ligada con otra distinción especial entre ambas informaciones: la información cuántica no puede ser copiada con perfecta fidelidad (el principio de no-clonación anunciado por Wootters, Zurek y Dieks en 1982). Si *pudiéramos* hacer una copia perfecta de un sistema cuántico, podríamos medir un observable de la copia sin perturbar al original y podríamos olvidarnos del principio de la perturbación. Por el otro lado, nada nos impide el hacer copias perfectas de la información clásica. Lo que nos lleva a un importante teorema, el Teorema de la No Clonación dado por Wootters y Zurek, el cual establece que no puede haber ningún dispositivo que produzca replicas exactas o copias de un sistema cuántico. La prueba es una aplicación muy simple de la linealidad de la mecánica cuántica. La idea clave es que el copiar es una transformación inherentemente cuadrática, mientras que las transformaciones unitarias de la mecánica cuántica son inherentemente lineales. Por lo tanto, el copiar no puede ser una transformación unitaria. La prueba formal usa la creación de operadores de la electrodinámica cuántica.

Estas propiedades de la información cuántica son muy importantes, pero la verdadera forma en la cual ambas informaciones difieren surge del trabajo de John Bell (1964), quien muestra que las predicciones de la mecánica cuántica no pueden ser reproducidas por ninguna teoría de una variable lo-

cal oculta. Bell también muestra que la información cuántica puede ser (y de hecho típicamente lo es) codificada en correlaciones no locales entre las diferentes partes de un sistema físico, correlaciones sin contraparte clásica.

Ahora ya se puede definir a la correspondiente unidad de información cuántica, el cual es conocido como el "bit cuántico" o *qubit.* Y en palabras de sus autores:

- Un qubit puro es un elemento del $\mathbb{C}$-espacio $\mathcal{H}$ con $\dim_{\mathbb{C}}\mathcal{H} = 2$. Un qubit, no necesariamente puro, es $\rho \in \mathcal{H} \otimes \mathcal{H}^*$ [Oziewicz, 2001].
- Un qubit es un sistema cuántico en el cual los estados Booleanos 0 y 1 están representados por un par de estados cuánticos normalizados y mutuamente ortogonales escritos como $\{|0\rangle, |1\rangle\}$ [Ekert et. al, 2000 pg. 1];
- Un qubit es un sistema cuántico $\mathcal{Q}$ cuyo estado yace en un espacio de Hilbert $\mathcal{H}$ de dos dimensiones [Lomonaco Jr. 2000 pg. 7];
- Un qubit es un sistema cuántico con un espacio de Hilbert, capaz de existir en una superposición de estados Booleanos y de estar enredado con los estados de otros qubits [Barenco et. al, 1995 pg. 4].

Los dos estados forman una 'base computacional' y cualquier otro estado (puro) del qubit puede ser escrito como una superposición $a|0\rangle + b|1\rangle$ para cualquier a y b tales que $|a|^2 + |b|^2 = 1$.

La definición física de un qubit. Un qubit sería un sistema microscópico representado con partículas de espín un medio, un átomo de dos niveles, o un fotón polarizado.

Una colección de n-qubits es llamado un *registro cuántico* de tamaño n, n-qubit $\in \mathcal{H} \otimes \cdots \otimes \mathcal{H}$, $\dim_{\mathbb{C}}(\mathcal{H}^{\otimes n}) = 2^n$

Éstas deficiciones son para qubits puros, pues todo estado incluido en un espacio de Hilbert es puro; no obstante, la definición de Ekert et. al, la más importante hasta este punto, menciona las propiedades de los mismos que independientemente del "grado de pureza" que deben poseer los qubits. Para los qubits no puros ver Sección 5.6.

Mencionando más propiedades no clásicas de los qubits: [Svozil, 2000 pg. 250]

1. Los qubits son contextuales. Un bit cuántico puede parecer diferente, dependiendo del método por el cual es inferido.

2. Los qubits no pueden ser copiados o "clonados". Esto es debido al hecho de que la evolución cuántica es reversible, es decir, uno a uno.

3. Los qubits no necesariamente satisfacen las tautologías clásicas como la ley distributiva.

4. Los qubits obedecen la lógica cuántica la cual es diferente de la lógica clásica.

5. Los qubits son superposiciones coherentes de información contradictoria, clásicamente distinta.

6. Los qubits están sujetos a la complementariedad.
La complementariedad es la imposibilidad de medir dos observables al mismo tiempo con posición arbitraria.

Bibliografía

[1] Barenco Adriano(1), Charles H. Bennett (2), Richard Cleve (3), David P. DiVicenzo (2), Norman Margolus (4), Peter Shor (5), Tycho Sleator (6), John Smolin (7)y Harald Weinfurter (8), *Elementary gates for quantum computation*;(1) Oxford University; (2) IBM Research; (3) University of Calgary; (4) MIT; (5) AT& T Bell Labs; (6) New York Univ.; (7) UCLA; (8) Univ. of Innsbruck. Enviado a Physical Review A, 22 de marzo de 1995 (AC5710). e-print: quant-ph\9503016.

[2] Ekert Artur, Patrick Hayden y Hitoshi Inamori, *Basic concepts in quantum computation*; Centro para la Computación Cuántica, Universidad de Oxford, Reino Unido. Noviembre de 2000. e-print: quant-ph\0011013.

[3] Lomonaco Samuel J., Jr.*A Rosetta Stone for quantum mechanics with an introduction to quantum computation.* Primera de ocho ponencias dadas en la Sociedad Matemática Americana AMS Curso breve sobre Computación Cuántica organizado en conjunción con la Reunión Anual de la AMS en Washington, DC, USA en enero de 2000, y será publicado en el volumen de la AMS PSAPM titulado "Quantum Computation". e-print: quant-ph\0007045.

[4] Oziewicz Zbigniew, *Computación cuántica.* Curso impartido durante el semestre 2001-II para la carrera de Informática.

[5] Steane Andrew, *Quantum computing*; Universidad de Oxford, Inglaterra. Julio de 1997. e-print, arXiv:quant-ph\9708022

[6] Svozil Karl, *Quantum Information: The New Frontier*; Instituto de Física Teórica, Universidad de Tecnología Vienna, Vienna, Austria. 2000.

Capítulo 4

Teoría Clásica de la Computación

Toca el turno a la teoría de la computación. Concerniente a las preguntas "¿qué es calculable?" y "¿qué fuentes son necesarias?"

Las fuentes fundamentales requeridas para la computación son medios para almacenar y manipular símbolos. Las preguntas importantes son cuán complicados son los símbolos, cuántos necesitaremos, cuán complicadas deben ser las manipulaciones, y cuántas de ellas usaremos?

La visión general es que la computación es juzgada *difícil* o ineficiente si la cantidad de fuentes requeridas se incrementa exponencialmente con la medida del tamaño del problema a ser direccionado. El tamaño del problema es dado por la cantidada requerida de *información* que especifica el problema. Aplicando esta idea al nivel más básico, descubrimos que una computadora debe ser capaz de manipular símbolos binarios, no sólo símbolos unarios (la notación unaria tiene un sólo símbolo, 1. Los enteros positivos son escritos 1, 11, 111, 1111,...) de otra manera el número ineluctable de localidades de memoria crecería exponencialmente con la cantidad de información a ser manipulada. Por el otro lado, no es menester trabajar con notación decimal o cualquier otra notación con un 'alfabeto' o con más de dos símbolos. Esto simplifica en gran medida los diseños y análisis de computadoras.

Para manipular n símbolos binarios, no es forzoso manipularlos al mismo tiempo, ya que se puede demostrar que cualquier transformación, manipulando pares de símbolos o de uno en uno daría el mismo resultado. Una

compuerta lógica binaria toma dos bits x, y como entradas, y calcula una función $f(x, y)$. Puesto que f puede ser 0 o 1, y hay cuatro posibles entradas, existen 16 posibles funciones f. Este conjunto de 16 diferentes compuertas lógicas es conocido como un 'conjunto universal', porque al combinar tales compuertas, cualquier transformación de n bits puede ser ejecutada. Además, el resultado de algunas de las 16 compuertas puede ser reproducido al combinar otras, así que no es imperioso todas las 16 compuertas, y de hecho sólo una, la compuerta NAND.

Concatenando compuertas lógicas, podemos manipular símbolos de n bits. Este acercamiento general es conocido como el modelo de red de la computación, y es útil para nuestros propósitos porque sugiere el modelo de computadora cuántica más factible experimentalmente. En este modelo, los componentes esenciales de una computadora son un conjunto de bits, muchas copias de la compuerta lógica universal, y cables conductores.

4.1 La computadora Universal; máquina de Turing

La palabra 'universal' tiene un significado adicional en relación a las computadoras. Turing demostró que es posible construir una computadora *universal*, la cual puede simular la acción de cualquier otra, en el siguiente sentido, Sea $T(x)$ la salida de una máquina de Turing T (figura 5a) que actúa sobre la cinta de entrada x.

Ahora, una máquina de Turing puede ser especificada completamente escribiendo como responde al 0 y al 1 de la cinta de entrada, para cada configuración interna posible de la máquina (de la cual hay un número finito). Esta especificación puede ser escrita como un número binario $d[T]$. Turing demostró que exista una máquina U, conocida como la máquina universal de Turing, con las propiedades

$$U(d[T], x) = T(x) \tag{4.1}$$

y el número de pasos tomados por U para simular cada paso de T es solo una función polinomial (no exponencial) de la longitud de $d[T]$. En otras palabras, si proveemos a U con una cinta de entrada que contenga a una descripción de T y a la entrada x, entonces U calculará la misma función como T lo hubiera hecho, para *cualquier* máquina T, sin ningún retardo

exponencial.

Para completar el argumento, se puede demostrar que otros modelos de computación, tales como el modelo de red, son *equivalentes computacionalmente* al modelo de Turing: ellos permiten el cálculo de las mismas funciones, con la misma eficiencia computacional (ver siguiente sección). Es así que, el concepto de la máquina universal establece que, cierto grado finito de complejidad en la construcción es suficiente, para permitir el procesamiento de información muy general. Este es el resultado fundamental de la ciencia computacional. Ciertamente, la potencia de la máquina de Turing y sus agnadas es tan grande que Church (1936) y Turing (1936) establecen la "tesis Church-Turing", al efecto que

Cada función 'la cual sería naturalmente vista como calculable' puede ser calculada por la máquina universal de Turing.

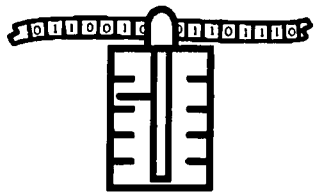


Fig. 5a La máquina de Turing. Esta es un dispositivo mecánico conceptual que al demostrarse es capaz de simular eficientemente todos los métodos clásicos de computación. La máquina tiene un conjunto finito de estados internos, y un diseño definido. Lee un símbolo binario a la vez, puesto en la cinta. La acción de la máquina al leer un símbolo dado s depende sólo de aquel símbolo en el estado interno G. La acción consiste en sobreescribir un nuevo símbolo s' en la localidad actual de la cinta, cambiando el estado a G', y moviendo la cinta una posicción en la dirección d (izquierda o derecha). La construcción interna de la máquina puede ser especificada por medio de una lista finita y bien definida de reglas de la forma $(s, G \rightarrow s', G', d)$.Un estado especial interno es el estado 'detención': una vez en este estado la máquina cesa la actividad. Un 'programa' de entrada en la cinta es transformado por la máquina en un resultado en la salida impreso en la misma.

Esta tesis no está comprobada, pero ha sobrevivido a varios intentos para encontrar un contra-ejemplo, haciéndola un resultado muy poderoso. A ella le debemos la versatilidad de la computadora moderna de propósito general,

porque 'funciones calculables' incluyen tareas tales como procesamiento de palabras, control de procesos, y así sucesivamente.

4.2 Complejidad Computacional

Una vez que ya se establece la idea de una computadora universal, las tareas computacionales pueden ser clasificadas en términos de dificultad de la siguiente manera. Dado un algoritmo, se estima que direccione no sólo un caso del problema, tal como "encontrar el cuadrado de 237," sino una clase del problema, tal como "dada x, encontrar su cuadrado." La cantidad de información dada a la computadora para especificar el problema es $L = \log x$, es decir, el número de bits necesarios para almacenar el valor de x. La *complejidad computacional* del problema está determinada por el número de pasos s que una máquina de Turing debe seguir hasta completar cualquier método algorítmico para solucionar el problema. En el modelo de red, la complejidad es determinada por el número de compuertas lógicas requeridas. Si existe un algoritmo con s dado por cualquier función polinomial de L (ejemplo, s a $L^3 + L$) entonces el problema es juzgado tratable y es puesto en la clase compleja "P". Si s se incrementa exponencialmente con L (ejemplo, s a $2^L = x$) entonces el problema se considera difícil y puesto en otra clase compleja. Algunas veces es más fácil verificar una solución, esto es, probar si es correcta o no, que encontrar alguna. La clase "NP" es el conjunto de problemas para las cuales las soluciones pueden ser verificadas en tiempo polinomial. Obviamente P $\in$ NP, y creeríamos que hay problemas en NP que no están en P, es decir, NP $\neq$ P, pero esto nunca ha sido probado, porque es muy difícil excluir la posible existencia de algunos logaritmos aún no descubiertos. Sin embargo, el punto importante es que la membresía de estas clases no depende del modelo de computación, es decir, la realización física de las computadoras, puesto que la máquina de Turing puede imitar a cualquier otra computadora con solo un retardo polinomial en lugar de exponencial.

Un ejemplo importante de un problema intratable es el de la factorización: dado un número compuesto x, esto es no primo, encontrar uno de sus factores. Si x es par, o múltiplo de cualquier número más pequeño, entonces es fácil encontrar un factor, el caso interesante es cuando los factores primos de x son, en ellos mismos muy grandes. Para este caso no hay un método simple conocido. El método mejor conocido, el de *la criba de número de campo* requiere un número de pasos computacionales del orden

de $s \sim \exp(2L^{1/3}(\log L)^{2/3})$ donde $L = \ln x$. Poniendo a una red substancial de máquinas a esta sola tarea, uno puede factorizar un número de 130 dígitos decimales, esto es $L \simeq 300$, dando $s \sim 10^{18}$. Esto es mucho tiempo, pero es posible (por ejemplo 42 días con 10^{12} operaciones por segundo). Sin embargo, si duplicamos L, s se incrementa hasta $\sim 10^{25}$, ahora el problema es intratable: tomaría un millón de años con la tecnología actual, o requeriría computadoras que corrieran un millón de veces más rápido que las actuales.

El problema de la factorización ha adquirido gran importancia práctica porque está en el centro de sistemas criptográficos ampliamente usados tales como el Rivest, Shamir y Adleman (1979). Para un mensaje dado M (en la forma de un gran número binario), es fácil calcular la versión encriptada $E = M^s \bmod c$, donde s y c son números enteros grandes bien elegidos que pueden hacerse públicos. Para desencriptar el mensaje, el receptor calcula $E^t \bmod c$, que es igual a M para un valor de t el cual puede ser rápidamente deducido a partir de s y los factores de c (Schroeder 1984). En la práctica se escoge que $c = pq$ sea igual al producto de dos números primos grandes p, q conocidos sólo por el usuario quien publicó c, de esta manera sólo ese usuario puede leer los mensajes -a menos que alguien sea capaz de factorizar c. Es una característica muy útil que no es necesario distribuir en el sistema ninguna clave secreta: la 'clave' c, s que permite el encriptamiento es del dominio público.

4.2.1 Funciones no computables

Hay todavía una forma más en la que una tarea puede resultar imposible para una computadora. En la búsqueda por resolver problemas, podemos 'vivir con' un logaritmo lento, pero que tal si no existe? Tales problemas son definidos como *no calculables*. El ejemplo más importante es el 'problema de detención'. Una característica de algunos programas es que nos llevan a ciclos infinitos. Considere, por ejemplo, la instrucción "mientras $x > 2$, dividir x entre 1", para x inicialmente mayor que 2. Se puede ver que este algoritmo nunca va a detenerse, sin nisiquiera correrlo. Un algoritmo más interesante, desde el punto de vista matemático, es "mientras x sea igual a la suma de dos números primos, suma 2 a x", comenzando con $x = 8$. El algoritmo ciertamente es factible. Pero alguna vez se detendrá? Usando tales técnicas, una vasta sección de la teoría matemática y física podría ser reducida a la pregunta "tal algoritmo se detendría si lo corriéramos?" Si encontráramos una forma general de establecer si los logaritmos se detendrán o no, tendríamos una herramienta matemática extremadamente poderosa.

En cierto sentido, resolvería todo lo de matemáticas![Steane, 1997 pg. 19]

Supongamos que es posible encontrar un algoritmo general el cual logrará que cualquier máquina de Turing se detenga para cualquier entrada. Dicho algoritmo resuelve el problema "dado x y $d[T]$, la máquina de Turing T se detendría si tuviera a x como entrada?". Aquí $d[T]$ es la descripción de T. Si tal algoritmo existiera, entonces es posible hacer una máquina de Turing T_H que se detenga si y sólo si $T(d[T])$ no se detiene, donde $d[T]$ sigue siendo la descripción de T. Aquí T_H toma como entrada a $d[T]$, lo cual es suficiente para decirle a T_H a cerca de la máquina de Turing T y la entrada a T. Por lo tanto tenemos

$$T_H(d[T]) \text{ se detiene} \leftrightarrow T(d[T]) \text{ no se detiene} \tag{4.2}$$

hasta aquí todo está bien. Sin embargo, qué pasa si ponemos como entrada de T_H la descripción de ella misma, $d[T_H]$? Entonces

$$T_H(d[T]) \text{ se detiene} \leftrightarrow T_H(d[T]) \text{ no se detiene} \tag{4.3}$$

Lo cual es una contradicción. Con este argumento Turing demostró que no hay medios automáticos de establecer si las máquinas de Turing se detendrán, en general: el "problema de detención" es no computable. Esto implica que las matemáticas, y el procesamiento de información, son un cuerpo rico de ideas diferentes que no pueden ser resumidos en un gran algoritmo.

Bibliografía

[1] Steane Andrew, *Quantum computing*; Universidad de Oxford, Inglaterra. Julio de 1997. e-print, arXiv:quant-ph\9708022

Capítulo 5

Conceptos Básicos de la Teoría Cuántica

La "cuantización" fue presentada por Max Karl Ernst Ludwig Planck alrededor de 1900. A groso modo, Planck asumió una *discretización* de la energía total U_N de N osciladores lineales ("resonadores"),

$$U_N = P_\epsilon \in \{0, \epsilon, 2\epsilon, 3\epsilon, 4\epsilon, \dots\},$$

de donde $P \in \mathrm{N}_0$ es cero o un entero positivo y ϵ es *el cuanto más pequeño de energía.* ϵ es una función lineal de la frecuencia ω y proporcional a la constante fundamental de Planck $\hbar \approx 10^{-34}\mathrm{J} \cdot \mathrm{s}$; esto es,

$$\epsilon = \hbar\omega$$

En extensión al modelo de energía del resonador discretizado, Einstein propuso la cuantización del campo electromagnético [Svozil, 2000 pg. 254]. Acorde a la hipótesis cuántica de la luz, la energía en un campo eléctrico caracterizado por la frecuencia ω puede ser producido, absorbido e intercambiado sólo en un número discreto n de "paquetes" o "cuantos" o "fotones"

$$E_N = n\hbar\omega \ , \ n = 0, 1, 2, 3, \dots$$

Por el otro lado, la paradoja del gato de Schrödinger postula la existencia del qubit, además de ser la clave fundamental para entender la naturaleza de todo:

Considérese una caja, un gato y un recipiente con ácido, poniendo los tres elementos dentro de la caja, la pregunta es la siguiente, el gato está vivo

o está muerto? NO lo sabemos a menos que abramos la caja y comprobemos como está el gato, pero sin hacerlo, para nosotros, el gato está tanto vivo como muerto.

Se presentarán las ideas de ésta teoría pero solamente como preludio.

5.1 Espacio de Hilbert

Definición:
Un espacio de Hilbert es una pareja de $\mathbb{C}$-espacios $\mathcal{H}$, con h: $\bar{\mathcal{H}} \to \mathcal{H}^*$ con las condiciones: $h = h^+$ y $\exists\ h^{-1}$. En donde $\langle\ |\ \rangle \approx h$, se le conoce como estructura hilbertiana y h^+ indica conjugación compleja.

$$\mathcal{H} \xrightarrow{h} \mathcal{H}^+$$

ó

$$\bar{\mathcal{H}} \xrightarrow{\bar{h}} \mathcal{H}^*$$

El espacio de Hilbert, se describe de mejor manera, como un objeto en una categoría de $\mathbb{C}$-espacios, con la elección de un morfismo $h = h^+$,

$$\begin{array}{ccc} \mathcal{H} & \xrightarrow{h} & \mathcal{H}^+ \\ - \downarrow & & \downarrow - \\ \bar{\mathcal{H}} & \xrightarrow{\bar{h}} & \mathcal{H}^* \end{array}$$

Donde,
$\mathcal{H}$ es un $\mathbb{C}$-espacio vectorial,
$\mathcal{H}^*$ es el $\mathbb{C}$-espacio Dual de $\mathcal{H}$ (contiene las mediciones de $\mathcal{H}$),
$\bar{\mathcal{H}}$ es el complejo conjugado del $\mathbb{C}$-espacio,

$\mathcal{H}^+$ es el $\mathbb{C}$-espacio dual de $\bar{\mathcal{H}}$ y contiene sus mediciones (Hermite).

El número de espacios vectoriales es de cuatro porque hay dos funtores, uno de los cuales es el funtor dualidad y el otro el funtor conjugado.

Al morfismo $h = h^+ : \mathcal{H} \to \mathcal{H}^+$ se le conoce como estructura de Hilbert. A la pareja $(\mathcal{H}, h)$ se le llama $\mathbb{C}$-espacio de Hilbert.

Una conclusión importante es que un qubit puro solo está en el espacio de Hilbert.

Un espacio de Hilbert está completo en la norma

$$||u|| = \sqrt{(u,u)}$$

inducida por el producto interno valuado en los números complejos, es decir, con una estructura de Hilbert o Hermiciana la cual se asemeja al producto punto de la geometría euclideana [Lomonaco Jr., 2001 pg. 7].

Observación. El producto interno valuado en los complejos, se refiere a un mapeo

$$h : \bar{\mathcal{H}} \otimes \mathcal{H} \to \mathbb{C}$$

Los elementos de un espacio de Hilbert $\mathcal{H}$ serán llamados **vectores ket, estados ket**, o simplemente **kets**.

Sea $\mathcal{H}^*$ la notación para denotar el $\mathbb{C}$-espacio de todos los morfismos del $\mathbb{C}$-espacio de $\mathcal{H}$ en el anillo de los números complejos $\mathbb{C}$, esto es,

$$\mathcal{H}^* = Hom_{\mathbb{C}}(\mathcal{H}, \mathbb{C})$$

Los elementos de $\mathcal{H}^*$ serán llamados **vectores bra, estados bra** o **bras**.

5.1.1 Definición: Estado

Es una descripción completa de un sistema físico. Un estado puro Ψ es un elemento del $\mathbb{C}$-espacio de Hilbert $\mathcal{H}$ y está representado por un ket estado $|\Psi\rangle$, $|\Psi\rangle \in \mathcal{H}$.

Ejemplos

Como ilustración de los conceptos anteriores, consideremos los estados de polarización de un fotón.

Los estados de polarización de un fotón están representados como kets estado en un $\mathbb{C}$-espacio $\mathcal{H}$ de dos dimensiones. Una base ortonormal de $\mathcal{H}$ consiste en los kets

$$|\circlearrowleft\rangle \quad \text{y} \quad |\circlearrowright\rangle$$

los cuales representan, respectivamente, los estados cuánticos de los fotones polarizados circularmente a la izquierda y derecha.

Otra base ortonormal consiste en los kets

$$|\updownarrow\rangle \quad \text{y} \quad |\leftrightarrow\rangle$$

que representan a los fotones polarizados linealmente, en forma vertical y horizontal respectivamente. Y todavía otra base ortonormal consiste en los kets

$$|\nearrow\rangle \quad \text{y} \quad |\searrow\rangle$$

para los fotones polarizados linealmente a los ángulos $\theta = \pi/4$ y $\theta = -\pi/4$ con respecto a la vertical, respectivamente.

Estas bases ortonormales se relacionan como sigue:

$$\begin{cases} |\nearrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle + |\leftrightarrow\rangle) \\ |\searrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle - |\leftrightarrow\rangle) \end{cases} \qquad \begin{cases} |\nearrow\rangle = \frac{1+i}{2}|\circlearrowleft\rangle + \frac{1-i}{2}|\circlearrowright\rangle \\ |\searrow\rangle = \frac{1-i}{2}|\circlearrowleft\rangle + \frac{1+i}{2}|\circlearrowright\rangle \end{cases}$$

$$\begin{cases} |\updownarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\searrow\rangle) \\ |\leftrightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\searrow\rangle) \end{cases} \qquad \begin{cases} |\updownarrow\rangle = \frac{1}{\sqrt{2}}(|\circlearrowleft\rangle + |\circlearrowright\rangle) \\ |\leftrightarrow\rangle = \frac{i}{\sqrt{2}}(|\circlearrowleft\rangle - |\circlearrowright\rangle) \end{cases}$$

$$\begin{cases} |\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle - i|\leftrightarrow\rangle) \\ |\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle + i|\leftrightarrow\rangle) \end{cases} \qquad \begin{cases} |\circlearrowleft\rangle = \frac{1-i}{2}|\nearrow\rangle + \frac{1+i}{2}|\searrow\rangle \\ |\circlearrowright\rangle = \frac{1+i}{2}|\nearrow\rangle + \frac{1-i}{2}|\searrow\rangle \end{cases}$$

Los productos bra-ket de los kets de polarización se muestran en la tabla:

	$\lvert\updownarrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\searrow\rangle$	$\lvert\circlearrowleft\rangle$	$\lvert\circlearrowright\rangle$
$\langle\updownarrow\rvert$	1	0	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$
$\langle\leftrightarrow\rvert$	0	1	$\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$	$-\frac{i}{\sqrt{2}}$	$\frac{i}{\sqrt{2}}$
$\langle\nearrow\rvert$	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$	1	0	$\frac{1-i}{2}$	$\frac{1+i}{2}$
$\langle\searrow\rvert$	$\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$	0	1	$\frac{1+i}{2}$	$\frac{1-i}{2}$
$\langle\circlearrowleft\rvert$	$\frac{1}{\sqrt{2}}$	$\frac{i}{\sqrt{2}}$	$\frac{1+i}{2}$	$\frac{1-i}{2}$	1	0
$\langle\circlearrowright\rvert$	$\frac{1}{\sqrt{2}}$	$-\frac{i}{\sqrt{2}}$	$\frac{1-i}{2}$	$\frac{1+i}{2}$	0	1

En términos de las bases $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ y las bases duales $\{\langle\updownarrow|, \langle\leftrightarrow|\}$, estos kets y bras pueden ser escritos como matrices:

$$\begin{cases} \langle\updownarrow| = \begin{pmatrix} 1 & 0 \end{pmatrix}, & |\updownarrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \langle\leftrightarrow| = \begin{pmatrix} 0 & 1 \end{pmatrix}, & |\leftrightarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{cases}$$

$$\begin{cases} \langle\nearrow| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \end{pmatrix}, & |\nearrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \langle\nwarrow| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \end{pmatrix}, & |\nwarrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{cases}$$

$$\begin{cases} \langle\circlearrowright| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \end{pmatrix}, & |\circlearrowright\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix} \\ \langle\circlearrowleft| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \end{pmatrix}, & |\circlearrowleft\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \end{cases}$$

En estas bases, por ejemplo,

$$|\nearrow\circlearrowright\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ 1 \\ -i \end{pmatrix}$$

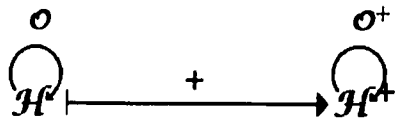
$$|\circlearrowright\rangle\langle\circlearrowleft| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$$

5.2 Operadores

Un **operador (lineal)** o una **transformación** $\mathcal{O}$ sobre un ket espacio $\mathcal{H}$ es un morfismo del espacio de Hilbert de $\mathcal{H}$ en $\mathcal{H}$, esto es un elemento de

$$Hom_{\mathbf{C}}(\mathcal{H}, \mathcal{H})$$

Lo **adjunto** $\mathcal{O}^+$ del operador $\mathcal{O}$ es el operador que



para todo $|\psi_1\rangle \in \mathcal{H}^+$ y $|\psi_2\rangle \in \mathcal{H}$.

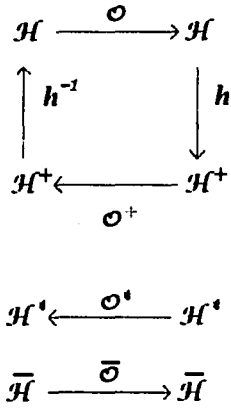
Análogamente, un operador (lineal) o transformación sobre un bra espacio $\mathcal{H}^*$ es un elemento de

$$Hom_{\mathbf{C}}(\mathcal{H}^*, \mathcal{H}^*)$$

5.3 Observables

En la mecánica cuántica un observable es simplemente un operador **Hermitiano** (también llamado **auto-adjunto**) sobre un $\mathbb{C}$-espacio $\mathcal{H}$, es decir, un operador $\mathcal{O}$ tal que

$$\mathcal{O}^+ \circ h = h \circ \mathcal{O}$$



Esto a partir del primer diagrama, se obtiene: $h^{-1} \circ \mathcal{O}^+ \circ h = \mathcal{O}$.

Definiciones:
Un **eigenvalor** a de un operador A es un número complejo para el cual hay un ket $|\psi\rangle$ tal que,

$$A|\psi\rangle = a|\psi\rangle.$$

El ket $|\psi\rangle$ es conocido como **eigenket** de A que corresponde al eigenvalor a.

Un teorema importante sobre observables se escribe a continuación:

Teorema. Los eigenvalores a_i de un observable A son todos números reales. Además, los eigenkets para distintos eigenvalores de un observable

son ortogonales.

Definición. Un eigenvalor es *degenerado* si hay al menos dos eigenkets linealmente independientes para dicho eigenvalor. De otra forma, es *no-degenerado.*

Ahora, si todos los eigenvalores a_i de un observable A son no-degenerados, entonces se puede etiquetar a los eigenkets de A con los eigenvalores a_i correspondientes. Así, se escribe:

$$A|a_i\rangle = a_i|a_i\rangle$$

para cada eigenvalor a_i.

Una excepción notable de lo anterior es el **operador de medición**

$$|a_i\rangle \otimes \langle a_i|$$

para el eigenvalor a_i, el cual es el producto tensorial del ket$|a_i\rangle$ con su adjunto el bra $\langle a_i|$, donde se asume que $|a_i\rangle$ (y por tanto, $\langle a_i|$) es unitario. Contiene dos eigenvalores 0 y 1. 1 es un eigenvalor no-degenerado con el eigenket $|a_j\rangle$. 0 es un eigenvalor degenerado con los correspondientes eigenkets $\{|a_i\rangle\}_{j\neq i}$

Definición: Un observable A se dice que está **completo** si sus eigenkets $|a_i\rangle$ forman una base del $\mathbb{C}$-espacio de Hilbert $(\mathcal{H}, h)$. Ya que, por convención todos los eigenkets son elegidos con longitud unitaria, produce que los eigenkets de un observable completo no-degenerado A formen una base ortonormal del $\mathbb{C}$-espacio de Hilbert subyacente.

Ejemplo. Las matrices de Pauli, para $\dim_{\mathbb{C}}\mathcal{H} = 2$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \in Hom(\mathcal{H}, \mathcal{H})$$

Son ejemplos de observables que con frecuencia aparecen en computación y mecánica cuántica.

Sus eigenvalores y eigenkets se describen en la siguiente tabla:

Matrices de Pauli	*Eigenvalor:Eigenket*	
$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$+1$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
	-1	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$+1$	$\frac{\|0\rangle + i\|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$
	-1	$\frac{\|0\rangle - i\|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$
$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$+1$	$\|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
	-1	$\|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

5.4 Mediciones

En esta Sección, A denotará a un observable completo no degenerado con eigenvalores a_i y eigenkets $|a_i\rangle$.

El resultado de una medición del observable A de un sistema cuántico $\mathcal{Q}$ el cual está en el estado $|\psi\rangle$ antes de la medición puede ser representado diagramáticamente como:

$$|\psi\rangle = \sum_i |a_i\rangle\langle a_i \mid \psi\rangle \quad \overset{\text{1a med. de } A}{\underset{Prob = \|\langle a_j \mid \psi\rangle\|^2}{\Longrightarrow}} \quad a_j|a_j\rangle \quad \approx \quad |a_j\rangle \quad \overset{\text{2a med. de } A}{\underset{Prob = 1}{\Longrightarrow}} \quad |a_j\rangle$$

Nótese que el valor medido es el eigenvalor a_j con probabilidad $\|\langle a_j|\psi\rangle\|^2$. Si la misma medición se repite en el sistema cuántico $\mathcal{Q}$ después de la primera, el resultado de la segunda medición ya no es estocástico. Produce el valor medido a_j previamente y el estado $\mathcal{Q}$ permanece igual, es decir, $|a_j\rangle$.

El observable

$$|a_i\rangle\langle a_i|$$

con frecuencia es llamado **operador de medición selectiva** (o una **filtración**) para a_i. Como fue mencionado, tiene dos eigenvalores 0 y 1. 1 es un eigenvalor no-degenerado con eigenket $|a_j\rangle$, y 0 es un eigenvalor degenerado con eigenket $\{|a_j\rangle\}_{j\neq i}$.

Así,

$$|\psi\rangle \quad \overset{\text{Medición de } |a_i\rangle\langle a_i|}{\underset{Prob = \|\langle a_i \mid \psi\rangle\|^2}{\Longrightarrow}} \quad 1 \cdot |a_i\rangle = |a_i\rangle \ ,$$

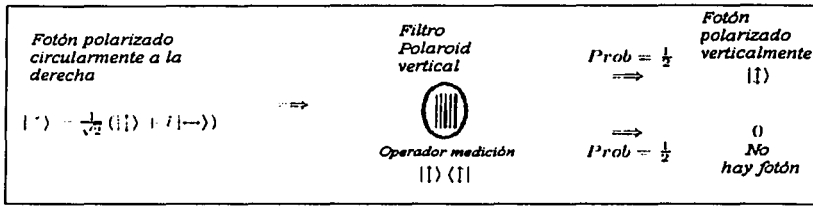
pero para $j \neq i$,

$$|\psi\rangle \quad \overset{\text{Medición de } |a_i\rangle\langle a_i|}{\underset{Prob = \|\langle a_j \mid \psi\rangle\|^2}{\Longrightarrow}} \quad 0 \cdot |a_j\rangle = 0$$

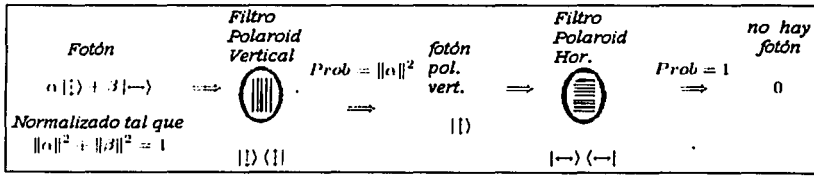
5.4.1 Ejemplos de medición cuántica

Podemos aplicar los principios anteriores de medición a la luz polarizada. Tres ejemplos se presentan a continuación:

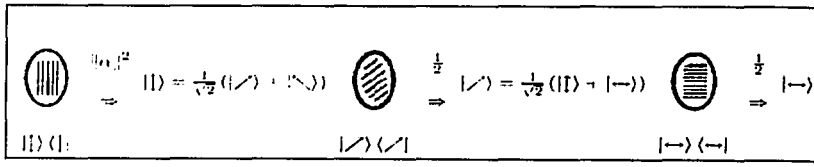
Ejemplo 1.



Ejemplo 2. Un filtro polarizado verticalmente seguido por un filtro polarizado horizontalmente.



Ejemplo 3. Pero si insertamos un filtro diagonalmente polarizado (45° con respecto a la vertical) entre los dos filtros polarizados en el ejemplo anterior, tenemos:



donde la entrada al primer filtro es $\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle$.

5.5 El Principio de Incertidumbre

Cuando se intenta aplicar la mecánica y la electrodinámica clásicas a la explicación de los fenómenos atómicos, ambas conducen a resultados que se encuentran en abierta contradicción con la experiencia. Un ejemplo muy claro de esto lo proporciona ya la contradicción a que se llega al aplicar la electrodinámica ordinaria al modelo del átomo en el que los electrones se mueven en torno del núcleo siguiendo órbitas clásicas. En este movimiento, como en cualquier movimiento acelerado de las cargas, los electrones deberían radiar continuamente ondas electromagnéticas. Con la radiación los electrones perderían su energía y esto debería conducir, en último término, a su caída sobre el núcleo. Así pues, según la electrodinámica clásica el átomo sería inestable, lo que en modo alguno corresponde a la realidad. [Lifshitz, 1975 pg. 1]

Existe esta contradicción entre, lo que en teoría, nuestro sentido común nos dice, y el experimento; hay entonces, una teoría aplicable a los fenómenos atómicos, esto es, a fenómenos que ocurren con partículas de masa muy pequeña y en muy pequeñas regiones del espacio, exige un cambio esencial en las leyes y nociones fundamentales de las teorías clásicas. El mejor ejemplo para comprenderlo es adoptar un fenómeno observado experimentalmente, la llamada difracción de los electrones. Cuando un haz homogéneo de electrones atraviesa un cristal, a la salida del mismo se observa una figura constituida por máximos y mínimos de intensidad consecutivos del todo análoga a la figura de difracción que se observa en la difracción de las ondas electromagnéticas. Así, en ciertas condiciones el comportamiento de las partículas materiales -de los electrones- presenta rasgos típicos de los procesos ondulatorios, por lo que son conocidos como: ondas de materia.

El siguiente experimento ideal, que corresponde a una esquematización de tal difracción electrónica por un cristal, pone claramente de manifiesto hasta qué punto es profunda la contradicción entre este fenómeno y las nociones ordinarias acerca del movimiento. Imaginemos una pantalla que no se deja atravesar por los electrones y en la cual se han hecho dos rendijas. Si se observa el paso del haz de electrones por una de ellas, cuando la otra rendija permanece cerrada, obtenemos sobre una pantalla plana colocada detrás de la rendija una cierta figura de distribución de la intensidad; de la misma manera obtenemos otra figura abriendo la segunda rendija y cerrando la primera. En cambio, observando el paso del haz simultáneamente por las dos rendijas, de acuerdo con las ideas ordinarias, deberíamos esperar una

figura consistente en la simple superposición de las dos anteriores, ya que cada electrón, moviéndose en su trayectoria, pasa por una de las rendijas sin ejercer influencia alguna sobre los electrones que pasan por la otra. El fenómeno de la difracción electrónica muestra, sin embargo, que en realidad se obtiene una figura de difracción que, gracias a la interferencia, de ningún modo se reduce a la suma de las figuras dadas por cada una de las rendijas por separado. Es claro que este resultado en manera alguna se puede conciliar con el concepto de movimiento de los electrones a lo largo de una trayectoria. El esquema del experimento es presentado en la figura 3a.

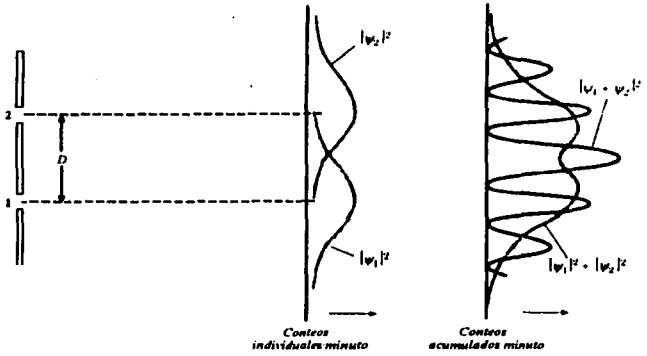


Fig. 3a La curva verde sobre la derecha representa el patrón acumulado de conteos por minuto cuando cada rendija se cierra a la mitad del tiempo. La curva negra representa el patrón de difracción con ambas rendijas abiertas al mismo tiempo.

Resulta así que la mecánica a la que obedecen los fenómenos atómicos -la llamada *mecánica ondulatoria o cuántica*-, debe basarse en nociones acerca del movimiento, diferentes en esencia, de las ideas de la mecánica clásica. En la mecánica cuántica no existe el concepto de trayectoria de una partícula.

La posibilidad de una descripción cuantitativa del movimiento de un electrón exige la existencia de objetos físicos que, con precisión suficiente, obedecen a la mecánica clásica. Si el electrón entra en interacción con el "objeto clásico", el estado de éste, en general, cambia. En tales circunstancias el objeto clásico se suele llamar *aparato* y del proceso de su interacción con el electrón se suele decir que se trata de una *medición.*

Ahora, el problema que se plantea la teoría cuántica consiste en predecir el resultado de una medición partiendo del resultado conocido de mediciones anteriores, y además considera, dentro de sus límites de aplicabilidad, que siempre es posible realizar la medición de las coordenadas de un electrón con precisión arbitraria.

Pero mientras en mecánica clásica una partícula posee en cada instante unas coordenadas y una velocidad determinadas, en mecánica cuántica las cosas ocurren de una manera completamente distinta. Si como resultado de una medida se atribuyen determinadas coordenadas al electrón, en tales condiciones no posee absolutamente ninguna velocidad determinada. Recíprocamente, si el electrón posee una velocidad determinada, no puede tener una posición determinada en el espacio.

Esta circunstancia constituye el contenido del llamado principio de indeterminación -uno de los conceptos fundamentales de la mecánica cuántica descubierto por Werner Heisenberg en 1927.

5.6 La matriz densidad

Además de los estados puros existen estados que no son puros y hay otra forma de representar a ambos estados cuánticos.

Sea $|\psi\rangle$ un ket de longitud unitaria (esto es, $\langle\psi|\psi\rangle = 1$) en el espacio de Hilbert $\mathcal{H}$ representando al estado de un sistema cuántico. Es decir, $|\psi\rangle \in \mathcal{H}$ y $\langle\psi| \in \mathcal{H}^+$. La **matriz densidad u operador densidad** ρ asociado con el ket estado $|\psi\rangle$ está definido como el producto tensorial del ket $|\psi\rangle$ (el cual puede ser visto como el vector columna) con el bra $\langle\psi|$ (el cual puede verse como un vector renglón), esto es,

$$\rho = |\psi\rangle \otimes \langle\psi|, \quad \in \mathcal{H} \otimes \mathcal{H}^*$$

Es importante aclarar que $\langle\psi| \in \mathcal{H}^*$ siempre en la definición del operador densidad. Esto es a causa de la notación de Dirac.

El formalismo de la matriz densidad tienen un número de ventajas sobre el formalismo del estado ket. Una ventaja es que el operador densidad puede ser usado para representar estados clásicos/cuánticos, es decir, estados que son una mezcla estadísticamente clásica de los estados cuánticos. Tales estados híbridos pueden considerarse como estados cuánticos para los cuales

no tenemos información completa.

Por ejemplo, considérese un sistema cuántico el cual se encuentra en los estados (cada uno de longitud unitaria)

$$|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$$

con probabilidades

$$p_1, p_2, \cdots, p_n$$

respectivamente, donde

$$p_1 + p_2, \cdots + p_n = 1$$

(nótese que los estados $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ no necesitan ser ortogonales.)Entonces la representación del operador densidad de este estado se define como

$$\rho = p_1|\psi\rangle \otimes \langle\psi_1| + p_2|\psi_2\rangle \otimes \langle\psi_2| + \cdots + p_n|\psi_n\rangle \otimes \langle\psi_n|$$

tomando en cuenta que se trata de operaciones con el producto tensorial,

$$\rho = p_1|\psi\rangle\langle\psi_1| + p_2|\psi_2\rangle\langle\psi_2| + \cdots + p_n|\psi_n\rangle\langle\psi_n|$$

Si una matriz densidad ρ puede ser escrita en la forma:

$$\rho = |\psi\rangle\langle\psi|,$$

se dice que representa a un **grupo puro**. Por el otro lado, se dice que representa a un **grupo mezclado** [Lomonaco Jr. 2000, pg. 21].

Se puede demostrar que un operador densidad representa a un estado puro si y solo si $\rho^2 = \rho$, o en forma equivalente, si y solo si $Trace(\rho^2) = 1$. Para todos los estado, ambos puros y mezclados, $Trace(\rho^2) \leqslant 1$.

En breve, la matriz densidad cumple con estas tres condiciones:

1. $h \circ \rho = \rho^+ \circ h$
2. $Tr\ \rho = 1$
3. $Tr\ \rho^2 \leqslant 1$

Y en realidad, la matriz densidad representa de mejor manera a los estados mezclados, puesto que es muy difícil encontrar a los estados totalmente puros para implementarlos de forma práctica. Esto nos lleva a temas para el operador espín-densidad [Oziewicz, 1984] en donde el operador densidad es descrito por medio de un conjunto de parámetros independientes, tales como la población, el grado de orientación y las direcciones de orientación para sistemas de partículas.

Teorema: Un resultado es que, para un qubit se cumple, si $\dim_{\mathbb{C}}\mathcal{H} = 2$

$$2(\rho^2 - \rho) = Tr\ \rho^2 - 1$$

Problema. Encontrar la analogía de esta igualdad para n-qubits, para $\dim_{\mathbb{C}}\mathcal{H} \geqslant 2$.

5.6.1 Ejemplos de operadores densidad.

Consideremos los siguientes grupos o estados mezclados del estado de polarización de un fotón:

Ejemplo 1.

Ket	$\lvert\updownarrow\rangle$	$\lvert\nearrow\rangle$
Prob.	$\frac{3}{4}$	$\frac{1}{4}$

En términos de las bases $|\leftrightarrow\rangle$, $|\updownarrow\rangle$ del $\mathbb{C}$-espacio de Hilbert $\mathcal{H}$ de dimensión dos, el operador densidad ρ del estado mezclado anterior puede ser escrito como:

$$\begin{aligned}\rho &= \tfrac{3}{4}|\updownarrow\rangle\langle\updownarrow| + \tfrac{1}{4}|\nearrow\rangle\langle\nearrow| \\ &= \tfrac{3}{4}\begin{pmatrix}1\\0\end{pmatrix}(1 \quad 0) + \tfrac{1}{4}\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}(1/\sqrt{2} \quad 1/\sqrt{2}) \\ &= \tfrac{3}{4}\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} + \tfrac{1}{8}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix} = \begin{pmatrix}\frac{7}{8} & \frac{1}{8}\\ \frac{1}{8} & \frac{1}{8}\end{pmatrix}\end{aligned}$$

Ejemplo 2. Las siguientes dos *preparaciones* producen estados mezclados con el mismo operador densidad:

Ket	$\lvert\updownarrow\rangle$	$\lvert\leftrightarrow\rangle$
Prob.	$\frac{1}{2}$	$\frac{1}{2}$

y

Ket	$\lvert\nearrow\rangle$	$\lvert\nwarrow\rangle$
Prob.	$\frac{1}{2}$	$\frac{1}{2}$

Para la preparación de la izquierda, tenemos

$$\begin{aligned}\rho &= \tfrac{1}{2}|\updownarrow\rangle\langle\updownarrow| + \tfrac{1}{2}|\leftrightarrow\rangle\langle\leftrightarrow| \\ &= \tfrac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}(1 \quad 0) + \tfrac{1}{2}\begin{pmatrix}0\\1\end{pmatrix}(0 \quad 1) \\ &= \tfrac{1}{2}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\end{aligned}$$

Y para la preparación de la derecha, tenemos

$$\begin{aligned}\rho &= \tfrac{1}{2}|\nearrow\rangle\langle\nearrow| + \tfrac{1}{2}|\nwarrow\rangle\langle\nwarrow| \\ &= \tfrac{1}{2}\tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}\tfrac{1}{\sqrt{2}}(1 \quad 1) + \tfrac{1}{2}\tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\tfrac{1}{\sqrt{2}}(1 \quad -1) \\ &= \tfrac{1}{4}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix} + \tfrac{1}{4}\begin{pmatrix}1 & -1\\-1 & 1\end{pmatrix} = \tfrac{1}{2}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\end{aligned}$$

No hay forma de distinguir físicamente los dos estados mezclados anteriores los cuales fueron preparados en dos formas completamente diferentes. El operador densidad representa todo lo que puede ser conocido sobre el estado del sistema cuántico.

5.7 El principio de superposición

Sea q el conjunto de las coordenadas del sistema cuántico (en el espacio de fase como dominio) y dq el producto de las diferenciales de estas coordenadas. A dq se le conoce como elemento de volumen del *espacio de configuraciones* del sistema; para una partícula dq con el elemento de volumen dV del espacio ordinario.

El elemento básico del formalismo matemático de la mecánica cuántica consiste en el hecho de que cada estado del sistema se puede describir, en un instante dado, por una determinada función (compleja) de las coordenadas $\psi(q)$, de forma tal que el cuadrado del módulo de esta función determina la distribución de probabilidades de los valores de las coordenadas: $|\psi|^2 dq$ es la probabilidad de que al realizar una medición de las coordenadas del sistema los valores de éstas pertenezcan al elemento dq del espacio de configuraciones; además: $|\psi|^2 = \psi^*\psi$ -en donde: ψ^* es el complejo conjugado de ψ-. La función ψ se llama *función de onda* del sistema (a veces se le llama también *amplitud de probabilidad*).

La función de onda ψ permite calcular las probabilidades de los diferentes resultados de cualquier otra medición (diferente a medir coordenadas). En todos estos casos las probabilidades se definen por expresiones que son bilineales respecto de ψ y ψ^*. La forma más general de una expresión de este tipo es

$$\int\int \psi(q)\psi^*(q')\phi(q,q')dqdq', \tag{5.1}$$

donde la función $\phi(q,q')$ depende del género y del resultado de la medición y la integración se extiende a todo el espacio de configuraciones. La propia probabilidad $\psi\psi^*$ de los diferentes valores de las coordenadas es también una expresión de este tipo. La suma de las probabilidades de todos los posibles valores de las coordenadas de un sistema debe ser, por definición [Lifshitz, 1975 pg. 8], igual a la unidad. Por lo tanto el resultado de la integración de $|\psi|^2$ en todo el espacio sea igual a uno:

$$\int |\psi|^2 dq = 1 \tag{5.2}$$

A continuación se enuncian una serie de proposiciones relativas a las propiedades de la función de onda [Lifshitz, 1975 pg. 8].

Supongamos que en el estado caracterizado por la función de onda $\psi_1(q)$ se efectúa una medición que conduce con certeza a un determinado resultado (resultado 1)y que al hacerlo en el estado $\psi_2(q)$ conduce al resultado 2, se admite entonces que toda combinación lineal de ψ_1 y ψ_2, esto es, toda función de la forma $c_1\Psi_1 + c_2\Psi_2$ (con c_1, c_2 constantes), representa un estado en el que la misma medición puede dar o el resultado 1 o el resultado 2. Además, cabe afirmar que si conocemos la dependencia de los estados respecto del tiempo, dependencia que en un caso viene dada por tal función $\psi_1(q,t)$ y en el otro por la $\psi_2(q,t)$, cualquier combinación lineal da también la dependencia posible de un estado con relación al tiempo. Estas proposiciones se generalizan a un número cualquiera de estados distintos.

El conjunto de estas proposiciones constituye el llamado *principio de superposición de los estados.* De él se sigue inmediatamente, en particular, que todas las ecuaciones a las que satisfacen las funciones de onda deben ser lineales respecto a ψ.

Toda esta interpretación de las ondas de materia -onda y partícula a la vez- fue sugerido por Max Born en 1927. En el mismo año, Erwin

Schrödinger propusó una ecuación de onda que describe la forma en la cual las ondas de materia cambian en el espacio y en el tiempo.

5.8 La ecuación de onda de Schrödinger

Toda función de onda debe satisfacer la ecuación de Schrödinger [Serway, 1997 pg. 1241]. La forma general de la ecuación de onda para las ondas que se desplazan a lo largo del eje x es:

$$\frac{\partial^2\psi}{\partial x^2} = \frac{1}{v^2}\frac{\partial^2\psi}{\partial t^2} \tag{5.3}$$

donde v es la rapidez de la onda y donde la función de onda ψ depende de x y t. Aquí se utiliza ψ en lugar de y por tratarse de la onda de De Broglie.

Para describir las ondas de De Broglie, se considera un sistema con energía total E constante. Puesto que $E = hf$, la frecuencia de la onda De Broglie asociada a la partícula permanece también constante. En este caso la función de onda $\psi(x,t)$ se expresa como el producto de un término que depende únicamente de x y otro que depende sólo de t. Esto es,

$$\psi(x,t) = \psi(x)\cos(\omega t) \tag{5.4}$$

Esto es análogo al caso de las ondas estacionarias en una cuerda, donde la función de onda se representa por $y(x,t) = y(x)cos\omega t$. La parte dependiente de la frecuencia de la función de onda es sinusoidal ya que la frecuencia se conoce con precisión. Sustituyendo la ecuación 5.4 en 5.3 produce

$$\begin{aligned}\cos(\omega t)\frac{\partial^2\psi}{\partial x^2} &= -\left(\frac{\omega^2}{v^2}\right)\psi\cos(\omega t)\\ \frac{\partial^2\psi}{\partial x^2} &= -\left(\frac{\omega^2}{v^2}\right)\psi\end{aligned} \tag{5.5}$$

y como $\omega = 2\pi f = 2\pi v/\lambda$, y para las ondas de De Broglie, $p = h/\lambda$. Por tanto,

$$\frac{\omega^2}{v^2} = \left(\frac{2\pi}{\lambda}\right)^2 = \frac{4\pi^2}{h^2}p^2 = \frac{p^2}{\hbar^2}$$

Se puede expresar la energía total E como la suma de la energías cinética y potencial:

$$E = K + U = \frac{p^2}{2m} + U,$$

$$p^2 = 2m(E-U),$$

$$\frac{\omega^2}{v^2} = \frac{p^2}{\hbar^2} = \frac{2m}{\hbar^2}(E-U),$$

Sustituyendo este resultado en la ecuación 5.5 da

$$\boxed{\frac{\partial^2\psi}{\partial x^2} = -\frac{2m}{\hbar^2}(E-U)\psi} \tag{5.6}$$

Esta es la ecuación de Schrödinger, independiente del tiempo, tal y como se aplica a un partícula confinada a moverse a lo largo del eje x.

5.9 Espín

El concepto más importante en la construcción de las compuertas cuánticas, es el del espín de las partículas, aquí presentado en forma abreviada.

El campo magnético producido por una corriente en una bobina nos brinda un indicio de lo que podría provocar que ciertos materiales muestren fuertes propiedades magnéticas. En general, cualquier espira de corriente tiene un campo magnético y un momento magnético correspondiente. De manera similar, los momentos magnéticos en una substancia magnetizada pueden describirse como si surgieran de corrientes internas a nivel atómico. Para los electrones que se mueven en torno al núcleo, lo anterior es consistente con el modelo de Bohr, después de modificar los números cuánticos [Serway, 1997 pg. 882]. También hay momento magnético intrínseco para electrones, protones, neutrones y otras partículas que sólo puede modelarse aproximadamente como si surgieran de cargas en rotación.

En el modelo clásico del átomo, un electrón orbital constituye una delgada espira de corriente, debido a que es una carga en movimiento, y el momento magnético atómico se asocia a su movimiento orbital. Aunque este modelo tiene muchas deficiencias, sus predicciones concuerdan bien con la teoría cuántica.

Consideremos un electrón que se mueve con velocidad constante v en una órbita circular de radio r alrededor del núcleo, como en la figura 3b. Debido a que el electrón recorre una distancia de $2\pi r$ (la circunferencia del círculo) en un tiempo T, donde T es el tiempo para una revolución, su velocidad orbital es $v = 2\pi r/T$. La corriente efectiva asociada a este electrón orbital

es igual a su carga dividiva por el tiempo correspondiente a una revolución. Al emplear $T = 2\pi/\omega$ y $\omega = v/r$, tenemos

$$I = \frac{e}{T} = \frac{e\omega}{2\pi} = \frac{ev}{2\pi r} \tag{5.7}$$

El momento magnético asociado con esta espira de corriente efectiva es $\mu = IA$, donde $A = \pi r^2$ es el área de la órbita. Por tanto,

$$\mu = IA = \left(\frac{ev}{2\pi r}\right)\pi r^2 = \tfrac{1}{2}evr \tag{5.8}$$

Ya que la magnitud del momento angular orbital del electrón es $L = mvr$, el momento magnético puede escribirse como

$$\mu = \left(\frac{e}{2m}\right)L \tag{5.9}$$

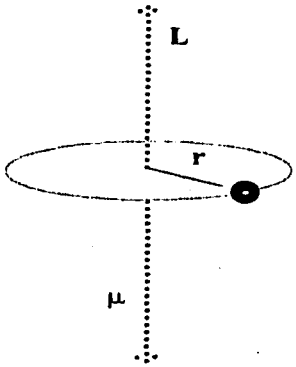


Fig. 3b. Un electrón que se mueve en una órbita circular de radio r tiene un momento angular L en una dirección, y un momento magnético μ en la dirección opuesta.

Este resultado indica que el *momento magnético del electrón es proporcional a su momento angular orbital.* Observamos que debido a que el electrón está cargado negativamente, los vectores μ y L apuntan en direcciones opuestas. Ambos son perpendiculares al plano de la órbita, como indica la figura 3b.

Un resultado fundametal de la física cuántica es que el momento angular orbital está cuantizado, y siempre es igual al múltiplo entero de $\hbar = h/2\pi = 1.06\,\mathrm{X}\,10^{-34}\mathrm{J{\cdot}s}$, donde h es la constante de Planck. Esto es

$$L = 0, \hbar, 2\hbar, 3\hbar, \ldots$$

Por lo tanto, el valor más pequeño no cero del momento magnético es

$$\mu = \frac{e}{2m}\hbar \tag{5.10}$$

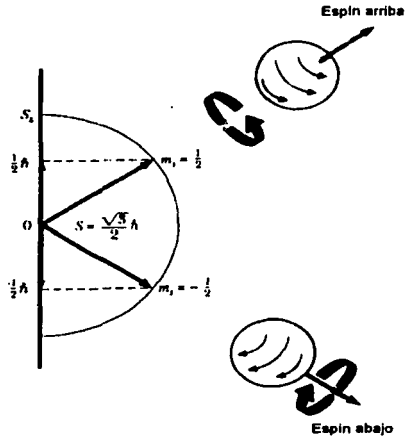


Fig. 3c El momento angular de espín presenta también cuantización del espacio. Esta figura presenta las dos orientaciones permitidas de un vector de espín S para una partícula de espín $\frac{1}{2}$, como el electrón.

El electrón tiene otra propiedad intrínseca, llamada espín, que también contribuye al momento magnético. La propiedad del espín surge de la dinámica relativista, la cual puede incorporarse a la mecánica cuántica. La magnitud del así llamado momento magnético de espín es del mismo orden de magnitud que el momento magnético debido al primer efecto de la espira de corriente, el movimiento orbital. La magnitud del momento angular de espín predicha por la teoría cuántica es

$$S = \frac{\hbar}{2} = 5.2729\,\mathrm{X}\,10^{-35}\mathrm{J{\cdot}s}$$

Q 1

El momento magnético intrínseco asociado al espín de un electrón tiene el valor

$$\mu_B = \frac{e}{2m}\hbar = 9.27\,\mathrm{X}\,10^{-24}\mathrm{J/T} \tag{5.11}$$

el cual se llama el **magnetón de Bohr**.

Desde un punto de vista clásico, el momento angular intrínseco se atribuye al electrón cargado que gira alrededor de su propio eje, y por eso recibe el nombre de espín - con frecuencia los físicos emplean la palabra *espín* cuando se refieren al momento angular del espín. Por ejemplo, es común utilizar la frase *el electrón tiene un espín* de $\frac{1}{2}$. El momento angular del espín del electrón *nunca cambia*. Esta idea contradice las leyes clásicas, donde una carga en rotación se frena en presencia de un campo magnético aplicado debido a la fuerza electromotriz de Faraday que acompaña al campo variable. Además si el electrón se ve como una bola de carga girando sujeta a las leyes clásicas, partes de su superficie cercana rotarían con velocidades superiores a la de la luz. De este modo, no se debe abusar de la descripción clásica; por último, el electrón girando es una entidad cuántica que desafía a cualquier simple interpretación clásica [Serway, 1997 pg. 1271]-.

En 1929, Dirac resolvió la ecuación relativista para el electrón en un pozo de potencial utilizando la forma relativista de la energía total. El análisis de Dirac confirmó la naturaleza fundamental del espín del electrón. Además, la teoría mostró que el espín del electrón puede describirse por medio de un solo número cuántico s, cuyo valor podría ser $\frac{1}{2}$. La magnitud del **momento angular del espín S** para el electrón es

$$S = \sqrt{s(s+1)}\hbar = \frac{\sqrt{3}}{2}\hbar \tag{5.12}$$

Del mismo modo que el movimiento angular orbital, el momento angular del espín está cuantizado en el espacio, como se describe en la figura 3c. Puede tener dos orientaciones, especificadas por el número cuántico magnético del espín m_s, donde $m_s = \pm\frac{1}{2}$. La componente s del momento angular del espín es

$$S_z = m_s\hbar = \pm\tfrac{1}{2}\hbar \tag{5.13}$$

Los dos valores de $\pm\hbar/2$ para S_z corresponden a las dos orientaciones posibles de S mostradas en la figura 3c. El valor $m_s = +1/2$ se refiere al caso de espín arriba, en tanto que el valor contrario se refiere al caso de espín abajo.

El momento magnético del espín del electrón, μ_s, se relaciona con su momento angular de espín **S** por medio de la expresión

$$\mu_s = -\frac{e}{m}S \tag{5.14}$$

Puesto que $S_z = \pm\frac{1}{2}\hbar$, la componente z del momento magnético del espín puede tener los valores

$$\mu_{sz} = \pm\frac{e\hbar}{2m} \tag{5.15}$$

Como se puede observar, la cantidad $e\hbar/2m$ es el magnetón de Bohr μ_B. Se advierte que la contribución del espín al momento angular μ es el doble de la contribución del movimiento angular orbital L. El factor de 2 se explica en un tratamiento relativista del sistema que fue realizado por primera vez por Dirac, y ésto a nuestro fin no concierne.

A concluir, atribuímos a una partícula elemental un cierto momento cinético 'propio', no ligado a su movimiento en el espacio. A este momento cinético propio de una partícula se le llama *espín*.

Bibliografía

[1] Landau L. D. y E. M. Lifshitz, *Física Teórica, Mecánica Cuántica, Teoría No-Relativista*, Editorial Reverté, 1975.

[2] Lomonaco Samuel J., Jr.*A Rosetta Stone for quantum mechanics with an introduction to quantum computation.* Primera de ocho ponencias dadas en la Sociedad Matemática Americana AMS Curso breve sobre Computación Cuántica organizado en conjunción con la Reunión Anual de la AMS en Washington, DC, USA en enero de 2000, y será publicado en el volumen de la AMS PSAPM titulado "Quantum Computation".

[3] Oziewicz Zbigniew, *Spin-density operator for the interacting two-spin systems.* Journal of Physics A: Mathematics and General vol. 18 1985. Páginas. 671-704.

[4] Serway Raymond A., *Física*; McGraw-Hill, Tomo 2, Cuarta edición, 1997.

[5] Svozil Karl, *Quantum Information: The New Frontier*; Instituto de Física Teórica, Universidad de Tecnología Vienna, Vienna, Austria, 2000.

Capítulo 6

Compuertas Cuánticas

En este punto ya se tiene una visión de la senda que sigue la construción del hardware cuántico. Empezamos, pues, con sus partes constitutivas.

Las computadoras digitales están construidas con circuitos que tienen estados discretos y definidos. En ingeniería se segura que estos circuitos nunca pasen a condiciones intermedias. Los sistemas cuánticos, por su naturaleza, ofrecen una gran discretización sin ningún esfuerzo ingenieril. Cuando se mide la orientación del espín de un eletcrón, por ejemplo, esta es siempre "arriba" o "abajo", nunca intermedia. También un átomo gana o pierde energía cuando hace un "salto cuántico" entre estados de energía específicos, sin pasar a través de niveles de energía intermedios.

En una computadora cuántica, las partes básicas serían electrones individuales o átomos, construir tal máquina está simplemente más allá de nuestras técnicas. Además del reto de la fabricación a escala atómica, hay algunos pormenores conceptuales hipersensitivos. Los sistemas cuánticos tienen comportamientos muy famosamente extraños, como el fenómeno conocido como interferencia cuántica, el cual se abordará posteriormente. Dos transistores cercanos el uno del otro pueden conmutar independientemente, pero dos objetos cuánticos (como dos electrones) están inextricablemente acoplados, siendo así que el estado futuro de un electrón no puede ser predicho sin tomar en cuenta a los electrones que lo rodean. Ciertamente, un electrón aislado puede interferir con él mismo.

6.1 La compuerta NOT probabilista

El dispositivo clásico booleano más simple es la compuerta NOT, la cual acepta un solo bit de entrada y produce un bit de salida. Esta compuerta es totalmente determinista. Supongamos que cambiamos esta compuerta por una probabilista, la cual usualmente invierte su entrada en un 90 por ciento de las veces pero ocasionalmente pasa la entrada sin cambiarla. Esta transformación puede ser representada por una matriz de probabilidad unitaria, como sigue:

Aquí los números a lo largo del borde izquierdo, representan las entradas, y los primeros de las columnas son las salidas. Para encontrar la probabilidad de que una entrada 0 produzca una salida de 1, se lee a lo largo del renglón 0 en donde intersecte la columna 1. Nótese que aun cuando las entradas de la matriz sean fraccionarias, esta compuerta "NOT probabilista" es todavía un dispositivo binario cuyas entradas y salidas son siempre 0 o 1. También nótese que las probabilidades en cada columna y en cada renglón suman 1, indicando que cualquier posible combinación de la entrada y salida han sido acumuladas.

La operación de la simple compuerta determinista NOT puede ser representada con la misma notación matricial descrita arriba:

	0	1
0	0	1
1	1	0

En este caso la probabilidad de obtener un 0 con un 0 de entrada es 0 por lo que la probabilidad de transformar un 0 en 1 es 1.

En el polo opuesto a una compuerta completamente determinista esta la aleatoria, produciendo un 0 o 1 con igual probabilidad, la matriz para esta función es:

	0	1
0	1/2	1/2
1	1/2	1/2

En efecto, la compuerta modela un volado justo, y por lo tanto es designada como CF (coin flip). Una compuerta de este tipo parecería inutil, pero de hecho la aleatoriedad es una fuente importante en ciertos algoritmos [Hayes, 1995 pg. 3].

6.2 Compuertas lógicas cuánticas

Ambas compuertas NOT, la Booleana y la probabilista todavía son construcciones de la física clásica. Una compuerta cuántica es más extraña porque contiene qubits que a diferencia de los cbits, éstos pueden ocupar una superposición de los estados 0 y 1 durante ciertas etapas de la computación. Esto no quiere decir que el qubit tiene algún valor intermedio entre 0 y 1. En lugar de eso, el qubit está en ambos estados el 0 y el 1 al mismo tiempo. Así, cuando el estado del qubit es medido u observado, invariablemente será 0 o 1.

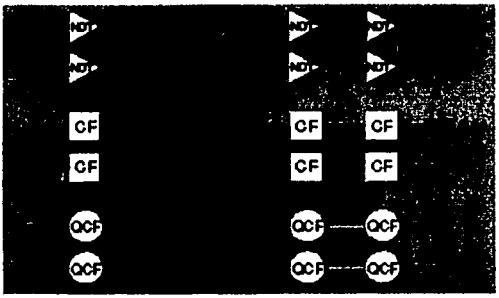


Fig. 6a

Los estados cuánticos y su superposición son representados por medio del mismo dispositivo notacional "ket: $|\,\rangle$". Recordando, el estado de un qubit se da como $a|0\rangle + b|1\rangle$, en donde los coeficientes a y b son las "amplitudes" de cada estado. En general las amplitudes son números complejos. La amplitud asociada con un estado determina la probabilidad de que el qubit sea encontrado en algún estado; específicamente, la probabilidad es igual al cuadrado del valor absoluto de la amplitud correspondiente.

La relación entre amplitud y probabilidad se hace más clara con el siguiente ejemplo. Una compuerta cuántica que Brassard designó QCF (para "quantum coin flip") tiene la siguiente matriz de amplitudes:

$$\begin{array}{c|cc} & |0\rangle & |1\rangle \\ |0\rangle & 1/\sqrt{2} & -1/\sqrt{2} \\ |1\rangle & 1/\sqrt{2} & 1/\sqrt{2} \end{array}$$

Para encontrar la probabilidad de cada transición, se toma el valor obsoluto de la amplitud corespondiente y se eleva al cuadrado: $|1/\sqrt{2}|^2 = 1/2$. Así todas las entradas de la matriz de probabilidad son 1/2, y QCF es igual a la CF, a primera vista.

Más el análisis indica lo contrario. Una forma de ver la diferencia es conectando dos compuertas en serie, como se muestra en la figura 6a. Como puede verse, dos compuertas NOT en serie dan como resultado la función identidad. Con dos compuertas CF, para cualquier valor en la entrada, la primera produce un 0 o un 1 al azar, y la segunda repite el proceso. De aquí, cualquier número de compuertas CF en serie son equivalentes en función a una sola CF.

Para dos QCF en serie, en los sistemas cuánticos no es posible asignar un valor definitivo a la señal intermedia no observada entre las dos compuertas. La salida de la primera QCF no es 0 sino una superposición de los estados $|0\rangle$ y $|1\rangle$. Específicamente, si la entrada a la primer compuerta es 1, la salida de la compuerta es la superposición $1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle$, como se indica en la matriz de amplitudes. Ahora esta superposición de estados se convierte en la entrada de la segunda compuerta QCF, que actúa acorde a la misma matriz de amplitudes. La parte 0 de la superposición se transforma en $1/\sqrt{2}(1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle)$, mientras que la parte 1 se convierte en $1/\sqrt{2}(1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle)$. De esta forma el estado completo del sistema da

$$(\text{QCF})^2|1\rangle = \tfrac{1}{\sqrt{2}}(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle) + \tfrac{1}{\sqrt{2}}(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle)$$

realizando las multiplicaciones se obtiene $1/2(|0\rangle + |0\rangle)$, o simplemente $|0\rangle$. Las dos compuertas implementan la función NOT, esto es $(\text{QCF})^2 = \text{NOT}$.

La fuente de estos efectos es el fenómeno conocido como interferencia cuántica. La superposición de los estados puede verse como la superposición de ondas, las cuales se cancelan o suman acorde a su amplitud y fase, justo como dos estados cuánticos interfieren constructiva o destructivamente acorde al signo de sus amplitudes.

Al diseñar compuertas para la computadora cuántica, ciertos puntos deben satisfacerse: la suma de las probabilidades de todos las salidas debe ser unitaria. Un problema de este requerimiento es que cualquier operación tiene que ser reversible (prefiero compartir que esta reversibilidad es una consecuencia [Fortnow, 2000 pg. 6]), debemos ser capaces de tomar el resultado de una operación y regresárselo a la máquina en dirección opuesta

para recobrar las entradas originales, y las compuestas clásicas no obedecen esta regla.

6.2.1 Lo básico

La unidad fundamental de la información clásica puede ser vista como un vector 1-dimensional $\in \mathbb{Z}_2$. Una cadena clásica de n-bits, la cual pertenece a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots$, toma los valores de un conjunto de 2^n estados posibles, $|\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots| = 2^n$. También es un vector n-dimensional sobre $\mathbb{Z}_2$. $2 - bit \in \mathbb{Z}_2\mathbb{Z}_2$. En contraste, el qubit puro es un vector 2-dimensional sobre el campo complejo $\mathbb{C}$. Un estado de n-qubits es un vector unitario sobre un espacio de Hilbert 2^n-dimensional el cual es un producto tensorial de n espacios de Hilbert 2-dimesionales. $\{|0\rangle, |1\rangle\}$ usualmente son las bases del qubit. Estas bases también son conocidas como *bases o principios computacionales.* El estado de un qubit arbitrario está dado por un vector $|\psi\rangle = a|0\rangle + b|1\rangle$ con el *cuadrado de la norma* $\langle\psi|\psi\rangle = 1$ que representa algo de la "probabilidad total". Un estado de n-qubits es también un vector sobre los estados bases con n-bits etiquetas, siguiendo la estructura del producto tensorial de n-qubits espacios de Hilbert. Las *bases conjugadas* están definidas como $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

En las computadoras cuánticas el qubit es representado por un sistema físico de dos estados, como se mencionó. Formalizando, para $n \geq 1$ un estado $|\psi\rangle$ de n-qubits es representado como una superposición de $|x\rangle$'s con $x \in \{0,1\}^n$, esto es

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} A_x|x\rangle, \tag{6.1}$$

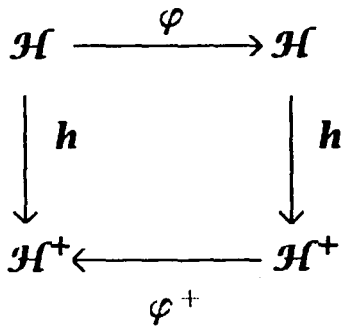
(también para $x \in \mathcal{H}^{\otimes n}$), en donde todas las A_x's son números complejos que satisfacen
$\sum_{x\in\{0,1\}^n} |A_x|^2 = 1$. Cada A_x es llamada la *amplitud* de $|x\rangle$ en $|\psi\rangle$, y B_x, la cual satisface $A_x = |A_x|e^{iB_x}$, es llamado la *fase* de $|x\rangle$ en el estado $|\psi\rangle$. [Abe, 2000]

El vector $|\psi\rangle$es un *estado puro.* Y como la fase total es irrelevante, un estado puro se representa de forma más precisa por un *proyector* $|\psi\rangle\langle\psi|$, en donde $\langle\psi|$ es lo dual del vector . En contraste, un estado *mezclado* es una *distribución* o un grupo de estados puros. Por ejemplo, el estado es $|\psi_k\rangle$ con probabilidad p_k. Matemáticamente, un estado mezclado es una

combinación convexa de proyectores. Por ejemplo, la distribución anterior es representada por la matriz densidad $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$ [Leung, 2000 pg. 7].

6.2.2 Propiedades de matrices unitarias

Definición
Sea ϕ una matriz unitaria de cualquier tamaño, 'h' la misma estructura hilbertiana ya definida, entonces, ϕ es un morfismo unitario si satisface la igualdad



$$\phi^+ \circ h \circ \phi = h$$

Teorema 1: Toda matriz unitaria de 2 x 2 puede ser expresada como [Barenco et. al 1995 pg. 8],

$$\begin{pmatrix} e^{id} & 0 \\ 0 & e^{id} \end{pmatrix} \cdot \begin{pmatrix} e^{ia/2} & 0 \\ 0 & e^{-ia/2} \end{pmatrix} \cdot \begin{pmatrix} cos\theta/2 & sen\theta/2 \\ -sen\theta/2 & cos\theta/2 \end{pmatrix} \cdot \begin{pmatrix} e^{ib/2} & 0 \\ 0 & e^{-ib/2} \end{pmatrix},$$

donde d, a, θ y b son evaluadas en los reales. Además, cualquier matriz especial unitaria (esto es, con determinante unitario) puede ser expresada como

$$\begin{pmatrix} e^{ia/2} & 0 \\ 0 & e^{-ia/2} \end{pmatrix} \cdot \begin{pmatrix} cos\theta/2 & sen\theta/2 \\ -sen\theta/2 & cos\theta/2 \end{pmatrix} \cdot \begin{pmatrix} e^{ib/2} & 0 \\ 0 & e^{-ib/2} \end{pmatrix} \cdot$$

Definición: En vista del teorema anterior, se define lo siguiente.

- $R_y(\theta) = \begin{pmatrix} cos\theta/2 & sen\theta/2 \\ -sen\theta/2 & cos\theta/2 \end{pmatrix}$ (rotación de θ alrededor de $\hat{y}$).
- $R_z(a) = \begin{pmatrix} e^{ia/2} & 0 \\ 0 & e^{-ia/2} \end{pmatrix}$ (rotación de a alrededor de $\hat{z}$).
- $Ph(d) = \begin{pmatrix} e^{id} & 0 \\ 0 & e^{id} \end{pmatrix}$ (un cambio de fase [phase-shift] con respecto a d).
- $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ("negación" o matriz de Pauli).
- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (La matriz identidad).

Teorema 2: Las siguientes propiedades se mantienen:

1. $R_y(\theta_1) \cdot R_y(\theta_2) = R_y(\theta_1 + \theta_2)$
2. $R_z(a_1) \cdot R_z(a_2) = R_z(a_1 + a_2)$
3. $Ph(d_1) \cdot Ph(d_2) = Ph(d_1 + d_2)$
4. $\sigma_x \cdot \sigma_x = I$
5. $\sigma_x \cdot R_y(\theta) \cdot \sigma_x = R_y(-\theta)$
6. $\sigma_x \cdot R_z(a) \cdot \sigma_x = R_z(-a)$

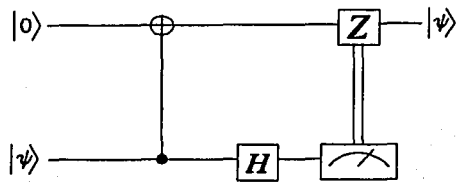
La partición a la mitad del ángulo de estas definiciones conforma a la relación usual entre las operaciones SO(3) y SU(2). Ver J. Mathews y R.L. Walker. Mathematical Methods of Physics, (2a edición, W.A. Benjamin, Menlo Park, CA, 1970), página 464, para el uso del lenguaje SO(3) (rotaciones del cuerpo rígido) para describir las operaciones SU(2).

Esta Sección es útil para la interpretación y tratamiento de las compuertas cuánticas.

6.3 Circuitos Cuánticos

El circuito cuántico es un modelo y una representación del procesamiento de información cuántica [Leung, 2000 pg. 8]; y es una red formada por compuertas cuánticas [Abe, 2000 pg. 124]. En esta parte presentaremos a

los elementos de circuito comunes. Considérese el siguiente ejemplo de un circuito cuántico.



Las siguientes convenciones son usadas en toda la tesis:

- Las direcciones horizontales y verticales esquemáticamente representan cambios en el tiempo y en el espacio.
- El tiempo va de izquierda a derecha.
- Las líneas horizontales representan registros cuánticos.
- Los estados de entrada están en la parte izquierda, y los estados de salida en la parte derecha.
- Las cajas que contienen letras representan compuertas. Algunas compuertas son representadoas con símbolos más especiales, justo como los símbolos '$\oplus$' y '$\bullet$' que conectan a los registros.
- La carátula representa una medición projectiva a lo largo de los principios computacionales
- La doble línea representa a la *información clásica*. Una operación conectada a un aparato de medición por medio de una línea doble es considerada *condicionada* sobre el resultado de la medición siendo $|1\rangle$.

Asumiremos que la información es almacenada en los registros en forma binaria. Por ejemplo, el número 6 es representado por un registro en el estado $|1\rangle \otimes |1\rangle \otimes |0\rangle$. En una notación más compacta: $|a\rangle$ representa el producto tensorial $|a_{n-1}\rangle \otimes |a_{n-2}\rangle \ldots |a_1\rangle \otimes |a_0\rangle$, donde $a_i \in \{1, 1\}$, y representa un registro cuántico preparado con el valor $a = 2^0 a_0 + 2^1 a_1 + \ldots 2^{n-1} a_{n-1}$.Hay 2^n estados de este tipo, representando a todas las cadenas binarias de longitud n o números del 0 al $2^n - 1$, y forman una base computacional conveniente. En lo siguiente $a \in \{0, 1\}^n$ (a es una cadena binaria de longitud n) implica que $|a\rangle$ pertenece a la base computacional.

Así un registro cuántico de tamaño tres puede almacenar números individuales tales como 3 o 7,

$$|0\rangle \otimes |1\rangle \otimes |1\rangle \equiv |011\rangle \equiv |3\rangle$$
$$|1\rangle \otimes |1\rangle \otimes |1\rangle \equiv |111\rangle \equiv |7\rangle$$

pero, también puede almacenar dos de ellos simultáneamente. Si tomamos el primer qubit y en lugar de ponerlo a $|0\rangle$ o $|1\rangle$ se prepara una superposición $1/\sqrt{2}(|0\rangle + |1\rangle)$ entonces obtenemos

$$\begin{aligned} \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle &\equiv \tfrac{1}{\sqrt{2}}(|011\rangle + |111\rangle) \\ &\equiv \tfrac{1}{\sqrt{2}}(|3\rangle + |7\rangle). \end{aligned}$$

De hecho podemos preparar este registro en una superposición de todos los ocho números -es suficiente con poner cada qubit en la superposición $1/\sqrt{2}(|0\rangle + |1\rangle)$. Esto da

$$\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

el cual también puede ser escrito en binario como (ignorando la constante de normalización $2^{-3/2}$),

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

o en notación decimal como

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

o simplemente como

$$\sum_{x=0}^{7} |x\rangle. \tag{6.2}$$

Estas preparaciones, y cualquier otra manipulación de los qubits, tienen que ser consideradas como operaciones unitarias. Una *compuerta cuántica* es un dispositivo que ejecuta una operación unitaria fija sobre qubits seleccionados en un periodo fijo de tiempo, y una *red cuántica* es un dispositivo consistente de compuertas lógicas cuánticas cuyos pasos computacionales están sincronizados en el tiempo como fue asentado por Deutsch en 1989. Las salidas de algunas de las compuertas están conectadas con cables hacia las entradas de otras. El *tamaño* de la red es el número de compuertas que contiene.

Una compuerta cuántica tiene el mismo número de entradas y de salidas. Una compuerta cuántica G con k-entradas y k-salidas se encuentra especificada por una matriz de 2^kx2^k unitaria $U_G = [u_{xy}]$ para $x, y \in \{0,1\}^k$ y realiza un mapeo de los estados de sus entradas hacia los estados de sus salidas [Abe, 2000 pg. 124] como sigue:

$$|x\rangle \mapsto \sum_{y \in \{0,1\}^k} u_{xy}|y\rangle. \tag{6.3}$$

6.4 Compuertas cuánticas de una entrada "Unarias"

6.4.1 Compuerta H

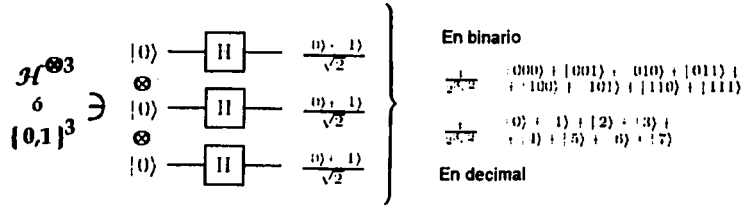
La compuerta cuántica más común es la compuerta Hadamard, una compuerta H de un solo qubit que ejecuta la transformación unitaria conocida como la transformada Hadamard. La matriz está escrita en la base computacional $\{|0\rangle, |1\rangle\}$ y el diagrama provee una representación esquemática de la compuerta H que actua sobre un qubit en el estado $|x\rangle$, con $x = 0, 1$. Una característica importante de esta compuerta es que el cuadrado de ella misma da la matriz identidad, $\mathrm{H}^2 = \mathrm{id}$, lo que implica, $\mathrm{H}^+ \circ h \circ \mathrm{H} = h$.
Y se define como:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad |x\rangle \boxed{H} \frac{(-1)^x |x\rangle + |1-x\rangle}{\sqrt{2}}$$

El **problema** a desarrollar es dar las soluciones del sistema $H^+ \circ h \circ H = h; H^2 = id$

Todas las matrices se tratarán al igual que en los ejemplos de la compuerta NOT probabilista y clásica, es decir, la parte superior izquierda siempre es 0, la parte inferior izquierda es 1; en la parte horizontal, a la izquierda será 0 y a la derecha siempre 1; los elementos de la línea horizontal son salidas y los elementos de la línea vertical entradas. Para nosotros lo más importante será el tratamiento de las compuertas cuánticas con las matrices, pues facilitan la visualización de las entradas y salidas.

Y aquí tenemos una red, de tamaño tres, la cual aplica la transformada Hadamard a tres qubits. Si éstos están inicialmente en el estado $|000\rangle$ entonces las salida es la superposición de todos los números desde 0 hasta 7.



Si los tres qubits están inicialmente en algún otro estado a la base computacional entonces el resultado es una superposición de todos los números desde 0 hasta 7 pero exactamente la mitad de ellos aparecerán en la superposición con el signo menos, por ejemplo,

$$|101\rangle \mapsto \frac{1}{2^{3/2}} \left\{ \begin{array}{l} |000\rangle - |001\rangle + |010\rangle - |011\rangle + \\ -|100\rangle + |101\rangle - |110\rangle + |111\rangle \end{array} \right\}.$$

En general, si iniciamos con un registro de tamaño n en algún estado $y \in \{0,1\}^n$entonces

$$|y\rangle \mapsto 2^{-n/2} \sum_{x \in \{0,1\}^n} (-1)^{y \cdot x} |x\rangle,$$

donde el producto de $y = (y_{n-1}, \ldots, y_0)$ y $x = (x_{n-1}, \ldots, x_0)$ es tomado bit a bit:

$$y \cdot x = (y_{n-1}x_{n-1} + \ldots y_1 x_1 + y_0 x_0).$$

6.4.2 Compuerta ϕ

La compuerta de cambio de fase ϕ (phase shift) es definida como $|0\rangle \mapsto |0\rangle$ y $|1\rangle \mapsto e^{i\phi}|1\rangle$, o en notación matricial,

$$\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \qquad |x\rangle \text{ —●— } \phi \text{ —} \; e^{i\phi x}|x\rangle$$

Las compuertas Hadamard y de cambio de fase pueden ser combinadas para construir la siguiente red (de tamaño cuatro), la cual genera el estado puro más general de un solo qubit (hasta una fase global),

$$|0\rangle \text{ —[H]—●—[H]—●— } \cos\theta\,|0\rangle + e^{i\phi}\sin\theta\,|1\rangle\,.$$

(sobre el primer ● aparece 2θ; sobre el segundo ● aparece $\frac{\pi}{2} + \phi$)

Consecuentemente, estas compuertas son suficientes para construir *cualquier* operación unitaria sobre un solo qubit.

De esta manera, las compuertas Hadamard y las compuertas de cambio de fase pueden ser usadas para transformar el estado de entrada $|0\rangle|0\rangle \ldots |0\rangle$ del registro de n qubits en cualquier estado del tipo $|\psi_1\rangle|\psi_2\rangle \ldots |\psi_n\rangle$, donde $|\psi_i\rangle$ es una superposición arbitraria de $|0\rangle$ y $|1\rangle$. Estos son estados especiales de n-qubits, llamados los estados producto o los estados separables. En general, un registro cuántico de tamaño $n > 1$ puede ser preparado en estados que no sean separables - que son conocidos como estados enredados (entangled states). Por ejemplo, para dos qubits ($n = 2$), el estado

$$a|00\rangle + b|01\rangle = |0\rangle \otimes (a|0\rangle + b|1\rangle)$$

es separable, $|\psi_1\rangle = |0\rangle$ y $|\psi_2\rangle = a|0\rangle + b|1\rangle$, mientras que el estado

$$a|00\rangle + b|11\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$$

está enredado ($a, b \neq 0$), porque no puede ser escrito como un producto tensorial.[Ekert et. al, 2000 pg. 4]

6.4.3 Compuerta NOT

Definida por la matriz

$$\mathbf{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_1$$

6.4.4 Compuertas de rotaciones

Se entiende la impotancia de estas compuertas ya que son básicas en la representación de matrices unitarias,

$$\boxed{e^{i\theta\sigma_1}} = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} = e^{i\theta\sigma_1}$$

$$\boxed{e^{i\theta\sigma_2}} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = e^{i\theta\sigma 2}$$

$$\boxed{e^{i\theta\sigma_3}} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} = e^{i\theta\sigma_3}$$

6.4.5 Raíz cuadrada de NOT

Esta operación ya se vió, como ejemplo a la presentación de las demás compuertas.

Se define como sigue:

$$\sqrt{\mathbf{NOT}} = \boxed{\sqrt{\mathbf{NOT}}} = \frac{1-i}{2}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} = \frac{1+i}{2}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$

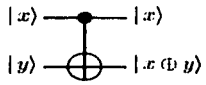
6.5 Compuertas de dos entradas "Binarias"

Con la finalidad de enredar dos o más qubits se tiene que extender el repertorio de compuertas cuánticas a compuertas de dos qubits.

6.5.1 Compuerta C-NOT

La compuerta de dos qubits más conocida es la NOT-controlada (C-NOT), también llamada, XOR o la compuerta de medición. Ésta voltea al segundo qubit y (objetivo) si el primero x(el de control) es $|1\rangle$ y no hace nada si el qubit de control es $|0\rangle$. La compuerta es representada por la matriz unitaria

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



donde $x, y = 0$ o 1, y $\oplus$ denota a una XOR.

La forma en que se acomodan los bits es la siguiente:

se lee x, y en base a los principios computacionales {00,01,10,11}, comenzando desde la esquina superior izquierda de la matriz, hacia abajo para las entradas y hacia la derecha para las salidas.

Si aplicamos la C-NOT a datos Booleanos en los cuales el qubit objetivo es $|0\rangle$ y el de control, ya sea $|0\rangle$ o $|1\rangle$ entonces el efecto consiste en dejar al de control sin cambio mientras que el de objetivo se convierte en una copia del de control, esto es

$$|x\rangle|0\rangle \mapsto |x\rangle|x\rangle \quad x = 0, 1$$

Podríamos suponer que esta compuerta podría usarse para copiar superposiciones tales como $|\psi\rangle = a|0\rangle + b|1\rangle$, de tal manera que

$$|\psi\rangle|0\rangle \mapsto |\psi\rangle|\psi\rangle \tag{6.4}$$

para cualquier $|\psi\rangle$. Esto no es así. Lo unitario de la C-NOT requiere que la compuerta convierta a las superposiciones en el qubit de control en *enredos* de ambos. Si el qubit de control está en un estado de superposición

$|\psi\rangle = a|0\rangle + b|1\rangle$, $(a, b \neq 0)$, y el objetivo en $|0\rangle$, entonces la C-NOT genera el estado enredado

$$(a|0\rangle + b|1\rangle)|0\rangle \mapsto a|00\rangle + b|11\rangle.$$

A partir de esto notamos que es imposible construir una máquina clonadora universal que efectue la transformación de la ecuación (6.4), o aún la más general

$$|\psi\rangle|0\rangle|W\rangle \mapsto |\psi\rangle|\psi\rangle|W'\rangle$$

en donde $|W\rangle$ hace referencia al estado de todo lo que resta y $|\psi\rangle$ es *cualquier* estado cuántico [Ekert et. al, 2000 pg. 4]. Para ver esto se toman dos estados normalizados $|\psi\rangle$ y $|\Phi\rangle$ que no son idénticos ($|\langle\Phi|\psi\rangle| \neq 1$) y no ortogonales ($\langle\Phi|\psi\rangle \neq 0$) y efectuemos la transformación,

$$|\psi\rangle|0\rangle|W\rangle \mapsto |\psi\rangle|\psi\rangle|W'\rangle$$
$$|\Phi\rangle|0\rangle|W\rangle \mapsto |\Phi\rangle|\Phi\rangle|W''\rangle$$

Como esto debe ser una transformación unitaria que preserve el producto interno por consiguiente debe satisfacer

$$\langle\Phi|\psi\rangle = \langle\Phi|\psi\rangle^2\langle W'|W''\rangle$$

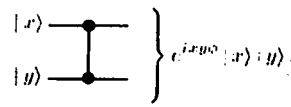
y esto sólo puede ser satisfecho cuando $|\langle\Phi|\psi\rangle| = 0$ o 1, lo cual contradice nuestras asunciones. Entonces los estados de los qubits, a diferencia de los clásicos, no pueden ser fielmente clonados. Guiándonos a aplicaciones más interesantes.

Problema: Puede ser la compuerta C-NOT representada por trenzas?[Kauffman, 2001]

6.5.2 Compuerta $B(\phi)$

Otra compuerta común de dos qubits es la compuerta controlada de cambio de fase $B(\phi)$ definida como

$$B(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix}$$



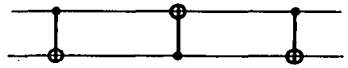
Nuevamente, la matriz está escrita en la base computacional:

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

y el diagrama de la derecha muestra la estructura de la compuerta.

6.5.3 Compuerta SWAP

Como su nombre lo indica, sólo intercambia de lugar a los qubits de las entradas.

$$\text{SWAP} = \quad \begin{matrix} b \\ a \end{matrix} \quad \text{  } \quad \begin{matrix} a \\ b \end{matrix} \quad = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

6.5.4 Raíz cuadrada de SWAP

Esta compuerta es la misma, la única diferencia es que se obtiene su raíz cuadrada.

Definida como:

$$\sqrt{\text{SWAP}} = \quad \text{} \quad = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1+i}{2} & \frac{1-i}{2} & 0 \\ 0 & \frac{1-i}{2} & \frac{1+i}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

6.6 Compuertas de tres entradas "Ternarias"

6.6.1 Compuerta Toffoli

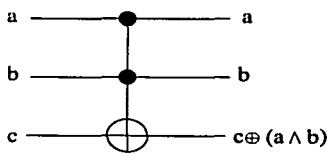
También conocida como la compuerta NOT-CONTROLADA-CONTROLADA o C^2-NOT. Esta compuerta tiene dos qubits de control (de arriba hacia abajo) y uno de objetivo el cual es negado sólo cuando los dos qubits de control están en el estado $|1\rangle|1\rangle$. La compuerta C^2-NOT da los conectores lógicos necesarios para la aritmética. Si el qubit objetivo es inicialmente puesto a $|0\rangle$ la compuerta actua como una AND reversible - después de la operación de la compuerta el objetivo se convierte en la AND lógica de los dos qubits de control.

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

la cual es su matriz y la siguiente formulación su interpretación

$$|x_1, x_2\rangle|0\rangle \mapsto |x_1, x_2\rangle|x_1 \wedge x_2\rangle$$

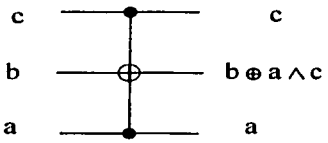
su diagrama:



La compuerta de tres qubits Toffoli (Toffoli 1980), demostró ser universal para la lógica Booleana reversible.

6.6.2 Compuerta Toffoli'

En esta variación ningún qubit es predispuesto a ningún estado. El diagrama para esta compuerta es:

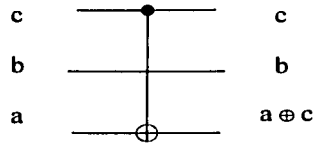


Esto corresponde a la transformación unitaria

$$\textbf{Toffoli'} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

6.6.3 Compuerta C-NOT'

Otra compuerta es la CNOT' representada por el diagrama



Cuya transformación unitaria es

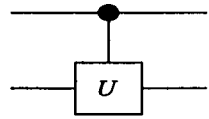
$$\mathbf{CNOT'} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Todos los diagramas que se usan para representar las compuertas, tienen la ventaja de ser un simple medio de describir algunas transformaciones unitarias, un poco complicadas. Sin embargo, sí tienen sus inconvenientes, y pueden ser mal interpretadas, si no se tiene cuidado.

Un problema con estos diagramas es que no son descripciones independientes de transformaciones unitarias. Cada diagrama describe a una transformación unitaria usando una base implícita comprendida. [Lomonaco Jr., 2000 pg. 54]

6.7 Conjunto universal de compuertas

Más generalmente, todas las compuertas controladas de 2 qubits son de la forma U-controlada, para alguna transformación unitaria U de un solo qubit. La compuerta U-controlada aplica la transformación identidad al qubit auxiliar (el más bajo) cuando el qubit de control esta en el estado $|0\rangle$ y aplica una U prescrita cuando el qubit de control esta en el estado $|1\rangle$. La compuerta mapea $|0\rangle|y\rangle$ a $|0\rangle|y\rangle$ y $|1\rangle|y\rangle$ a $|1\rangle(U|y\rangle)$, y se representa gráficamente como



La compuerta Hadamard, todas las compuertas de fase, y la C-NOT, forman un conjunto universal de compuertas, esto es, cualquier operación unitaria de n-qubits puede ser simulada por un determinado número de compuertas siendo este $\mathcal{O}(4^n n)$ [Ekert et. al, 2000 pg. 5].

Este no es el único conjunto universal de compuertas, sin embargo han sido las más estudiadas, y todo en la investigación son acuerdos, en cada conjunto de compuertas universales, estas compuertas han tenido siempre su lugar. Se podría ampliar el número de compuertas hasta ahora presentado en las investigaciones y probar su universalidad, más no es el objetivo de esta obra. (Para este punto se puede ver [Aharonov y M. Ben-or, 1999 pg. 38])

Un conjunto de compuertas para la computación cuántica es universal si genera a un conjunto *denso* en el conjunto de todas las operaciones unitarias. En otras palabras, una operación arbitraria unitaria puede ser *aproximada* con precisión arbitraria por medio de la composición de compuertas del conjunto [Leung, 2000 pg. 11].

Las compuertas de 1 qubit han probado ser universales. Estudios sobre compuertas universales de 2 y 3 qubits ya se han hecho, y se continuan mejorando. En concordancia con la conjetura de Deutsch, casi cualquier compuerta de 2 qubits es universal.

La construcción de las compuertas tendrá un acercamiento, pero hasta este punto, la simplicidad en la forma de las interacciones para hacer funcionar a las compuertas no siempre es lo más importante. Es deseable que sean tan genéricas como sea posible [Barenco, 1995 pg. 3].

Una línea más para la presentación de estas compuertas es con el fundamento en los niveles de ruido para la construcción de éstas. Ya se tendrían si los niveles de ruido pudieran hacerse menores. El punto en el cual los datos físicos se encuentran con el umbral teórico es donde la computación cuántica se convierte en realización práctica [Aharonov y M. B, 1999 pg. 59].

Para resolver el problema del ruido cuántico, P. Shor y A. Steane presentaron códigos para la corrección de errores. Esta idea fue expandida y aplicada por numerosos grupos de investigadores para probar bajo que asunciones físicamente razonables, es posible la computación cuántica tolerante a fallas. Entre las asunciones están los requerimientos que el ruido cuántico sea suficientemente débil (abajo de algún umbral de error constante por qubit y operación) y para que las operaciones básicas puedan ser ejecutadas en paralelo. Como resultado, actualmente, se realizan experimentos muy intensos para la realización de la computación cuántica, en una amplia y creciente variedad de sistemas físicos. El progreso hasta el 2000 ha sido modesto, con sistemas existentes limitados a algunos qubits, y con cientos de operaciones [Knill y Nielsen, 2000 pg. 2].

Hasta ahora una computadora cuántica es vista como una red cuántica o familia de redes cuánticas y la computación cuántica es definida como una evolución unitaria de la red que convierte su estado inicial "entrada" en algún estado final "salida".

6.8 Tipos de Compuertas

En el mundo digital todo es discretizado; la principal concepción de las computadoras cuánticas fue también en ese terreno, la discretización nos ofrece muy grandes ventajas, pero la naturaleza analógica nunca podrá hacerse a un lado.

Tradicionalmente los qubits tienen la ventaja, apoyados por los logros de su contraparte clásica. Muchas variables cuánticas son contínuas, tales como la posición, momentum y las amplitudes de los campos electromagnéticos.

Aunque el ruido y exactitud finita hacen intrínsecamente más difícil la manipulación de las variables contínuas que la manipulación de las variables discretas, a causa de los desarrollos recientes en la corrección de errores cuánticos y teletransportación es provechoso tomar el tema.

Como primer punto podría considerarse a la computación cuántica con variables contínuas como un concepto mal definido. Una computadora cuántica con variables discretas con sus qubits se puede definir como un dispositivo que es capaz, mediante operaciones locales, de ejecutar cualquier transformación unitaria. Ahora el caso contínuo. Puesto que una transformación unitaria arbitraria con una sola variable contínua requiere un número infinito de parámetros a definir, típicamente no puede ser aproximado a modos del campo electromagnético por medio de un número finito de operaciones cuánticas contínuas como, por ejemplo, la aplicación de divisores de haces, cambiadores de fase, compresores (squeezers), y dispositivos no lineales. Sin embargo, es posible definir la noción de una computadora con variables contínuas para varias subclases de transformaciones como aquellas correspodientes a los Hamiltonianos que son funciones polinomiales de los operadores correspondientes a las variables contínuas: un conjunto de operaciones contínuas sera definido universal para un conjunto particular de transformaciones si es posible acercarse a cualquier transformación en el conjunto mediante un número finito de aplicaciones de las operaciones [Lloyd, 1998 pg. 1].

6.8.1 Discretas

Todas las compuertas presentadas anteriormente fueron diseñadas para trabajar con qubits, son discretas, y son el principal objetivo. De éstas no es necesario reafirmar lo que potencialmente contienen.

6.8.2 Contínuas

Ya se han provisto [Lloyd, 1998 pg. 2] condiciones suficientes y necesarias para una computadora de este tipo y, que son exclusivamente para transformaciones que son polinomiales en esas variables.

Los cálculos apuntan principalmente a los operadores Hamiltonianos, los cuales se definen como polinomios arbitrarios sobre un conjunto de variables contínuas. Además, dentro de este campo, se destaca el concepto de información cuántica contínua, que es medida con unidades de qu-'nats' (1 nat

$= \log_2 e$ bits).

Este tipo de computación puede ser visualizado como la creación sistemática y la manipulación de qunats.

Al igual que la computación analógica permite, en principio, resolver problemas más rápidamente de lo que es posible digitalmente. En la práctica, debido a la precisión finita de una computadora cuántica contínua -preferiría llamarla "computadora analógica-cuántica"- resolvería los mismos problemas que una computadora discreta, aunque puede ser capaz de ejecutar algunas operaciones con más eficiencia.

La habilidad para crear y manipular qunats depende crucialmente de la fuerza de compresión y de las no-linealidades que uno puede aplicar. Compresores de 10 dB (6 dB después de la atenuación en el aparato de medición) ya existen [Lloyd et.al, 1995 pg. 5]. La electrodinámica cuántica con cavidad de alta Q y las compuertas cuánticas pueden simular estas computadoras. No obstante, la dificultad de ejecutar operaciones no lineales repetitivas de una manera coherente y sin pérdidas es probable que limite sus posibilidades sobre las amplitudes del campo electromagnético.

Las variables contínuas son más susceptibles al ruido, pero las rutinas de corrección de errores contínuos son más sencillas de lo que se cree [Lloyd et.al, 1995 pg. 7].

6.8.3 Híbridas

La razón principal para investigar a las computadoras cuánticas híbridas es porque la naturaleza contiene a ambas, variables discretas como espines, polarizaciones del fotón y niveles de energía atómicos; y variables contínuas tales como posición, momentum y las amplitudes del campo electromagnético. En la computación cuántica convencional, las variables contínuas son una molestia: son fuentes de ruido y decoherencia. En la computación cuántica híbrida, el amplio rango de variables contínuas puede usarse.

Tales dispositivos han demostrado [Lloyd, 2000 pg. 1] ser más eficientes que los computadoras cuánticas convencionales al ejecutar algunos algoritmos cuánticos, tales como el cálculo de eigenvectores y eigenvalores.

Nuevamente, las bases teóricas son Hamiltonianos que representan interacciones entre los qubits y osciladores. A puntualizar, los qubits son caracterizados, generalmente con los operadores de Pauli: $\sigma_x, \sigma_y, \sigma_z$; y los qunats que son osciladores armónicos se caracterizan por la aniquilación y creación de operadores: $a, a^\dagger([a, a^\dagger] = 1)$ y por los operadores de 'posición' y 'momentum', $X = (a + a^\dagger)/2$, $P = (a - a^\dagger)/2i, ([X, P] = i)$. Es conveniente ver a los osciladores armónicos como modos del campo electromagnético con X y P proporcional al cuadrado de las amplitudes del modo. Esto es físicamente posible en el sentido de que las transformaciones sobre espines físicos o átomos son logradas haciendo que los espines interactúen con el campo electromagnético y viceversa. Las interacciones se hacen aplicando pulsos láser o de microondas.

Varios diseños para la computadora cuántica pueden ser fácilmente modificados para hacer una computadora híbrida. Por ejemplo, las computadoras de trampa de iones que operan por medio del acoplamiento de los estados internos de los iones en una trampa de ión (qubits) vía su estado de movimiento (osciladores armónicos). Otro tipo es: los estados traducidos de átomos en un condensador de Bose, los estados contínuos del electrón en los semiconductores o el estado de un circuito de conjunción de Josephson. Esencialmente, cualquier sistema híbrido que presente un control preciso sobre las interacciones entre las variables discretas y contínuas es un buen candidato para una computadora híbrida [Lloyd, 2000 pg. 6].

También presenta nuevos tipos de algoritmos y puede mejorar algunos, que posiblemente serán investigados en alguna otra parte.

6.9 Compuertas de variable contínua e híbridas

Continuando con los esquemas para la construcción de estos tipos de compuertas, únicamente de forma teórica, las técnicas para su construcción se verán más adelante.

A manera de resumen, definiendo las compuertas matemáticamente,

Compuertas de 1 qubit.
Incluyen a la compuerta NOT la cual es expresada por el operador de Pauli

σ_x, y a la compuerta Hadamard

$$\mathrm{H} = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$$

cuya transformación

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

Ambas compuertas son auto-inversas, esto es, el cuadrado de ellas da el operador identidad.

Compuertas de dos qubits.
Para la compuerta CNOT:

$$\mathrm{CNOT}_{12}|i\rangle_1|j\rangle_2 = |i\rangle_1|i \otimes j\rangle_2$$

en donde $i, j = 0, 1$ son los estados bases de los qubits.

Para la compuerta SWAP, construida a partir de compuertas CNOT:

$$\mathrm{SWAP}_{12} = \mathrm{CNOT}_{12}\mathrm{CNOT}_{21}\mathrm{CNOT}_{12}$$

La cual efectúa la transformación

$$\mathrm{SWAP}_{12} = |i\rangle_1|i\rangle_2 = |j\rangle_1|i\rangle_2$$

Compuertas de 3 qubits:
La compuerta Toffoli y la compuerta Fredkin, las cuales también son conocidas como la NOT-(controlada)^2 y la SWAP-controlada, respectivamente. La compuerta CSWAP realiza la siguiente transformación

$$\mathrm{CSWAP}_{(12)3}|i\rangle_1|j\rangle_2|0\rangle_3 = |i\rangle_1|j\rangle_2|0\rangle_3,$$
$$\mathrm{CSWAP}_{(12)3}|i\rangle_1|j\rangle_2|0\rangle_3 = |j\rangle_1|i\rangle_2|1\rangle_3$$

en donde el tercer qubit es el de control. Todas las compuertas vistas anteriormente son discretas. En la presente sección se darán su versiones contínuas e híbridas.

6.9.1 Con variables contínuas

Compuerta NOT

Bajo estas variables se define como

$$\mathrm{NOT} = (-1)^{a^\dagger a}, \tag{6.5}$$

en donde a y $a^\dagger$ son los operadores bosónicos de aniquilación y creación respectivamente. Por lo que se ve

$$\begin{aligned} \mathrm{NOT}|x\rangle &= |-x\rangle, \\ \mathrm{NOT}|p\rangle &= |-p\rangle, \\ \mathrm{NOT}^2 &= 1 \end{aligned} \tag{6.6}$$

en donde $|x\rangle$ es el eigenstado del operador de posición $\hat{x}$, y p es el eigenstado del operador de momentum $\hat{p}$.

Compuerta Hadamard

La versión contínua de ésta, es la transformada de Fourier y definida como

$$\mathrm{F}(\sigma)|x\rangle = \frac{1}{\sigma\sqrt{\pi}} \int dy e^{\frac{2ixy}{\sigma^2}} |y\rangle, \tag{6.7}$$

donde σ es la longitud escalada. Esta es la trasformación usada para ir desde las bases de posición hasta las de momentum si tomamos $\sigma = \sqrt{2}$. La inversa $\mathrm{F}^\dagger(\sigma)$ se obtiene reemplazando a i por $-i$ dando el resultado

$$\mathrm{F}(\sigma)\mathrm{F}^\dagger(\sigma)|x\rangle = \mathrm{F}^\dagger(\sigma)\mathrm{F}(\sigma)|x\rangle = |x\rangle. \tag{6.8}$$

Nótese que esta compuerta no es auto-inversa.

Compuerta CNOT

Extendida al caso de las variables contínuas, las compuertas CNOT_{12}^{+} y CNOT_{12}^{-}, se definen

$$\mathrm{CNOT}_{12}^{\pm}|x\rangle_1|y\rangle_2 = |x\rangle_1|x \pm y\rangle_2, \tag{6.9}$$

$$\mathrm{CNOT}_{12}^{+} = e^{-i\hat{x}_1\hat{p}_2} \tag{6.10}$$

$$\mathrm{CNOT}_{12}^{-} = \mathrm{NOT}_2 e^{i\hat{x}_1\hat{p}_2} = e^{-i\hat{x}_1\hat{p}_2}\mathrm{NOT}_2 \tag{6.11}$$

en donde el operador de posición del sistema i $(i = 1, 2)$ es definido por medio de $\hat{x}_i$ y el operador de momentum por medio de $\hat{p}_i$. En espacio del momentum la compuerta puede ser definida [Wang, 2001 pg. 3] como

$$\mathrm{CNOT}_{12}^{\pm}|p\rangle_1|q\rangle_2 = |p\rangle_1|p \pm q\rangle_2, \tag{6.12}$$

$$\mathrm{CNOT}_{12}^{+} = e^{i\hat{x}_2\hat{p}_1} \tag{6.13}$$

$$\mathrm{CNOT}_{12}^{-} = \mathrm{NOT}_2 e^{i\hat{x}_2\hat{p}_1} = e^{i\hat{x}_2\hat{p}_1}\mathrm{NOT}_2 \tag{6.14}$$

Las definiciones de las compuertas CNOT son dependientes de las bases. Ambas compuertas son unitarias, esto a partir de las ecuaciones 6.10, 6.11 y 6.14, la compuerta CNOT_{12}^{+} es no Hermitiana y no auto-inversa, mientras que CNOT_{12}^{-} es Hermitiana y auto-inversa.

Compuerta SWAP

Puede ser construida como

$$\begin{aligned}\mathrm{SWAP}_{12} &= \mathrm{NOT}_1\mathrm{NOT}_2\mathrm{CNOT}_{12}^{-}\mathrm{CNOT}_{21}^{-}\mathrm{CNOT}_{12}^{-} \\ &= \mathrm{CNOT}_{12}^{-}\mathrm{CNOT}_{21}^{-}\mathrm{CNOT}_{12}^{-}\mathrm{NOT}_1\mathrm{NOT}_2 \end{aligned} \tag{6.15}$$

$$\mathrm{SWAP}_{12}|x\rangle_1|y\rangle_2 = |y\rangle_1|x\rangle_2 \tag{6.16}$$

O utlizando la compuerta CN_{ij}^{+} y las ecuaciones 6.10 y 6.11

$$\mathrm{SWAP}_{12} = \mathrm{NOT}_2\mathrm{CNOT}_{12}^{-}\mathrm{CNOT}_{21}^{-}\mathrm{CNOT}_{12}^{+} \tag{6.17}$$

$$= e^{i\hat{x}_1\hat{p}_2}\mathrm{NOT}_1 e^{i\hat{x}_2\hat{p}_1} e^{-i\hat{x}_1\hat{p}_2} \tag{6.18}$$

Compuerta NOT-controlada^n

Definiendo [Wang, 2001] una generalización contínua Hermitiana de la compuerta discreta NOT-controlada^n como

$$\begin{aligned}&\mathrm{CNOT}_{(12\ldots N)N+1}^{\pm}|x_1\rangle_1|x_2\rangle_2\ldots|x_N\rangle_N|x_{N+1}\rangle_{N+1} \\ &= |x_1\rangle_1|x_2\rangle_2\ldots|x_N\rangle_N| - x_{N+1} + \sum_{n=1}^{N} x_x\rangle_{N+1}, \end{aligned} \tag{6.19}$$

$$\mathrm{CNOT}_{(12\ldots N)N+1}^{\pm} = \mathrm{NOT}_{N+1}e^{i\hat{p}_{N+1}}\sum_{n=1}^{N}\hat{x}_n \tag{6.20}$$

La compuerta definida en espacio de momentum es unitaria, Hermitiana y auto-inversa. Para el caso de $N = 3$ y 2, la compuerta se convierte en la compuerta Toffoli y CNOT de variable contínua.

Compuerta clonadora de $1 \rightarrow 2$

De ésta sólo es necesario saber que, no viola el Teorema de la No Clonación, Las razones se dan y se describe por [Wang, 2001],

$$C = \mathrm{CNOT}_{31}\mathrm{CNOT}_{21}\mathrm{CNOT}_{13}\mathrm{CNOT}_{12} \tag{6.21}$$

en términos de cuátro compuertas CNOT. Generalizando directamente del caso anterior, obtenemos

$$C' = \mathrm{CNOT}_{31}^{-}\mathrm{CNOT}_{21}^{-}\mathrm{CNOT}_{13}^{-}\mathrm{CNOT}_{12}^{-} \tag{6.22}$$

6.9.2 Híbridas

Ahora toca el turno de presentarse a las dos compuertas híbridas de la CNOT y CSWAP.

Compuerta CNOT

Definida como

$$\mathrm{CNOT}'_{12}|0\rangle_1|x\rangle_2 = |0\rangle_1|x\rangle_2,$$
$$\mathrm{CNOT}'_{12}|1\rangle_1|x\rangle_2 = |1\rangle_1|-x\rangle_2$$

la cual puede realizarse en sistemas de trampa de iones.

Compuerta CSWAP

Una compuerta general de este tipo está descrita por la siguiente transformación

$$|\psi\rangle_1|\Phi\rangle_2|0\rangle_3 \rightarrow |\psi\rangle_2|\Phi\rangle_1|0\rangle_3 \tag{6.23}$$
$$|\psi\rangle_1|\Phi\rangle_2|1\rangle_3 \rightarrow |\psi\rangle_2|\Phi\rangle_1|1\rangle_3 \tag{6.24}$$

La compuerta tiene tres entradas y la tercera es el qubit de control. Sea el estado de entrada de la compuerta $\frac{1}{\sqrt{2}}|\psi\rangle_1|\Phi\rangle_2(|0\rangle_3 + |1\rangle_3)$ y midamos el estado de salida. Si medimos el qubit en el estado $|\pm\rangle_3 = \frac{1}{\sqrt{2}}(|0\rangle_3 \pm |1\rangle_3)$, obtenemos exactamente los estados enredados $|\psi\rangle_1|\Phi\rangle_2 \pm |\Phi\rangle_2|\psi\rangle_1$. Esta compuerta es un enredador universal. Considerándola en la forma 6.23 cuando los estados $|\psi\rangle_1$ y $|\Phi\rangle_2$ son de variables contínuas, a partir de 6.18, la CSWAP formalmente se construye como

$$\mathrm{CSWAP}'_{12(3)} = e^{i\hat{x}_1\hat{p}_2\mathcal{P}_3}e^{i\pi a_1^\dagger a_1\mathcal{P}_3}e^{i\hat{x}_2\hat{p}_1\mathcal{P}_3}e^{-i\hat{x}_1\hat{p}_2\mathcal{P}_3} \tag{6.25}$$

donde $\mathcal{P}_3 = |1\rangle_3\langle 1|$ es el operador de proyección del sistema de control 3.

6.10 La compuerta fundamental de dos qubits

Después que Bennet en 1973 anuncia que la computación puede ser reversible, a finales de los setentas, Tom Toffoli investiga como ésta podría ser hecha con el lenguaje tradicional de las compuertas lógicas Booleanas. Él demostró que un conjunto de compuertas modificadas podría ser usado en lugar de las compuertas lógicas Booleanas. Una de éstas, la cual resultó ser de mucha importancia en los trabajos subsecuentes de compuertas cuánticas, es la compuerta XOR reversible o NOT-controlada, ya descrita generalmente.

La implementación de la compuerta C-NOT puede hacerse con la espectroscopia ENDOR (Electron-Nucleus Double Resonance) [DiVicenzo, 1997 pg. 6], pero esto en realidad es sólo una simulación del comportamiento de la compuerta. ENDOR es usada en muchos contextos como Biología, Física y Química para transferir la polarización (alta) de un electrón hacia el núcleo (inicialmente no polarizado).

Lo importante para la construcción de ésta compuerta son sus propiedades más importantes:

(i) La XOR es la operación idealizada discreta que produce estados cuánticos enredados. Como la indica la figura 6a, una entrada particular producto-estado hacia la compuerta, usando dos estados a partir de bases no ortogonales (relacionadas mediante la transformada Hadamard), produce a la salida el estado no producto $\frac{1}{2}(|01\rangle - |10\rangle)$, un estado equivalente al par Einstein-Podolsky-Rosen-Bohm.

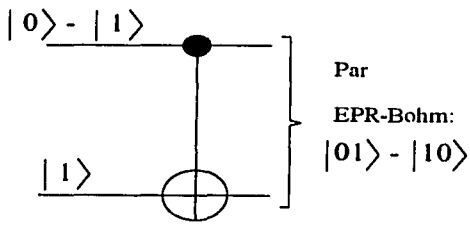


Figura 6a. La XOR produce perfectamente estados cuánticos enredados a partir de los no enredados.

(ii) Como Deutsch lo determinó en 1989, la XOR también funciona como

una "compuerta de medición" A lo que se refiere con esto se muestra en la figura 6b: si el objetivo es medir el estado del qubit superior ($|0\rangle$ o $|1\rangle$), podemos hacerle una XOR con un segundo bit inicialmente en el estado $|0\rangle$; entonces una medición del segundo bit revelará el resultado esperado. Esto puede no parecer de mucha ventaja sobre la medición del primer qubit directamente. Sin embargo, tiene la característica de ser una medición "no demoledora" [DiVicenzo, 1997 pg. 6] en la cual, el estado cuántico original permanece en existencia después de la medición. Permanece así solamente si está en el estado $|0\rangle$ o $|1\rangle$; porque si se inicia en una superposición, el estado es "colapsado" por la medición.

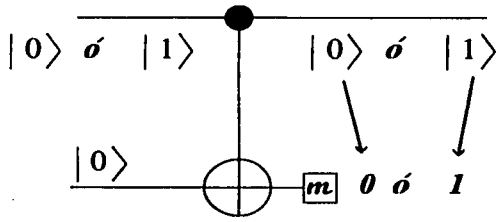


Figura 6b. La XOR funciona como un aparato de medición ideal para el qubit.

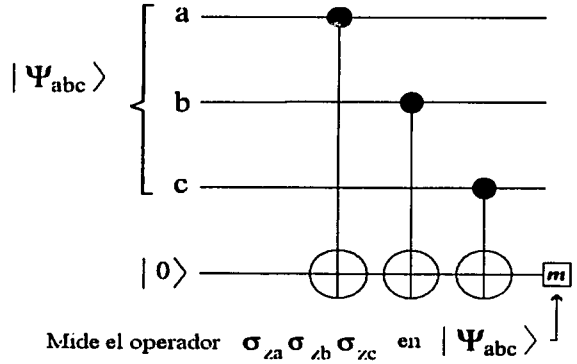


Figura 6c. Un circuito con XOR's puede ser usado para realizar una medición no demoledora de los operadores de tres partículas.

(iii) Para apreciar la capacidad de la compuerta al medir, considere el circuito cuántico simple de la figura 6c. El efecto de las tres XOR's sucesivas, seguido por una medición del qubit objetivo es alcanzar una medición altamente no trivial y sin "demoler" de los operadores Hermitianos de tres partículas $\sigma_{za}\sigma_{zb}\sigma_{zc}$. Todas las dicusiones [DiVicenzo, 1997 pg. 7] siempre asumían que tendría que ser necesario el hacerlo de una manera "demoledora" en donde cada uno de los tres operadores fueran medidos separadamente. Esta propiedad forma los principios del uso de la compuerta XOR en la implementación de corrección de errores y por tanto en la computación tolerante a fallas.

Bibliografía

[1] Abe Hideaki y Shao Chin Sung, *Parallelizing with Limited Number of Ancillae*; Escuela de Ciencia de la Información, Instituto Avanzado de Ciencia y Tecnología Japón, Ishikawa, Japón. 2000.

[2] Aharonov y Michael Ben-or; *Fault-tolerant quantum computation with constant error rate*; Una versión preliminar de este formato, fue publicada en Proceedings of the 29th Annual Symposium on Theory of Computation (STOC) 1997. Escuela de matemáticas, Instituto para Estudios Avanzados, Princeton, New Jersey. Departamento de Ciencia Computacional, La Universidad Hebrea, Jerusalem, Israel. Junio de 1999. e-print: quant-ph\9906129.

[3] Barenco Adriano(1), Charles H. Bennett (2), Richard Cleve (3), David P. DiVicenzo (2), Norman Margolus (4), Peter Shor (5), Tycho Sleator (6), John Smolin (7)y Harald Weinfurter (8), *Elementary gates for quantum computation*;(1) Oxford University; (2) IBM Research; (3) University of Calgary; (4) MIT; (5) AT& T Bell Labs; (6) New York Univ.; (7) UCLA; (8) Univ. of Innsbruck. Enviado a Physical Review A, 22 de marzo de 1995 (AC5710)

[4] Barenco Adriano, *A universal two-bit gate for quantum computation*; Universidad de Oxford, Reino Unido. Mayo de 1995. e-print: quant-ph\9505016.

[5] DiVicenzo David P., *Quantum Gates and Circuits*, e-print: quant-ph\9705009.

[6] Ekert Artur, Patrick Hayden y Hitoshi Inamori, *Basic concepts in quantum computation*; Centro para la Computación Cuántica, Universidad de Oxford, Reino Unido. Noviembre de 2000.

[7] Fortnow Lance, *One Complexity Theorist's view of Quantum Computing*; Basado en una charla presentada en el Segundo Taller sobre Algoritmos en el Procesamiento de Información Cuántica en la Universidad DePaul, Chicago, enero de 1999. Instituto de Investigaciones NEC, 4 Independence Way, Princeton, NJ 08540. Marzo de 2000. El Real audio de la charla está disponible en www.cs.depaul.edu/aqip99.

[8] Hayes Brian, *The square root of NOT*; Conceptos publicados en American Scientist, de julio a agosto de 1995.

[9] Kauffman Louis H., *Quantum Computing and the Jones polynomial*; Departamento de Matemáticas, Estadística y Ciencia de la Computación. Universidad de Illinois en Chicago, Mayo de 2001. e-print: quant-ph\0105255.

[10] Knill E.H. y M.A. Nielsen; *Theory of quantum computation*; Artículo, ver también "www.wkap.nl/series.htm/ENM". Octubre de 2000.

[11] Leung Debbie W., *Towards robust quantum computation*; Disertación enviada al Departamento de Física y al Comité de Estudios de Grado de la Universidad de Stanford en cumplimiento parcial de los requerimientos para el grado de Doctor en Filosofía. Julio de 2000.

[12] Lloyd Seth y Samuel L. Braunstein, *Quantum computation over continuos variables*. 27 de octubre de 1998.

[13] Lloyd Seth, *Hybrid quantum computing*; 11 de agosto de 2000. e-print.

[14] Lomonaco Samuel J., Jr.*A Rosetta Stone for quantum mechanics with an introduction to quantum computation*. Primera de ocho ponencias dadas en la Sociedad Matemática Americana AMS Curso breve sobre Computación Cuántica organizado en conjunción con la Reunión Anual de la AMS en Washington, DC, USA en enero de 2000, y será publicado en el volumen de la AMS PSAPM titulado "Quantum Computation".

[15] Wang Xiaoguang, *Continuos-variable and hybrid quantum gates*; Institute of Physics and Astronomy, Aarhus University, Denmark. 16 de abril de 2001.

Capítulo 7

Interferómetros

Las computadoras cuánticas difieren de las clásicas en el uso de la superposición de los estados no locales. Una computadora cuántica es un interferómetro sofisticado el cual está programado para interferir constructivamente respuestas correctas y a las incorrectas destructivamente. De aquí nuestro paso por la interferometría; y aún más, la no-localidad permitida en la mecánica cuántica puede ser utilizada para alcanzar soluciones exponencialmente rápidas [Chuang et. al, 1998 pg. 1].

7.1 Condiciones para la interferencia

Fundamentalmente, toda interferencia surge cuando se combinan los campos electromagnéticos que constituyen las ondas individuales.

Para alcanzar interferencia sostenida, deben cumplirse las siguientes condiciones [Serway, 1997 pg. 1096]:

- Las fuentes deben ser **coherentes**, es decir, deben mantener una fase constante entre sí.
- Las fuentes deben ser **monocromáticas**, esto es, de una sola longitud de onda.
- Debe aplicarse el principio de superposición. Esta condición refleja la condición esencial de que un fotón sólo puede interferir consigo mismo.

Con el fin de producir un patrón de interferencia estable, coherencia, *las ondas luminosas deben mantener una relación de fase constante entre sí.*

7.2 El interferómetro de Michelson

Este aparato, inventado por el físico estadounidense A. A. Michelson (1852-1932), divide un haz luminoso en dos partes y después las recombina para formar un patrón de interferencia.

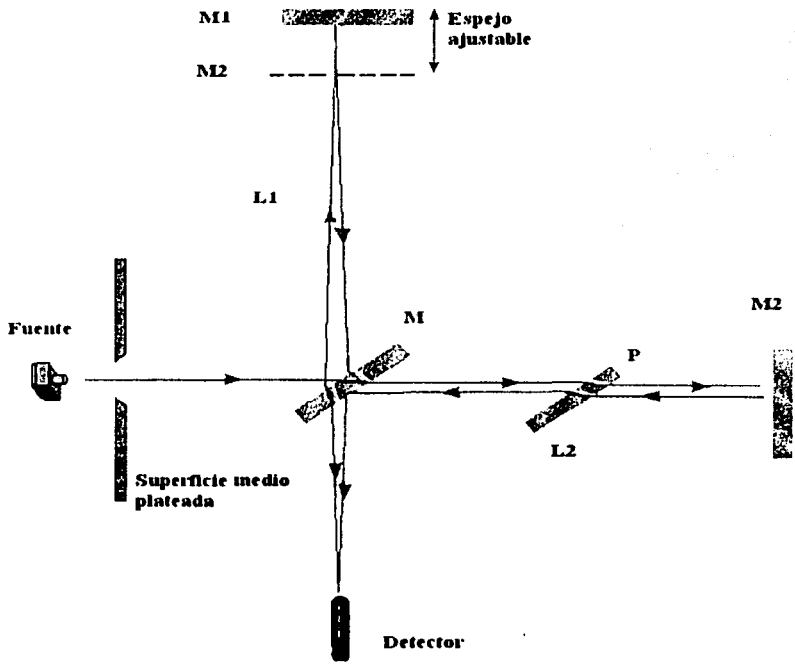


Figura 7a. Diagrama del interferómetro de Michelson

Un diagrama esquemático del interferómetro se muestra en la figura 7a. Un haz de luz proporcionado por una fuente monocromática se divide en dos rayos por medio de un espejo parcialmente plateado M inclinado a 45° en relación con el haz de luz incidente. Un rayo se refleja verticalmente hacia arriba, hacia el espejo M1, en tanto que el segundo rayo se transmite horizontalmente a través de M hacia el espejo M2. Por lo tanto, los dos rayos recorren trayectorias independientes L1 y L2. Después de reflejarse en

M1 y M2, los dos rayos se recombinan finalmente para producir un patrón de interferencia, el cual puede verse a través de un detector. La placa de vidrio P, de igual espesor que el espejo M, se coloca en la trayectoria del rayo horizontal para asegurar que los dos rayos recorran la misma distancia a través del vidrio.

La condición de interferencia para los dos rayos se determina por la diferencia de sus longitudes de trayectoria óptica. Cuando los dos rayos son vistos como se muestra, la imagen de M2 está en M'2 paralela a M1. Por lo tanto, M'2 y M1 forman el equivalente de una película de aire. El espesor efectivo de la película de aire varía moviendo el espejo M1 a lo largo de la dirección del haz de luz con un tornillo de rosca fina. En estas condiciones, el patrón de interferencia es una serie de anillos brillantes y obscuros. Si un círculo obscuro aparece en el centro del patrón, los dos rayos interfieren destructivamamente. Si M1 se mueve después una distancia $\lambda/4$, la diferencia de trayectoria cambia en $\lambda/2$ (el doble de la separación entre M1 y M'2). Los dos rayos ahora interfieren constructivamente, dando un círculo brillante a la mitad. A medida que M1 se mueve una distancia adicional $\lambda/4$, otro círculo obscuro aparece en el centro del patrón. Así, vemos que círculos sucesivos obscuros o brillantes se forman cada vez que M1 se mueve una distancia de $\lambda/4$. La longitud de onda de la luz se mide después contando el número de franjas corridas para un desplazamiento determinado de M1. Por el contrario, si la longitud de onda se conoce con precisión (como con un haz láser), los desplazamientos del espejo pueden medirse hasta una fracción de una longitud de onda.

7.3 Interferencia de una sola partícula

Aplicando el concepto anterior, pero a nivel de partículas elementales, nos damos cuenta que un fotón no puede ser dividio en dos por el espejo parcialmente plateado: cuando enviamos un fotón hacia dicho espejo es detectado con igual probabilidad, ya sea en un detector A o en un detector B. Esto no significa que el fotón deje el espejo al azar en la posición horizontal (H) o vertical (V). De hecho el fotón toma ambos caminos a la vez. Como es ilustrado en la figura 7b. Lo anterior puede ser demostrado con la ayuda del aparato que se muestra en la figura 7c. Dos espejos normales son colocados de tal manera que realizen la intersección en el segundo espejo parcialmente plateado. Con este arreglo podemos observar el fenómeno de la interferencia de una partícula con ella misma.

Supongamos que un fotón sigue el camino horizontal marcado con H en la figura 7c después de pasar a través del espejo. Entonces (comparándolo con la figura 7b) deberíamos encontrar que ambos detectores registraron golpes con igual probabilidad. Ocurriría exactamente lo mismo si el fotón siguiera el camino vertical V. De aquí que si el fotón toma cualquier camino a través del aparato, en promedio, los detectores A y B lo sensarían con igual probabilidad cada vez que el experimento se realize. Sin embargo esto no es así. Resulta que en el arreglo mostrado, el fotón *siempre* llega al detector A y *nunca* al detector B.

Figura 7b. Un espejo parcialmente plateado refleja la mitad de la luz que incide sobre él

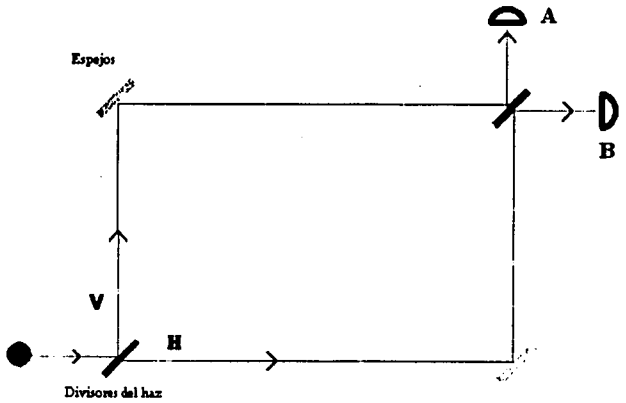


Figura 7c. Interferencia de una sola partícula. Un fotón que entra al interferómetro siempre golpea al detector A y nunca al B.

La inescapable conclusión es que el fotón debe haber viajado, de alguna forma, ambas rutas al mismo tiempo - como si cualquiera de los dos caminos fuera bloqueado por una pantalla absorbente, inmediatamente la probabilidad es la misma de que A o B sean golpeados. En otras palabras, "desbloqueando" cualquiera de las dos trayectorias ilumina a B; con ambas trayectorias abiertas, el fotón de algún modo recibe información que lo previene de alcanzar B [Deutsch y Ekert, 1998 pg. 2], la información que viaja a lo largo del otro camino a la velocidad de la luz, reflejándose en el espejo, exactamente como un fotón lo haría. Esta propiedad de interferencia cuántica se aplica no solo a las partículas sino a todos los sistemas físicos.

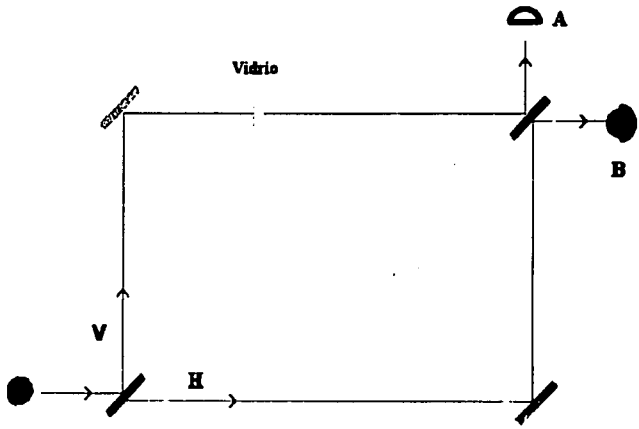


Figura 7d. Una astilla de vidrio en cualquiera de las dos trayectorias puede redireccionar a los fotones desde un detector hacia el otro.

Un efecto que es especialmente útil en la computación cuántica puede ser demostrado si retardamos el fotón en cualquiera de los caminos H o V. Esto puede ser hecho insertando una astilla de vidrio en dicho camino, como se ilustra en la figura 7d. Ya que la interferencia entre el fotón y su contraparte invisible depende de sus tiempos exactos de llegada, podemos, por ejemplo, elegir el ancho del vidrio y por tanto el tiempo de retardo de tal manera que el fotón llegue al detector B en lugar del detector A.

Como el fotón puede estar en una superposición coherente de estar en el camino H o V, cualquier qubit puede ser preparado en una superposición de sus dos estados lógicos 0 y 1. Así es como el qubit puede almacenar un 0 o 1 en proporciones arbitrarias. Pero si se mide el qubit, sólo uno de los dos estados será detectado.

Cualquier registro cuántico de n qubits podrá almacenar hasta 2^n combinaciones haciendo uso de los dispositivos anteriores. Si los qubits son átomos, entonces pulsos ajustados de laser sintonizados afectarían sus estados electrónicos y evolucionarían a las superposiciones iniciales de números codificados en diferentes superposiciones.

7.4 Construcción de compuertas

En principio sabemos como construir computadoras cuánticas, iniciamos con simples compuertas y las conectamos hasta crear redes cuánticas.

Una compuerta lógica cuántica, al igual que una clásica es un dispositivo simple de computación que ejecuta una operación elemental en un tiempo dado, pero éstas pueden crear y ejecutar operaciones un superposiciones cuánticas.

Sin embargo, a medida que se incrementa el número de compuertas en una red, más qubits interactuantes se involucran y se hace más difícil controlar la interacción de la interferencia cuántica. A parte de las dificultades técnicas al trabajar con escalas de una sola partícula o átomo, uno de los problemas más importantes es la decoherencia, porque ocasiona que la información salga de la computadora y se pierda en el medio ambiente. Nuestra tarea es "ingenierizar" los sistemas submicroscópicos para que los qubits interactuen solamente entre ellos.

Mientras tanto podemos dar el siguiente acercamiento a la compuerta $\sqrt{\text{not}}$.

En lógica no existe una operación razonable como la raíz cuadrada de NOT, lo que implica que la máquina tampoco. Pero existe. La construcción de tal se aprecia en la figura 7b.

La representación esquemática de la misma compuerta se puede ver en

la figura 7b.1.

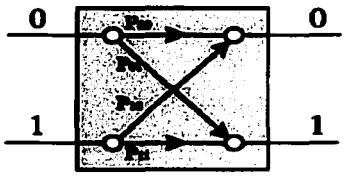


Figura 7b.1. Representación esquemática de la compuerta $\sqrt{\text{NOT}}$. Aquí p_{ij} es la probabilidad de que la mquina produzca la salida j cuando se presenta la entrada i.

Esta compuerta da un 0 o 1 con igual probabilidad e independientemente del valor en la entrada. Pero cuando dos compuertas se conectan en serie, actuando independientemente, producen la operacin lgica NOT, eso es el porque se le llama a esta compuerta $\sqrt{\text{NOT}}$. Esto no va a la par de las suposiciones usuales.

Para entenderlo, hay que recordar el concepto de *amplitudes de probabilidad* -números complejos c tal que las cantidades $|c|^2$ pueden ser interpretadas, bajo condiciones apropiadas, como probabilidades. Cuando una transición, como "una máquina compuesta de dos sub-máquinas idénticas inicia en el estado 0 y genera la salida 0, y nada más pasa", puede ocurrir en varias formas alternas, la amplitud de probabilidad total para la transición es la suma, no de las probabilidades, sino de las amplitudes de probabilidad para cada una de las transiciones constituyentes consideradas separadamente.[Deutsch et. al, 1999 pg. 8].

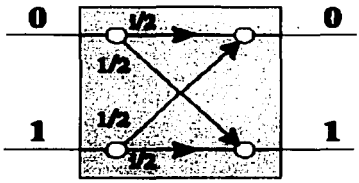


Figura 7e. Las transiciones en las máquinas cuánticas se describen con amplitudes de probabilidad. Son números complejos tal que su módulo puede ser interpretado, bajo situaciones convenientes, como probabilidades.

En la máquina $\sqrt{\text{NOT}}$, la amplitud de probabilidades de las transiciones $0 \mapsto 0$ y $1 \mapsto 1$, ambas son $i/\sqrt{2}$, y la amplitud de probabilidades para las transiciones $0 \mapsto 1$ y $1 \mapsto 0$ es $1/\sqrt{2}$. Esto significa que la máquina $\sqrt{\text{NOT}}$ preserva el valor del qubit con la amplitud de probabibilidad $c_{00} = c_{11} = i/\sqrt{2}$ y lo niega con la amplitud de probabilidad $c_{01} = c_{10} = 1/\sqrt{2}$. Para obtener las probabilidades correspondientes tenemos que tomar el cuadrado del módulo de las amplitudes de probabilidad el cual da un medio para ambos casos, preservar e intercambiar el valor del qubit. Esto describe el comportamiento de la máquina $\sqrt{\text{NOT}}$, en la figura 7b.1. Sin embargo, cuando concatenamos las dos máquinas, como en la figura 7b.2, entonces, para calcular la amplitud de probabilidad de la salida 0 a la entrada 0, tenemos que sumar las amplitudes de probabilidad de todos los caminos que guían a la entrada 0 a la salida 0. Hay sólo dos de ellas $-c_{00}c_{11}$ y $c_{01}c_{10}$. El primer camino tiene la amplitud de probabilidad $i/\sqrt{2} \times i/\sqrt{2} = -1/2$ y la segunda $1/\sqrt{2} \times 1/\sqrt{2} = 1/2$. Primero sumamos las dos amplitudes y luego obtenemos el cuadrado del módulo de la suma. Encontramos que la probabilidad de la salida 0 es cero. A diferencia de las probabilidades, las amplitudes de probabilidad pueden cancelarse la una a la otra.

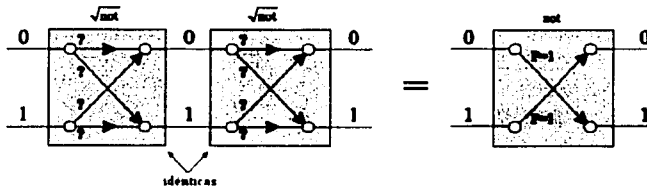


Figura 7b.2. Concatenación dos máquinas idénticas.

La realización experimental de la concatenación de las dos compuertas $\sqrt{\text{NOT}}$ se ve en la figura 7c.

Bibliografía

[1] Chuang L. Isaac, Raymond Laflamme y Yoshihisa Yamamoto, *Decoherence and a Simple Quantum Computer.*

[2] Deutsch David and Artur Ekert, *Quantum Computation*; Artículo de 'Physics World', número de marzo de 1998.

[3] Deutsch David, Artur Ekert y Rosella Lupacchini; *Machines, Logic and Quantum Physics*, 19 de noviembre de 1999. e-print: quant-ph\9911150.

[4] Serway Raymond A., *Física*; McGraw-Hill, Tomo 2, cuarta edición, 1996.

Capítulo 8

Decoherencia

Aquí se abordará uno de los temas principales en la contrucción de los dispositivos cuánticos. El tema, en sus conceptos generales no es muy extenso, razón válida para cubrir solamente lo que a nuestros fines interesa.

8.1 Conceptos generales

Durante los últimos 25 años se hizo claro que un rol crucial, en la transición clásica-cuántica, es representado por el ambiente natural de un sistema cuántico. Las propiedades clásicas emergen de manera irreversible a través de la inevitable interacción con los ubicuos grados de libertad del medio ambiente - proceso conocido como *decoherencia.*

Veamos en detalle algunos de los mecanisnos y fenómenos que surgen de la interacción de un (posiblemente macroscópico) sistema cuántico con su ambiente. No es necesario decir que todos los efectos dependen de la fortaleza del acoplamiento entre el grado de libertad considerado y el resto del mundo. Puede sorprender, sin embargo que, aún el esparcimiento de un fotón o la interacción gravitacional con objetos muy lejanos pueden guiar a efectos dramáticos. Algunos resultados análogos se pueden encontrar en la teoría clásica (èg. La influencia de una pequeña masa situada en Sirio sobre la trayectoria de las moléculas de aire aquí en la Tierra ; o El Efecto Mariposa), pero en al teoría cuántica encontramos un fenómeno característico la destrucción de la coherencia. En cierto modo esto constituye una violación del principio de superposición: ciertos estados ya no pueden ser medidos, aunque éstos sean permitidos por la teoría. Irónicamente, esta "violación" es una consecuencia de la asumida validez no restringida del principio de su-

perposición. La destrucción de la coherencia -y para alguna extensión de las propiedades clásicas- fue tomado en cuenta por los pioneros de la mecánica cuántica (Landau 1927, Mott 1929, y Heisenberg 1958). En aquellos días y aún después, la influencia del medio ambiente fue vista como una forma de perturbación, ejercida por una fuerza (clásica). Todavía en nuestros días esas ideas están por todos lados, aunque sean completamente incompatibles con la teoría cuántica.

8.2 Decoherencia y mediciones

Los mecanismos que son más importantes para el estudio del fenómeno de la decoherencia tienen mucho en común con aquellos que surgen en la teoría cuántica de las mediciones. Se discuten las reacciones de un punto de masa con su medio ambiente con algo de detalle. Si el punto de masa es macroscópico -un grano de polvo- el esparcimiento de fotones o de moléculas de gas transferirán información sobre la posición del grano de polvo en el ambiente. En este sentido, la posición del grano es "medida" en el transcurso de su interacción: El estado del resto del universo (al menos del fotón) obtiene información acerca de su posición.

Obviamente la reacción en respuesta será despreciable en tal caso, de aquí que tengamos una medición "ideal": Sólo el estado del "aparato" (en nuestro caso el fotón) cambiará apreciablemente. Por lo tanto no hay perturbación de ningún tipo en el sistema medido, en llamativo conflicto con las tempranas interpretaciones de la teoría cuántica.

Un tratamiento completo de los casos reales tiene que incluir al Hamiltoniano gobernando la evolución del sistema al igual que la del ambiente. La dinámica exacta de un subsistema es muy difícil de manejar, formalmente está dada por una ecuación integro-diferencial [Kiefer y Joos, 1997 pg. 107].

Bibliografía

[1] Kiefer Claus y Erich Joos, *Decoherence: Concepts and examples.* Proceedings of the Xth Max Born Symposium en Przesieka, Polonia. Del 24 al 27 de septiembre de 1997. pg. 105-128. Springer.

Capítulo 9

Construcción

El camino presuntivo hacia la computadora cuántica incluye [Freedman et. al, 2001 pg. 4], de manera muy general: construir qubits y compuertas, minimizar los niveles de error, y que las compuertas estén protegidas contra la decoherencia. Impresiciones y decoherencia pueden ser consideradas en una forma unificada como "errores".

El presente capítulo describirá las técnicas con las que han estado experimentando para la realización física de las computadoras. Las trampas de iones han presentado resultados muy interesantes [Hai et. al, 2000 pg. 1408]; Con la técnica NMR fue posible hacer la computadora cuántica de siete qubits mencionada al inicio; el proceso de creación partícula-antipartícula especifican operaciones unitarias; se intenta hacer un transistor con solo un electrón [Levy, 2001 pg. 1].

Mientras que la teoría de la computación cuántica está bien entendida, construir una computadora cuántica ha probado ser extremadamente problemático. Varios acercamientos han sido estudiados, a parte de los ya mencionados, pero hasta ahora sólo ha sido posible demostrar las operaciones más simples, por ejemplo, la operación NOT mediante una transición simulada entre dos niveles de energía $|0\rangle, |1\rangle$, la operación XOR puede identificarse con una transición dirigida de un sistema de cuatro niveles.

Es muy complicado encontrar tales sistemas. Esperaríamos fabricar dispositivos cuánticos en microchips de estado sólido - aunque ahora exiten dichos dispositivos solamente utilizan los principios de la teoría cuántica como se instruye en el texto [Yariv, 1988]- esta es la progresión lógica de las

técnicas de microfabricación que han permitido a las computadoras clásicas ser tan potentes. No obstante, la computación cuántica cuenta con los efectos complicados de interferencia y el problemas mayor, el ruido. Ningún sistema cuántico está realmente aislado, la decoherencia destruye la computación. En los dispositivos de estado sólido, el ambiente es el substrato y el acoplamiento con este ambiente es muy fuerte, produciendo tiempos de decoherencia típicos del orden de picosegundos. Es importante darse cuenta que no es suficiente tener a los dos estados $|0\rangle$ y $|1\rangle$ en forma estable, también se requiere que las superposiciones tales como $|0\rangle + |1\rangle$ preserven su fase, y esto no se alcanza cuando los tiempos para la decoherencia son muy cortos.

Aún no hay una implementación satisfactoria para decidir cual técnica se va a emplear; en el presente hay dos candidatos que permitirían la computación con 10 y hasta 40 qubits. Estas son las propuestas de la trampa de iones y la de resonancia magnética nuclear. En ambos casos, al igual que toda la tesis, confíamos en los impresionantes esfuerzos de la gran comunidad de investigadores que desarrollaron las técnicas experimentales. Hubo previas propuestas para la computación cuántica las cuales tocaron algunos métodos importantes pero no fueron experimentalmente asequibles. Hay otras más en el terreno del estado sólido que pueden ser realizables en el futuro.

9.1 Resonancia Magnética Nuclear

La propuesta del uso con resonancia magnética nuclear (NMR) se ilustra en la figura 9a. El procesador cuántico en este caso es una molécula que contiene una "espina dorsal" de alrededor de 10 átomos, con otros átomos como el de Hidrógeno adherido de tal manera que se usen todos los enlaces químicos. Es el núcleo el que nos interesa, cada uno tiene su momento magnético asociado con el espín nuclear, y los estados del espín dan los qubits. La molécula es puesta en un campo magnético, y los estados del espín del núcleo son manipulados aplicando campos magnéticos oscilantes en forma de pulsos de duración controlada.

Aquí lo que se usa son los dos estados del espín de un núcleo atómico de espín 1/2 en un campo magnético. Se pueden distinguir átomos diferentes en una molécula, y de esta manera una puede ser usada como una computadora cuántica, con cada núcleo de espín 1/2 representando a un qubit. Las

compuertas de un solo qubit son fácilmente implementadas aplicando pulsos de radio frecuencia sintonizados a las frecuencias de Larmor de los espines [Laflamme et. al, 2000 pg. 1], los cuales interactúan fuertemente con los espines nucleares lo que permite controlarlos con gran precisión. El enredo y las operaciones de dos espines se logran con retardos para permitir la interacción entre los espines. Para las compuertas más complejas el estado de un qubit interactúa con los demás qubits de tal forma que el otro qubit puede "sentir" su estado.

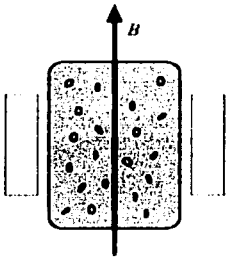


Figura 9a. Procesador de información cuántica NMR. Un líquido de $\sim 10^{20}$ moléculas es colocado en un magnetómetro sensitivo, el cual puede generar campos magnéticos oscilantes y también detectar la precesión de la media del momento magnético del líquido, la situacióin equivale a tener 10^{20} qubits. La información cuántica es almacenada y manipulada en los estados nucleares del espín. Los niveles de energía de los estados del espín de un núcleo dado son influenciados por el núcleo circundante en la molécula, lo cual crea a las compuertas XOR.

El procesamieto de información puede dividirse en tres pasos [Laflamme et. al, 2000 pg. 1] que consisten en la preparación, computación y lectura. Cada uno de estos pasos es equivalente a una operación de ciertas operaciones cuánticas idénticas a cada miembro del grupo. El problema está en la lectura del estado del espín. La señal NMR de una sola molécula es muy débil para ser detectada, por lo que se tiene que usar una gran cantidad de copias para amplicar la señal, el líquido debe contener alrededor de 10^{20} moléculas. Lo que es imposible es asegurar que todas las copias inicien en el mismo estado, lo cual dificulta medir el resultado deseado.

Cuando se prepara el estado inicial, el líquido está en equilibrio térmico, así los diferentes estados del espín tienen probabilidades de posición dadas

por la distribución de Boltzman [Steane, 1997 pg. 35]. Se hace uso del hecho que los estados del espín son cercanos en energía y por tanto tienen posiciones iguales.

Este método no es muy bueno cuando el número de qubits se incrementa, por ejemplo, con n qubits la señal medida se escala a 2^{-n}. También se limita la posibilidad de medir el estado, ya que solamente el estado promedio es detectable. Esto restringe la habilidad al aplicar la corrección de errores, y complica el diseño de los algoritmos cuánticos. Pero los tiempos para la decoherencia son muy largos.

Una demostración formal de como esta técnica puede ser implementada haciendo que la relación señal/ruido dependa solamente de la tecnología NMR y no del tamaño de la computadora se da en todo el escrito de [Schulman y Vazirani, 2000], con pasos desde la preparación hasta el proceso de amplificación de la señal.

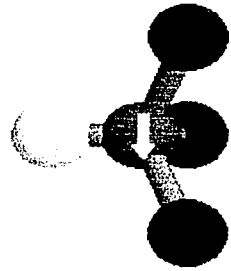


Figura 9b. Los núcleos ^1H y ^{13}C se comportan como magnetos e interactúan con un campo magnético externo. Los espines nucleares alineados con el campo corresponden a los qubits en el estado $|0\rangle$ mientras que los alineados contra el campo corresponden al estado $|1\rangle$. Los tres núcleos clorados, mostrados en verde, pueden ser ignorados. Con esta molécula se logró crear las primeras computadoras cuánticas de 2 qubits [Jones, 1997 pg. 1].

9.2 La trampa de iones

El método de la trampa de iones se ilustra en la figura 9c, y se describe en detalle en [Steane, 1996 v2]. Una cadena de iones es confinada por medio de campos eléctricos oscilantes y estáticos en una "trampa de Paul" lineal al alto vacío ($\sim 10^{-8}$Pa). Un haz láser es dividido en varios pares por medio de espejos semi-plateados y moduladores acusto-ópticos, cada par ilumina a un solo ión.

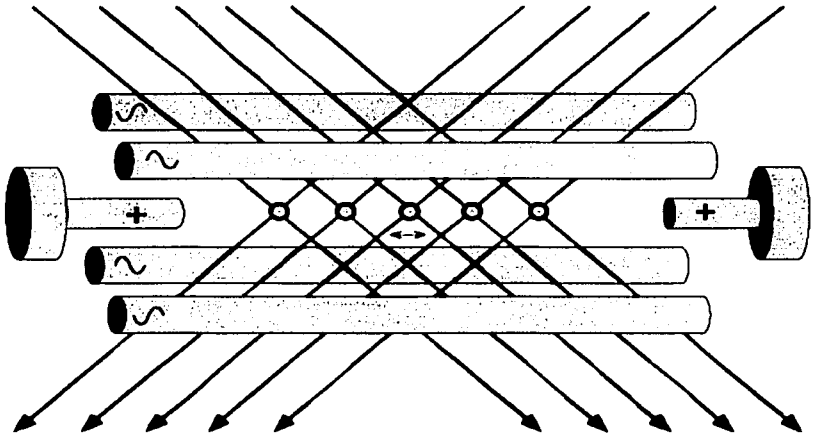


Figura 9c. El procesador de trampa de iones. Una cadena de átomos individualmente cargados es almacenada en una trampa de iones. Los iones están separados por $\sim 20\mu$m por repulsión mutua. Cada ión es direccionado por un par de haces láser los cuales coherentemente manejan ambas transiciones en los iones, y también las transiciones en el estado de movimiento de la cadena. El grado de libertad de movimiento sirve como un 'bus' de un solo qubit que transporta la información cuántica entre los iones. La preparación del estado es por medio de bombeo óptico y enfriamiento por láser; la lectura es hecha al encerrar al electrón (electron shelving) y con resonancia fluorescente.

Cada ión tiene dos estados de larga duración, por ejemplo, diferentes niveles del estado principal con estructura hiperfina (la larga duración de esos estados contra el decaimiento espontáneo puede exceder los miles de años). Refirámonos a estos dos estados como $|g\rangle$ y $|e\rangle$; son ortogonales y juntos representan a un qubit. Cada par láser puede manejar transiciones coherentes entre los estados internos del ión relevante. Esto permite que

cualquier compuerta de un qubit sea aplicada a cualquier ión, pero no a compuertas de dos qubits. Las últimas requieren una interación entre los iones, y esta es provista por la repulsión de Coulomb.

Cuando un par láser interactúa con el ión intercambian momentums. De hecho, la repulsión mutua de los iones significa que toda la cadena de iones se mueve "en masa" cuando el movimiento se cuantiza (Efecto Mössbauer). El movimiento de la cadena de iones se cuantiza porque la cadena de ioines está confinada en el potencial provisto por la trampa. Los estados cuánticos del movimiento corresponden a los diferentes grados de excitación ('fonones') de los modos normales de vibración de la cadena. En particular se enfoca en el estado principal del movimiento $|n = 1\rangle$ del modo fundamental. Para lograr, por ejemplo la Z-controlada entre el ión x y el ión y, se empieza con el movimiento del estado principal $|n = 0\rangle$. Un pulso de los láser sobre el ión x conduce la transición $|n = 0\rangle|g\rangle_x \rightarrow |n = 0\rangle|g\rangle_x, |n = 0\rangle|e\rangle_x \rightarrow |n = 1\rangle|g\rangle_x$, así el ión termina en el estado principal, y el movimiento termina en el estado inicial del ión: esto es una operación SWAP. Luego un pulso de los haces láser sobre el ión y conduce la transición

$$|n = 0\rangle|g\rangle_y \rightarrow |n = 0\rangle|g\rangle_y \tag{9.1}$$
$$|n = 0\rangle|e\rangle_y \rightarrow |n = 0\rangle|e\rangle_y \tag{9.2}$$
$$|n = 1\rangle|g\rangle_y \rightarrow |n = 1\rangle|g\rangle_y \tag{9.3}$$
$$|n = 1\rangle|e\rangle_y \rightarrow -|n = 1\rangle|e\rangle_y \tag{9.4}$$

finalmente se repite el pulso inicial sobre el ión x. El efecto completo de los tres pulsos es

$$|n = 0\rangle|g\rangle_x|g\rangle_y \rightarrow |n = 0\rangle|g\rangle_x|g\rangle_y$$
$$|n = 0\rangle|g\rangle_x|e\rangle_y \rightarrow |n = 0\rangle|g\rangle_x|e\rangle_y$$
$$|n = 0\rangle|e\rangle_x|g\rangle_y \rightarrow |n = 0\rangle|e\rangle_x|g\rangle_y$$
$$|n = 0\rangle|e\rangle_x|e\rangle_y \rightarrow -|n = 0\rangle|e\rangle_x|e\rangle_y$$

Lo cual es exactamente una Z-controlada (descrita por la matriz de Pauli σ_z [Leung, 2000 pg. 9])entre x y y. Cada pulso láser debe tener una frecuencia y duración controlada. La Z-controlada y todas las demás compuertas de un solo qubit forman un conjunto universal de compuertas [Steane, 1997 pg. 35].

La preparación del estado inicial es posible a través de los métodos de bombeo óptico y enfriamiento por láser. Y el proceso de lectura vía

las técnicas de medición 'salto cuántico' o 'encerrando al electrón'. Estas técnicas son empleadas en física atómica. Pero todas éstas sólo han conseguido hacer la computación con solo una trampa de iones.

Recientemente, se han logrado implementar compuertas de dos qubits con cuatro iones enredados [Kielpinski et. al, 2001 pg. 6]

9.3 Estado Sólido

Muchas propuestas de estado sólido han permanecido en etapas de modelo a causa de las inmensas dificultades experimentales. Mientras que las arquitecturas de moléculas y ópticas han sido cruciales en la demostración de los principios de la computación cuántica, generalmente se cree que las arquitecturas de estado sólido, con sus ventajas sobre posibilidades controlables de escalabilidad, ofrecen el potencial más prometedor para realizar el hardware a gran escala [Hu y Das Sarma, 2001 pg. 1]. Las anteriores técnicas demuestran los principios pero encuentran dificultades en la expansión, mientras que en las arquitecturas de estado sólido, las cuales pueden ser fácilmente escalables, no se ha demostrado nisiquiera el qubit.

En esta sección se da una revisión muy general de propuestas de estado sólido para la contrucción de las compuertas. Hay algunos temas que requieren mayores conceptos de los que conciernen a mi estudio, y no por ser menos importantes no se tratan, el ejemplo es la computación con puntos cuánticos [Hu y Das Sarma, 2001*], las nanoestructuras semiconductoras [Reina et. al., 2001], la espectroscopia NMR [Cory, et. al., 1997] o la Microscopia de Fuerza [Berman et. al., 1999]. Es muy extenso el hablar aquí sobre cada tema. Sin embargo, amplia la visión de quienquiera que los lea.

9.3.1 Óptica Lineal

Una propuesta es la de [Knill, Laflamme y Milburn, 2000], ellos establecen en principio realizar las compuertas cuánticas utilizando óptica lineal pasiva con fotodetectores. Su propuesta es conocida como Computación Cuántica con Óptica Lineal (LOQC), y depende de una serie de protocolos ópticos que requieren la preparación y medición del estado de un solo fotón cuyo resultado puede ser usado para controlar otros elementos ópticos. Esto es muy útil puesto que realiza mediciones no-demoledoras con alta eficiencia.

El principal problema con esta propuesta es el acoplamiento no-lineal de dos modos ópticos que contengan algunos fotones. Además satisface las necesidades de medir los resultados de las operaciones ejecutadas por las compuertas cuánticas, pero solo a no muy gran escala. Lo que es importante, es que ya se puede disponer de todos estos elementos ópticos para demostrar el procesamiento de información cuántica. A consecuencia, LOQC tiene más posibilidades en el área de la comunicación cuántica.

9.3.2 Electrones Balísticos

Describe una implementación de la computadora cuántica usando electrones balísticos unitarios [Ionicioiu et. al., 2000 pg. 1] como qubits 'voladores' en nanocables 1D. Preparan el estado inicial, la medición del estado final y un conjunto universal de compuertas. Una ventaja importante de este modelo es el hecho de que no necesita optoelectrónica ultra rápida para la operación de las compuertas. Definen a las compuertas antes de lanzar a los electrones, esto puede ser hecho usando campos eléctricos solamente.

Aquí el qubit consiste en dos cables cuánticos adyacentes 1D, llamados el riel-0 y el riel-1. Definen el estado lógico $|0\rangle$ con la presencia de un solo electrón de energía E_k en el riel-0 y el estado lógico $|1\rangle$ con la presencia de un electrón con la misma energía. La desventaja son sus tiempos muy cortos de decoherencia.

9.3.3 El transistor de Resonancia de Espín de electrón

Se aplica todo el conocimiento de la ingeniería electrónica de estructura de banda para diseñar un transistor que puede sensar y controlar un espín de un solo electrón donador; el diseño del transistor SRT (Spin Resonance Transistor) de efecto de campo podría ser una demostración a corto plazo de qubits en obleas de silicio. [Vrijen et. al, 1999 pg. 1].

La figura muestra al SRT. Y a continuación lo que su estructura intenta hacer: La multi-estructura mostrada es hipotética y comprime a dos dispositivos "SRT". La estructura por arriba del plano base está completamente no dopada, excepto por únicamente dos impurezas donadoras P centradas bajo las compuertas. Estos donadores se intenta que no estén ionizados, y es un electrón débilmente circundado en cada P que actuará como qubit, en realidad el qubit es el espín del electrón. Así, lo que se muestra es un par de dispositivos de un qubit [DiVicenzo 2000+].

Ahora para la inicialización de los qubits en el estado cero, razón por la cual los dispositivos de estado sólido sean criogénicos. Para obtener el espín del electrón donador arriba, es decir, en el estado cero y que se quede ahí, requiere que trabaje alrededor de 1K, y en un campo magnético de 1T.

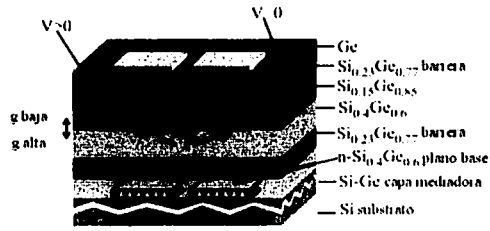


Figura 9d. El transistor de la izquierda se polariza V> 0, produciendo transformaciones unitarias de un qubit en el SRT izquierdo. La compuerta -como en un FET- de la derecha no esta polarizada, V=0. El plano base esta en contra del electrodo de la compuerta y que también actúa como un canal FET para sensar el espín.

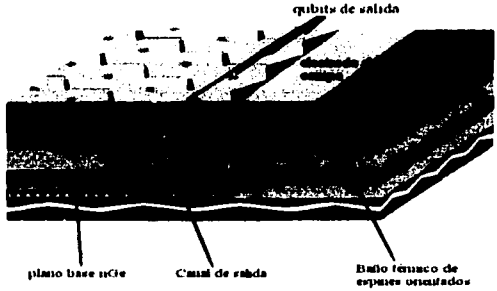


Figura 9e. En un arreglo más grande, el electrodo de campo permite que qubits al leerse interactúen con el baño de espines orientados, estos qubits estarían en la periferia. Canales FET incinerados sensarían el estado carga/espín de un qubit seleccionado. La corriente del canal pudiera cambiar algún porcentaje en respuesta a una sola carga electrónica.

9.4 Mediciones

Esta sección, de muy corta extensión, puntualiza el proceso de medición físicamente realizable en las arquitecturas de estado sólido.

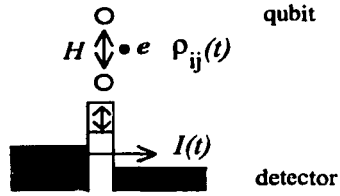


Figura 9f. Juntura Tunel como detector de la posición del electrón el cual afecta a la altura de la barrera. La corriente $I(t)$ (salida del detector) refleja la evolución de la matriz densidad $\rho_{ij}(t)$ del qubit.

Entre los métodos para obtener el resultado deseado en los sistemas cuánticos de dos niveles se encuentra el de la medición contínua [Korotkov, 2001 pg. 12]. El qubit es medido de forma contínua por medio de un detector débilmente acoplado, y la señal del detector es puesta en las ecuaciones* del caso más simple para monitorear la evolución de la matriz densidad del qubit $\rho_{ij}(t)$ -Figura 9f-. Ésta se compara con la evolución deseada y la diferencia es usada para generar la señal de realimentación la cual controla los parámetros del qubit con el fin de reducir la diferencia con el estado deseado del qubit.

Aquí demuestra en forma teórica y prácticamente realizable las mediciones en base a la evolución de los estados y la purificación de ellos haciendo uso de la matriz densidad del qubit.

Lo más interesante es el método de ciclo de realimentación cuántica, el cual evita perturbaciones instantáneas fuertes, por lo que presenta una forma de suprimir la coherencia debida al medio ambiente. El diagrama de bloques se presenta en la figura 9g.

Las ecuaciones a las que el dibujo hace referencia describen la evolución de la matriz densidad del qubit durante un proceso de medición en particular, pero las variables que intervienen están lejos del alcanze de la Tesis.

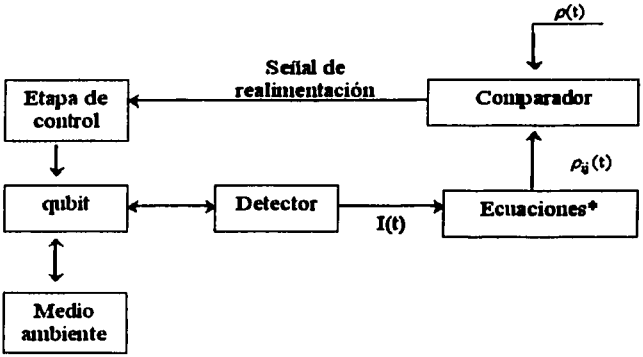


Figura 9g. Diagrama de bloques de la purificación contínua del qubit usando realimentación cuántica.

La limitación de este capítulo esta en función de mi trasfondo teórico, pues los intentos para el desarrollo de dispositivos cuánticos requieren amplios y profundos conocimientos de cada tema.

Bibliografía

[1] Berman G.P, G.D. Doolen, P.C. Hammel y V.I. Tsifrinovich, *Solid-State Nuclear Spin Quantum Computer Based on Magnetic Resonance Force Microscopy*; e-print: quant-ph\9909033. 9 de septiembre de 1999.

[2] Cory David G, Mark D. Price y Timothy F. Havel, *Nuclear Magnetic Resonance Spectroscopy: An experimentally accessible paradigm for Qauntum Computing*; Versión expandida de la charla presentada en Fourth Workshop on Physics and Computation, Boston University, 24 de noviembre de 1996. e-print.

[3] DiVicenzo David P, *Prospects for Quantum Computing.* Para el IEDM Tech, Digest, Diciembre de 2000.+

[4] Freedman Michael H., Alexei Kitaev, Michael J. Larsen y Zhenghan Wang; *Topological Quantum Computation*; e-print, 4 de Enero de 2001.

[5] Hai Wenhua, Mang Feng, Xiwen Zhu, Lei Shi, Kelin Gao, Ximing Fang, y Min Yan; *Energy Eigenstates of a Quantum Gate System*; International Journal of Theoretical Physics. Vol. 39, No. 6, pg. 1405-1411, 2000.

[6] Hu Xuedong y S. Das Sarma, *Solid State Quantum Computation with Spin Qubits: Can it be Done in Multielectron Quantum Dots?*; Department of Physics of Maryland, 8 de enero de 2001.

[7] Hu Xuedong y S. Das Sarma, *Theoretical Issues in Spin-Based Quantum Dot Quantum Computation*; Department of Physics of Maryland, 8 de enero de 2001*.

[8] Ionicioiu, Gehan Amaratunga, y Florin Udrea, *Quantum Computation with Ballistic Electrons*; 13 de noviembre de 2000.

[9] Jones Jonathan A, *Nuclear Magnetic Resonance Quantum Computers*, New Chemistry Laboratory, UK. 1998.

[10] Kielpinski, A. Ben-Kish, J. Britton, V. Meyer, M.A. Rowe, C.A. Sackett, W.M. Itano, C. Monroe, y D.J. Wineland, *Recent Results in Trapped-Ion Quantum Computing at NIST*;Time and Frecuency Division, National Institute of Standards and Technology, USA. 16 de febrero de 2001. quant-ph/0102086.

[11] Knill E, R. Laflamme, y G. Milburn, *Efficient Linear Optics Quantum Computation*; 20 de junio de 2000. e-print.

[12] Korotkov Alexander N, *Selective evolution of a qubit state due to continuos measurement*; Department of Physics and Astronomy, State University of New York, 19 de marzo de 2001. e-print.

[13] Laflamme R, E. Knill, W. H. Zurek, P. Catasti, S.V.S Mariappan, *NMR GHZ*, 1 de diciembre de 2000.

[14] Leung Debbie W., *Towards robust quantum computation*; Disertación enviada al Departamento de Física y al Comité de Estudios de Grado de la Universidad de Stanford en cumplimiento parcial de los requerimientos para el grado de Doctor en Filosofía. Julio de 2000.

[15] Levy Jeremy; *Quantum Information Processing with Ferroelectrically Coupled Quantum Dots*; Department of Physics and Astronomy, University of Pittsburgh, USA. e-print.

[16] Reina John Henry, Luis Quiroga y Neil F. Johnson, *Quantum information processing in semiconductor nanostructures*, 10 de enero de 2001.

[17] Schulman Leonard J, Umesh Vazirani, *Scalable NMR Quantum Computation*, 1 de noviembre de 2000.

[18] Steane Andrew, *Quantum computing*; Julio de 1996.

[19] Steane Andrew, *The Ion Trap Quantum Information Processor*; 8 de agosto de 1996.

[20] Vrijen Rutger,Eli Yablonovitch, Kang Wang, Hong Wen Jiang, Alex Baladin, Vwani Roychowdhury, Tal Mor y David DiVicenzo, *Electron Spin Resonance Transistors for Quantum Computing in Silicon-Germanium Hetero-structures.* arXiv:quant-ph\9905096. 11 de julio de 1999.

[21] Yariv Amnon, *Quantum electronics*, John Wiley & Sons, Tercera edición.

Capítulo 10

Requerimientos

Por varios años se han propuesto varios criterios para la construcción de la computadora, no obstante, los estudios recientemente hechos para la construcción, se han basado en cinco requerimientos para la computación cuántica, dados por DiVicenzo y seguidos por todos los investigadores del área.

La descripción básica de estos requerimientos se expone a continuación, directamente del escrito actualizado de [DiVicenzo, abril 2000 pg. 16].

Primer requerimiento
Un sistema físico escalable con qubits bien definidos

Por principio, se necesita un sistema físico que contenga un conjunto de qubits. Un qubit o más precisamente un sistema cuántico de dos niveles como los dos estados del espín de una partícula de 1/2 espín, como el estado principal o excitado de un átomo, o como las polarizaciones horizontal y vertical de un solo fotón. La notación genérica para los estados de un qubit denota a un estado como $|0\rangle$ y al otro como $|1\rangle$. La característica esencial que distingue a un qubit de un bit son, acorde a las leyes de la mecánica cuántica, los estados permitidos de un solo qubit llenan un vector de espacio complejo de dos dimesiones; el estado general es escrito como $a|0\rangle + b|1\rangle$, donde a y b son número complejos, y se adopta una condición de normalización $|a|^2 + |b|^2 = 1$. El estado general de dos qubits, $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, es un vector de cuatro dimensiones, una dimensión para cada estado distinguible de los dos sistemas. Tales estados se encuentran genéricamente *enredados*, lo que significa que no pueden ser escritos como el producto de

los estados de dos qubits individuales. El estado general de n qubits se especifica por un vector complejo de 2^n dimensiones.

Un qubit estando "bien definido" significa varias cosas. Sus parámetros físicos deberían ser conocidos con precisión, incluyendo el Hamiltoniano interno del qubit (el cual determina los eigenstados de energía del qubit, lo que son usualmente, aunque no siempre, tomados como los estados $|0\rangle$ y $|1\rangle$), la presencia y el acoplamiento de otros qubits, y el acoplamiento a campos externos que pudieran ser usados para manipular el estado del qubit. Si el qubit tiene, tres, cuatro, etc., niveles, el aparato de control de la computadora debería ser diseñado de tal manera que la probabilidad del sistema que siempre vaya en estos estados sea pequeña. La pequeñez de ésto y otros parámetros serán determinadas por las capacidades de la corrección de errores cuánticos, lo cual será visto bajo el requerimiento tres.

Segundo requerimiento
La habilidad para inicializar el estado de los qubits a $|000\ldots\rangle$

Esto surge directamente de los requerimientos de todos los sistemas digitales al iniciar cualquier cálculo. Hay una segunda razón para inicializarlos: la corrección de errores cuánticos requiere una entrega contínua de qubits en un estado de baja entropía (como el estado $|0\rangle$).

Tercer requerimiento
Tiempo de decoherencia más largo que el tiempo de operación de la compuerta

Los tiempos de decoherencia de los qubits deberían ser del orden $10^4 - 10^5$ veces el "tiempo del reloj" de la computadora cuántica, esto es el tiempo para la ejecución de una sola compuerta cuántica, solo entonces la técnica de corrección de errores será satisfactoria.

Cuarto requerimiento
Un conjunto 'universal" de compuertas cuánticas.

Las operaciones lógicas deberán ser posibles.

Bibliografía

[1] DiVicenzo D.P. (1), G. Burkard (2), D. Loss (2). E.V. Sukhorukov (2), *Quantum computation and spin electronics*; (1) IBM Research Division; (2) Dept. of Physics and Astronomy, University of Basel, Switzerland. Publicado en Quantum Mesoscopic Phenomena and Mesoscopic Devices in Microelectronics, eds. I.O. Kulik y R. Ellialtioglu (NATO Advanced Study Institute, Turkye, junio 13-25, 1999). e-print:cond-mat\9911245.

[2] DiVicenzo David P, *The Physical Implementation of Quantum Computation*; 14 de abril de 2000. quant-ph/0002077 v3.

Capítulo 11

Implementación LANL

En el presente capítulo se aborda la primera aplicación sobre los conceptos expuestos anteriormente. Es necesario una breve introducción a la criptografía cuántica.

11.1 Criptografía Cuántica

La criptografía, la ciencia de las comunicaciones secretas, se ha tornado muy importante con el crecimiento de las redes de computadoras y las transacciones electrónicas. Cuando la información financiera, militar o nacional se transmite de un lugar a otro, es vulnerable a tácticas indiscretas que potencialmente pueden ser catastróficas. Tales problemas pueden ser evitados encriptando la información para darlo a terceras partes de forma ininteligible. Dicho objetivo puede alcanzarse, si ambos, transmisor y receptor, poseen una secuencia secreta de bits aleatorios, conocidos como el material "clave" (key), el cual es usado para el encriptamiento por el transmisor y el desencriptamiento por el receptor.

Por lo tanto, el material clave es una valiosa fuente aún y cuando no lleve información. Sin embargo el paso inicial para la "distribución clave," con que las dos partes adquieren el material clave, debe ser hecho con un alto nivel de seguridad para que una tercera parte no pueda adquirir información alguna sobre la secuencia de bits.

Con las comunicaciones convencionales, las cuales pueden estar sujetas a monitoreos pasivos por un escucha, es imposible generar una clave certificablemente secreta, y tan tediosa seguridad física, mide la generación de la

clave, distribución, almacenamiento y destrucción que son requeridas después de usarse. Sin embargo, la distribución clave segura es posible si las dos partes pueden comunicarse usando transmisiones de un sólo electrón haciendo uso de la tecnología reciente de la criptografía cuántica o en una forma más precisa, distribución cuántica clave (QKD). La seguridad de QKD está basada en los principios fundamentales de la física cuántica. Nuestra tecnología facilita el irrompible encriptamiento de comunicación entre "islas" seguras enlazadas mediante redes de fibra óptica "abiertas" permitiendo la generación de la clave cuando se requiera.

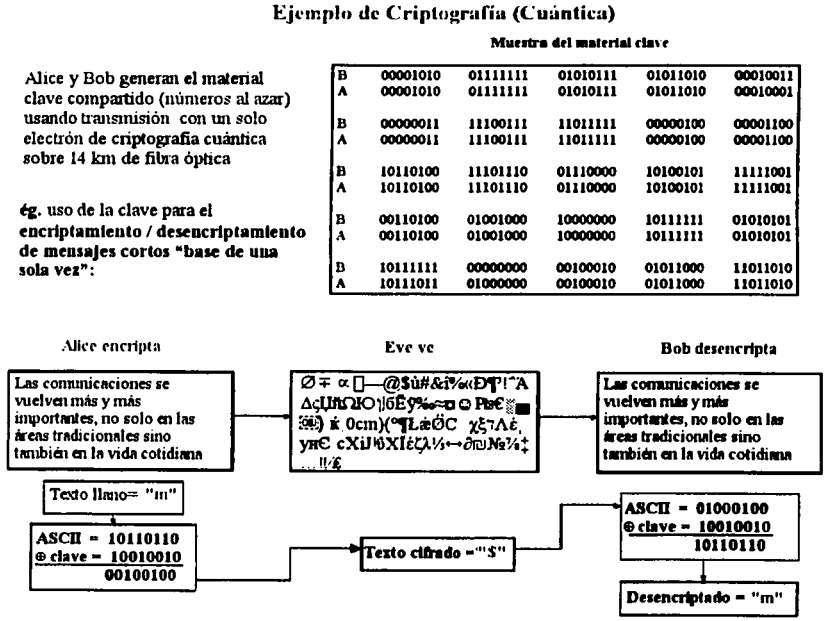
Dos partes (Alice y Bob) inician un procedimiento cuántico de generación de clave produciendo sus propios conjuntos independientes de bits aleatorios. Ellos poseen un canal cuántico y un canal público sobre el cual pueden comparar sus números para destilar un subconjunto común. Alice prosigue con la preparación de un solo fotón con su fuente láser para cada bit en su conjunto de números en una de dos formas posibles, dependiendo si su número es un 0 ó un 1. Luego cada fotón es enviado por el canal cuántico. Bob, quien también procede con la misma acción bit a bit en sincronía con Alice, ejecuta una de las dos posibles mediciones sobre cada fotón, dependiendo si el número es 0 ó 1. Un fotón nunca activará al detector de Bob si su número es diferente al de Alice, pero activará al detector con un 50 por ciento de probabilidad cuántica si sus número son iguales. Bob etiqueta a un número de su conjunto como "golpeado" si él detecta al fotón y entonces pasa esta información (pero no el número) a Alice por el canal público. Después Alice etiqueta sus números que fueron golpeados en el caso de Bob y una clave secreta emerge como el conjunto común de bits golpeados.

Una escucha (Eve) no puede "palpar" las transmisiones claves, debido a la indivisibilidad del fotón, ni copiarlos debido al teorema de la no-clonación. Además, la naturaleza no-ortogonal de los estados cuánticos asegura que si Eve hiciera sus propias mediciones, sería detectada a través del elevado cociente de error que surge del irreversible "colapso de la función de onda" que ella introduce.

QKD ofrece muchas ventajas de seguridad y facilidad de manejo sobre la distribución clave existente. La distribución clave tradicional, haciendo uso de mensajeros de confianza, requiere tediosos procedimientos de seguridad para preparar, transportar y manejar la clave antes de que cualquier comunicación se lleve a cabo, y aún puede ser impráctica (ég. el cambio de claves a un satélite). En contraste, las claves cuánticas no existen antes que

las transmisiones QKD sean hechas, y una clave puede ser generada en el tiempo de la transmisión del mensaje.

Este es un resumen gráfico del proceso de la criptografía cuántica:



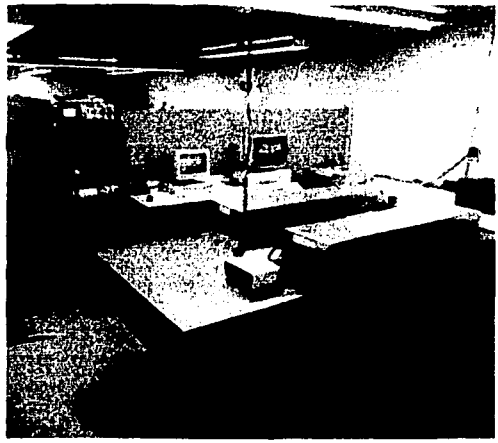
11.2 Experimento en los Alamos

Los sistemas físicos que pueden soportar transmisiones QKD determinan los usos potenciales de la criptografía cuántica. Han demostrado en el Laboratorio de Los Alamos que QKD es posible en trayectorias de fibras ópticas multi kilómetros: la coherencia cuántica necesaria de las transmisiones QKD persiste aún afuera del ambiente controlado de un laboratorio de física. En las longitudes de onda requeridas, se puede lograr que fotodiodos avalancha de arseniuro de germanio o de indio-galio detecten fotones individuales, pero a multa de ruido elevado y por tanto un cociente de error alto. Quitando estos errores se reduce la cantidad del material clave y limita la distancia de transmisión a 100 km aproximadamente. (Los amplificadores ópticos no pueden ser usados para extender este rango porque no pueden hacer réplicas de los estados cuánticos no-ortogonales usados en QKD.)

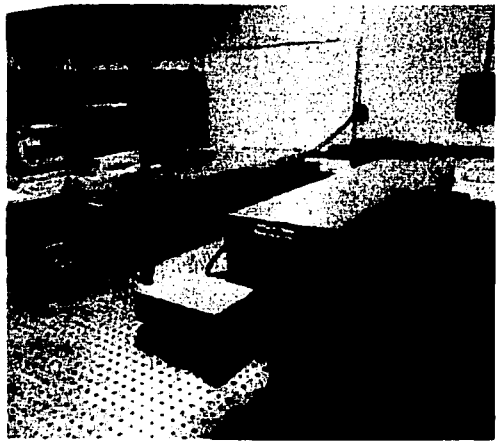
En el experimento se demostró la criptografía cuántica sobre 24 km de fibra óptica que había sido instalada para aplicaciones de red entre dos áreas técnicas LANL (Los Alamos National Laboratory.) Recientemente han incrementado la distancia de propagación a 48km. El sistema incorpora una característica de encriptamiento/desencriptamiento que permite usar el material cuántico clave para encriptar mensajes de texto cortos en la computadora transmisora y desencriptarlos en la computadora receptora. Este experimento demuestra que QKD podría ser usada para generar claves criptográficas en vínculos de fibra óptica "abiertos" entre "islas" seguras, ég. entre dos agencias gubernamentales diferentes en el área de Washington DC.

En un experimento por separado están desarrollando QKD para las comunicaciones en la línea de visión y en "el espacio libre", tales como base terrestre-a-aeronaves, e incluyendo posiblemente, la generación de nuevas claves para satélites en órbitas cercanas a la tierra. Hasta aquí, se han alcanzado transmisiones con una razón de error baja sobre 205 metros en el interior del laboratorio, pero extenderán la distancia a varios de kilómetros en un futuro cercano. Estos experimentos nuevos se llevarán a cabo en exteriores y permitirán evaluar los problemas del trasfondo de la luz solar y los de la óptica atmosférica que impactarán a las razones de la clave y del error. La criptografía cuántica es muy probable que sea la primera aplicación práctica de los fundamentos de la mecánica cuántica, la cual ilustra el valor usualmente inesperado de la investigación básica.

Imágenes:

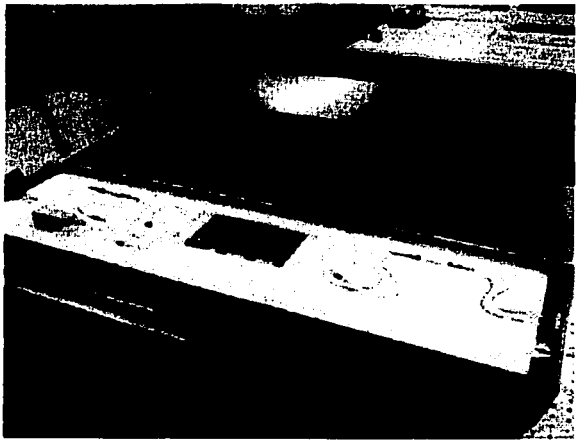


Laboratorio de Criptografía Cuántica. Una vista de todo el laboratorio

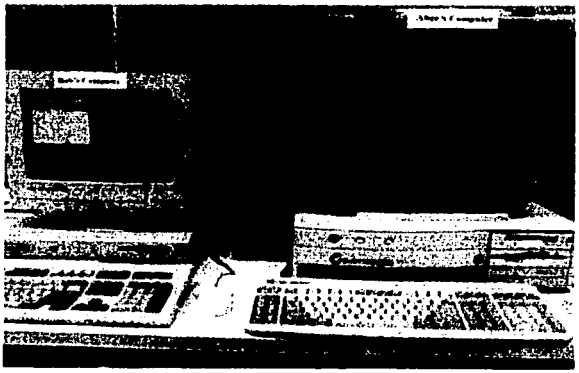


Interferómetros. El exterior de los interferómetros de Bob y Alice.

Imágenes:



Interferómetro. El interior de uno de los interferómetros.



Computadoras. Las computadoras de Bob y Alice

Bibliografía

[1] La información presentada puede ser consultada en el sitio del Laboratorio Nacional de Los Alamos, E.U. en http://p23.lanl.gov/Quantum/

Ilación

He presentado el camino que el conocimiento humano está siguiendo para poder construir este tipo de computadora. Se dice que dicha máquina no estará disponible sino hasta 20 años más tarde.

Los experimentos hasta ahora realizados se enfocan más en los fundamentos teóricos, los cuales crecen más rápido que los logros técnicos, siendo estos últimos los de mayor dificultad y limitaciones a causa de la tecnología actual.

Mientras tanto, las computadoras cuánticas no serán utilizables por todos sino exclusivamente para tareas que conciernan a Matemáticas, Física e Ingeniería, porque presentan el potencial mayor en la simulación de sistemas reales. El solo hecho de saber que en cualquier microprocesador de 64 qubits pudiéramos tener 1.84467440737 x10^{19} combinaciones al mismo tiempo es algo que sobrepasa nuestra capacidad para el diseño con tales máquinas en la actualidad.

En el lado de la velocidad, el ciclo de tiempo efectivo de una computadora cuántica estaría determinado por la razón más lenta a la cual los espines cambian. Esta razón depende de las interacciones y de cientos de ciclos por segundo hasta algunos ciclos por segundo. Si pudiéramos poner en marcha algunos ciclos de reloj, cada segundo parecería extremadamente lento comparado con los gigahertz de las computadoras actuales, pero una computadora cuántica con suficientes qubits lograría factorizar un número de 400 dígitos en aproximadamente un año.

Más el incremento de velocidad sólo será posible en la resolución de ciertos problemas, a saber, aquellos que tengan algunas soluciones o soluciones únicas como es presentado en [Calude et. al, 2000].

Por la etapa técnica, lo fundamental han sido los interferómetros, ya que demuestran que *sí* tienen existencia los qubits; lo que sigue es tratar de implementarlos en otros medios y con otro tipo de sistemas de partículas. Mas, un fotón siempre es puro, y las moléculas siempre contienen impurezas, razón más para que los dispositivos electrónicos cuánticos operen únicamente con partículas elementales o átomos.

Se hablo de la reversibilidad de las operaciones de las compuertas, la posibilidad de ser reversibles da origen a nuevos tipos de procesos.

Además, dentro del tema analógico-digital, se debería investigar la formación de los convertidores DAC/ADC, esto independientemente del avanze en el desarrollo del hardware cuántico. Podría existir un sólo convertidor el cual, por su naturaleza reversible, sería ambos convertidores a la vez.

Los elementos constitutivos de tal convertidor, deberían ser, las compuertas híbridas, son candidatos perfectos pues, en una misma compuerta manejan ambos tipos de variables. Existe la gran posibilidad de no volver a usar amplificadores como el medio indispensable para adecuar una señal a ser medida.

Las redes cuánticas, darían dan más libertad al diseñar circuitos, más libertad de elección en la toma de decisiones, podríamos tener gran cantidad de condiciones sin incrementar el uso de más compuertas. Sería necesario "otros" tipos o métodos de diseño de circuitos digitales, pero qué tan diferentes serían?, este tema solo debería ser desarrollado por la ingeniería.

Hay muchas aplicaciones después de todo esto.

$\rightsquigarrow$ En el área de la instrumentación habría muchas más posibilidades de medir exactamente y con gran sensibilidad, redefinir y/o reencontrar nuevas etapas de los estados alfa, beta del cerebro humano. Aún más para la biotecnología.

$\rightsquigarrow$ Extensión del espectro electromagnético.

$\rightsquigarrow$ La comunicación cuántica presenta a la teletransportación, además de dar ya gran seguridad en el encriptamiento.
$\rightsquigarrow$ Obtención de ecuaciones a partir de fractales.

La conclusión forzada para la computadora analógica-cuántica es que, no tendrá lugar, por la misma razón que la computadora analógica-clásica no lo tuvo. No así para el desarrollo de los dispositivos analógicos.

Tratándose de, una teoría cuyos principios ponen en tela de juicio la existencia misma de cada experimento hasta ahora realizado, considero que no se debe abordar el desarrollo de las compuertas cuánticas, ni mucho menos la creación de cualquier otro tipo de dispositivo que en principio funcione, íntegramente con los preceptos cuánticos, a partir de ellos mismos, esto es, se deben obtener ecuaciones para la descripción de una compuerta cuántica, pero ésta debe ser una solución particular a esta ecuación, no una sola ecuación que presente el comportamiento de la compuerta misma.

Es necesario la creación de diagramas para la representación de las compuertas cuánticas que, sin necesidad de la ecuación, como no sea para diseño, se pueda explicar su comportamiento, es lo ideal para la consecución del desarrollo tecnológico.

En el terreno teórico, es interesante hacer la observación acerca de la matriz densidad para uno y dos qubits como estados mezclados, estudiadas por separado, al igual que las propiedades que se deriven de estos análisis.

Emplazo mi razón y plena confianza, en que algún día la computadora cuántica será construida. Esto no implica que todas los ordenadores con los que ahora contamos estarán siendo relevados por éstas en los primeros años de su presentación, por la misma razón que la física cuántica no excluye a la física clásica; el tiempo está en función de la facultad de creación en el procedimiento de los algoritmos, no se tiene que adaptar cada programa de computadora actual a una computadora cuántica, esta debería tener sus propios programas que en verdad haga uso de las capacidades del sistema o en forma inversa, sólo con la finalidad de que las computadoras cuánticas estén en forma de ordenadores personales, de no ser así, el género humano tan solo continuará desarrollando tecnología. A mi entendimiento la computadora cuántica es la nueva Piedra Rosetta cuyo desciframiento estará íntimamente ligado a, lo que *queramos* ver, o a lo que podamos *obtener*.

"It is astonishing when the chthonian hammer of the engineer resonates precisely to the gossamer fluttering of theory*

*Es sorprendente cuando el infernal martillo del ingeniero resuena precisamente a la tenue palpitación acelerada de la teoría. [Freedman, 2000]

Referencias

Freedman Michael H, *Quantum Computation and the localization of Modular Functors*; Basado en conferencias preparadas para la junta de celebración de Matemáticas de Microsoft/University of Washington en abril de 2000 y la reunión AMS de Matemáticas en el nuevo milenio UCLA, agosto de 2000.

Calude Cristian S. (1), Michael J. Dinneen (1), y Karl Svozil (2), *Reflections on Quantum Computing*;Centre for Discrete Mathematics and Theoretical Computer Science. (1) Department of Computer Science, University of Auckland, New Zealand; (2) Institut für Theretische Physik, University of Technology Vienna, Austria. CDMTCS-130 marzo de 2000.

Apéndice I

Expresiones notables

FALTA
PAGINA

152

Expresiones.

Resumo las ecuaciones y las matrices que definen a las compuertas cuánticas que destacan.

Expresión ⌜ Página	Define
Sección 5.1 ⌜ 40	Espacio de Hilbert compuesto por 3 más.
$S(\{p(x)\}) = -\sum_x p(x)\log_2 p(x)$ ⌜ 24	Contenido de Información.
$\rho = \|\psi\rangle \otimes \langle\psi\|, \quad \in \mathcal{H} \otimes \mathcal{H}^*$ ⌜ 53	Matriz densidad para estados puros.
$\|\psi\rangle = \sum_{x\in\{0,1\}^n} A_x\|x\rangle$, ⌜ 71	Superposición de estados.
$\|\psi\rangle\|0\rangle \mapsto \|\psi\rangle\|\psi\rangle$ ⌜ 80	Copias de estados.

Compuertas.

Tienen que representarse por una tabla de verdad, como lo son las compuertas lógicas clásicas, es por eso que resumo a éstas con una tabla de verdad, la razón de haber sido escritas en forma de matrices es exclusivamente, por parte de los autores, para simbolizar las operaciones que realizan.

Unarias

1. Compuerta H.
La salida es multiplicada por $\frac{1}{\sqrt{2}}$. Es importante porque fue la primera compuerta cuántica; y al concatenar dos compuertas H, la entrada es la misma que la salida. Página 76.

Entradas	Salidas
$\|0\rangle$	$\|0\rangle + \|1\rangle$
$\|1\rangle$	$\|0\rangle - \|1\rangle$

2. Compuerta ϕ.
La importancia está en que es realizado un corrimiento del ángulo de fase de la onda de la partícula que esté predispuesta como entrada. Página 78.

Entradas	Salidas
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$e^{i\phi}\|1\rangle$

3. Compuerta NOT.
Es importante puesto que representa al equivalente cuántico del inversor lógico clásico. Página 79.

Entradas	Salidas
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$

4. Compuerta $\sqrt{NOT}$.
Su importancia estriba en que NO existe una operación con esta característica, sino que fue creada directamente de forma experimental. Una sola QCF calcula esta operación (ver página 70 antes del cuarto párrafo.) En palabras de los autores "es como si hubiéramos inventado una máquina que hiciera huevos revueltos y luego los regresara a su estado inicial, antes de ser revueltos (Ver página 99 referencia [8])." Página 108.

Entradas	Salidas
$\|0\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$

Binarias

5. Compuerta C-NOT.
Es importante por ser la pieza cuántica de la compuerta OR-exclusiva. Ver páginas 80, 95.

Entradas	Salidas
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

6. Compuerta SWAP.
Es una compuerta que solamente intercambia de lugar a los qubits. Ver página 82.

Entradas	Salidas
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|10\rangle$
$\|10\rangle$	$\|01\rangle$
$\|11\rangle$	$\|11\rangle$

Ternarias

7. Compuerta Toffoli.
Su importancia la obtuvo por ser la primera compuerta cuántica de tres qubits, actúa como una AND reversible y como una AND lógica. Página 83.

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

Apéndice II

Términos selectos

Falta

Página

158

Glosario

Bell, desigualdad de, 10.
Desigualdad que confirma una clase de teorías, que intentaban "completar" a la mecánica cuántica, nombradas *teorías de variable local oculta*, son, de hecho, inconsistentes con la mecánica cuántica. Como consecuencia, un comprendimiento puramente clásico de la realidad cuántica no es posible.
En la mecánica cuántica, mediciones idénticas de sistemas idénticos no necesariamente producen resultados idénticos. A causa de esto Einstein sugiere que la mecánica cuántica está incompleta y que deben existir variables "ocultas" (o todavía no observadas) que distinguieran estos sistemas aparentemente idénticos. Además para ser consistente con la Relatividad y la Teoría de campo electromagnética, estas variables deberían ser "locales" en el sentido de lo que sucede aquí y ahora debería estar en función con las cosas cercanas en espacio y tiempo.
Esta desigualdad sugiere a muchos que habitamos en una realidad no local, lo que significa que lo que sucede aquí y ahora podría depender solo de algo muy lejano en el espacio, tiempo o ambos.

Boltzmann, distribución de, 118.
Término aplicable a la distribución empleada en Mecánica Estadística.

Bose-(Einstein), Condensador de, 90.
Material transparente altamente denso usado para aminorar la velocidad de la luz, hasta 17 m/s.

Cavidad óptica High-Q, 89.
En la amplificación de luz por emisión estimulada (LASER), los fotones necesitan estar confinados en el sistema para permitir que el número de fotones creados mediante emisión estimulada superen excesivamente a todos los demás mecanismos, esto se alcanza delimitando el medio láser entre dos espejos, uno parcialmente reflejante y el otro totalmente reflejante, y esto forma una Cavidad Óptica Resonante.
El factor de calidad Q de una cavidad óptica es la cantidad que mide la capacidad para almacenar energía electromagnética en su interior. La forma en la que esta energía es almacenada es mediante la formación de ondas estacionarias entre los espejos láser.
El factor Q es proporcional a la razón de la energía almacenada en el interior

de la onda estacionaria y la energía perdida por la onda durante un viaje de ida y vuelta entre los espejos.

Efecto Mariposa, 111.
Nombre común para: *Dependencias sensitivas a condiciones iniciales*, es decir, que pequeños cambios ahora pueden tener puntos críticos en el futuro de un sistema.

Electrodinámica Cuántica (QED), 27.
Teoría que describe la interacción entre partículas cargadas eléctricamente y campos magnéticos. QED describe a ambos, partículas y campos en términos cuánticos.

EPR, experimento, 10.
Mejor conocida como Teoría de variable oculta (ver Bell, desigualdad de), propuesta por Einstein, Podolsky y Rosen en 1935, objetando vehementemente contra el enredo cuántico. Pero se puede demostar ahora que dos qubits separados por distancias espaciales interactúan el uno con el otro.

Hamiltoniano, 11.
Sea $|\psi(t)\rangle$ que denota el estado como una función del tiempo t de un sistema cuántico cerrado $\mathcal{Q}$. Entonces el comportamiento dinámico del estado de $\mathcal{Q}$ es determinado por la ecuación de Schrödinger

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle,$$

donde $\hbar$ denota la constante de Planck ($6.6260755\text{x}10^{-34}$ J· s) dividida entre 2π, y donde H denota a un observable de $\mathcal{Q}$ llamado el **Hamiltoniano**. El Hamiltoniano es la analogía cuántica del Hamiltoniano de la mecánica clásica. En física clásica, el Hamiltoniano es la energía total del sistema.

Josephson, efecto, 90.
El flujo de corriente eléctrica, en la forma de pares de electrones (llamados pares Cooper), entre dos materiales superconductores que están separados mediante un aislador extremadamente delgado.

Larmor, frecuencia de, 117.
Frecuencia de precesión a la cual rotan las dos componentes de un vector para describir la dirección y magnitud del momento dipolar de una partícula. La componente longitudinal es alineada con el eje de precesión y la componente transversal es alineada perpendicularmente al campo magnético externo. La frecuencia de Larmor está dada por la ecuación $\omega = \gamma \mathrm{T}$, en donde

ω es la frecuencia de precesión, T la magnitud del campo magnético y, γ una constante (razón giroscópica) única para cada átomo, como es aplicado en las técnicas de Imágenes por Resonancia Magnética.

Lógica cuántica, 28.
Trata con los fundamentos de la mecánica cuántica y, relacionada a ella, sistemas discretos deterministas. El acercamiento de ésta lógica es particularmente recomendable para la investigación y exclusión de ciertos modelos de parámetros ocultos de la mecánica cuántica.

Mapeo,76.
Se usa la palabra mapeo como un sinónimo de 'función'.

Mecánica estadística, 53.
Es el estudio de un tipo particular de leyes al que se ajusta el comportamiento y las propiedades de los cuerpos macroscópicos, es decir, a los cuerpos constituidos por una enorme cantidad de partículas individuales -de átomos y de moléculas. el caracter general de estas leyes es en buena medida independiente de cual sea la mecánica mediante la que se describe el movimiento de las partículas individuales del cuerpo, trátese de la mecánica cuántica o de la clásica. Sim embargo, su fundamentación exige razonamientos distintos en uno y otro caso.

No-localidad, Principio de la, 27.
Regiones del espacio-tiempo separadas por distancias espaciales son físicamente independientes. En otras palabras, a distancias espaciales ningún tipo de señal puede viajar entre dos puntos que esten separados por espacios. A menos que la señal viaje más rápido que la luz. Esto es

$$Distancia((x_1, y_1, z_1), (x_2, y_2, z_2)) > c|t_2 - t_1|$$

Para dos puntos $P_1 = (x_1, y_1, z_1, t_1)$ y $P_2 = (x_2, y_2, z_2, t_2)$

Paul, trampa de, 119.
Sistema para confinar iones en un espacio muy reducido mediante un campo eléctrico alterno, lo que permite medir sus propiedades con gran precisión.

Puntos Cuánticos, 14.
Son cajas de dimensiones de algunos nanómetros, hay una corriente considerable de interés en los puntos auto ensamblados que se forman sobre la superficie de un semiconductor como gotas condensadas sobre ventanas a baja temperatura. Debido a los confines cuánticos de los electrones y agu-

jeros en las tres dimensiones, los puntos cuánticos son esencialmente, átomos artificiales.

Red, modelo de, 33.
Modelo en que las compuertas lógicas actuales son conectadas para formar las diferentes escalas de integración.

Trace, 54.
La suma de la diagonalización de los elementos de la matriz. La diagonal se forma a partir de la esquina superior izquierda terminando en la esquina inferior derecha.

Trenza, 81. Es una relación entre dos tensores tipo tres a tres, que se construye desde una compuerta tipo dos a dos.