UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE INGENIERIA

COMPUTACION CUANTICA:
"UNA REVOLUCION TECNOLOGICA" .

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN COMPUTACION
P R E S E N T A :

OSWALDO CAMARGO VIDALS

DIRECTOR DE TESIS:
FIS. RAYMUNDO HUGO RANGEL GUTIERREZ

CIUDAD UNIVERSITARIA 2007

DEDICATORIAS Y AGRADECIMIENTOS

Quiero agradecer a todas aquellas personas que estuvieron conmigo durante ya mi primer cuarto de siglo, durante todo este tiempo en el cual he obtenido una cierta maduración sobre el entendimiento de la vida, en especial por tratar de comprender la mía.

En primer lugar quiero dedicar este trabajo a mis padres por haberme dado la vida… gracias a mi Papá por darme la facilidad abstracta del entendimiento mecánico… gracias a mi Mamá, por darme esa diplomacia y carácter que desde hace tiempo se salieron de control de una manera arrogante y soberbia, revueltas de humildad y decisión que hace que pueda seguir adelante con mis sueños e ideas…

Adalberto Vidals Marín, (Pale), por otorgarme su grandiosa necedad sobre lo que uno quiere y ayudarme a manejarme lo más correctamente posible.

María Elena López Navarrete, (Male), por instruirme, darme la visión de hasta donde uno puede llegar con su esfuerzo y dedicación, gracias también por solapar todos mis relajitos de nieto desobediente.

Rufino Camargo Hernández, (Mi Papá), gracias por darme la vida y el don del conocimiento abstracto de la Naturaleza, hoy puedes estar tranquilo y orgulloso de saber que puedo salir adelante.

Alma Lilia Vidals López, (Mi Mamá), gracias por darme la vida, este trabajo es muestra de lo que lograste en mi y de que aún puedo hacer mucho más.

Carlos Piza Vega, (Maestro), por hostigarme en lo que ahora es mi herramienta principal de trabajo, la lectura, la escritura y el habla, procurando siempre que lo hiciera correctamente.

Alejandro Alberto Camargo Vidals (Mi hermano, el picos), por los días en que podíamos jugar, reír, pelearnos por todo.

Okairy Camargo Vidals (Mi hermana), por su inocente comportamiento e ingenuidad de su vida.

Hugo Vidals López, (Morro), por ser el 1er compañero que me encuentro desde mi nacimiento y gracias a él he comprendido según yo, la incondicionalidad.

Mireya Vidals López, (Miye), por reprimirme por cualquier cosa y tachar mi tarea una y otra vez hasta que hiciera todo bien y gracias a ella hoy en día hago las cosas bien y de buena manera o mejor no hago nada.

Edith Vidals López (Edy) y Salomón Bustos (el buen Salo), por darme la alegría de mis primas Karen y Karlita.

Ernesto López Rodríguez, (Harry), por su ayuda incondicional, sabemos que siempre contamos el uno con el otro.

Joe y Angelina Ochoa, por las alegría de saber que me tienen en su mente y corazón siempre.

Raymundo, Gilda y la otra Gilda, por sus palabras entre mezcladas en la confianza incondicional de mostrarme su cariño siempre.

Rosales Nieves Ana Lilia (karnala), por todo tiempo que hemos pasado en esta vida sin sentido y lo más curioso, que es interesante.

Andrés Jimenez Villarreal (karnalin), por enseñarme a ver la vida directamente tal cual cruda es y por motivarme a no ser una persona “saganizada”.

Gloriany, Mauricio y Adriana, por confiar en que puedo hacer las cosas bien.

Alfredo Landa (gnomo), cuando pasa algo bueno bebes para celebrarlo, darte un homenaje, mutuo, recíproco... unilateral... Cuando pasa algo malo bebes, y vuelves a beber... para olvidar, nublarte el cerebro... cuando yo solo sé que sientes mucho más... Quieres confundirte y perfectamente sabes que no puedes engañarte a ti mismo, gracias por tratar de comprenderme.

Daniel Gutiérrez Zúñiga (karnal), por tener su apoyo, aprecio y comprensión todo el tiempo.

Mauricio Torres Villa (Negrito), por su constante pérdida de la realidad que hace orientar mi sentido en la vida.

Ángel M. Arévalo López (Serpientes), por la confianza depositada en mí y en esa hermandad que tenemos.

Federico (Fedepp), por estar conmigo, brindarme un abrazo y la comprensión de seguir adelante.

Paola Arévalo López (Payos), por su absoluta amistad.

Luis David Alcaraz, por las sorpresas de bondad y camaradería inigualable.

Cesar (Gruñon), por todas esas pláticas sin sentido en el estacho de ciencias.

Ray (Pachon), por el aprecio de una verdadera amistad.

Apolo Isaac Hernández Ávila, (niño Isaac), por mostrarme su confianza y apoyarme en todo momento.

Juan Manuel Cruz Alvarado, (Juanito), por su presencia humilde e inocente.

Me vienen tantas personas a la mente que me gustaría agradecerlas a todas y a cada una de ellas, mando un abrazo y una sonrisa a donde quiera que se encuentren y gracias por todo, precediendo inmediatamente al sustantivo indeterminado: Kiko, Lidya, Cuper, Gabychica y John, Gabriela Martínez Serrano, Rocío Herrera, Memo, Karen, Miguel Ángel López Ayala, (Erika, donde Dios te haya puesto, gracias), Crisitos y a la Licha, al Sha, Ferny, Cristo, David Canibal, Cruzito, Pachekin, Bebelem, Rolas, Raúl y Norma, Lunix, a Mecanse y la Mosca, a Mireille, Pamela y la Chela y a todos los que pasan siempre por mi mente muchas gracias…

a todos, mi fraternal agradecimiento…

Oswaldo Camargo Vidals

Al amor de mi vida…

Es tan difícil tratar de explicar o comprender con palabras o pensamientos, lo inmenso y profundo que mi amor es por ti, sería extremadamente difícil pensar que pueda existir una vida o un lugar en la que yo no me encuentre junto a ti, alejado, de tu ser, de tus labios, de tu piel, de todo lo maravilloso que significas para mi, tú eres mi mayor inspiración, mi verdadero y único amor, eres lo mejor que me ha pasado en la vida, y con la arrogancia y soberbia que me caracteriza puedo decir con mi corazón que eres y serás lo más importante para mi, hoy, mañana y siempre en cualquier parte del universo…

Te amo Sarah.

Computación Cuántica

"Una revolución tecnológica"

DEDICATORIAS Y AGRADECIMIENTOS

ÍNDICE

INTRODUCCIÓN

Capítulo I: El azar, la ignorancia y la Mecánica Cuántica

Una extraña forma de pensar 1

Ondas o partículas, he ahí el dilema 8

¿Y el gato de Schrödinger? 14

Postulados de Mecánica Cuántica 16

El Operador Densidad y los Postulados 20

Discusión 22

Capítulo II: La esencia del Cómputo Cuántico

Motivación para la Computación Cuántica 26

Teoría Clásica de Computación 28

El Quantum contra la Física Clásica 30

Bit's y Qubit's 35

El Bit 36
El Qubit 36
Bit's vs Qubit's 39

Compuertas Cuánticas 40

Discusión 41

Capítulo III: Criptografía Cuántica

Despertando la curiosidad 46

Criptografía 47

Distribución de Claves 48

Principio básico 50
Comunicación 50
El algoritmo BB84 52
Alicia, Bob y alguien más 53
En la actualidad y un futuro en desarrollo 55
Discusión 59

Capítulo IV: Una propuesta real, Resonancia Magnética Nuclear

Computación Cuántica y la Resonancia Magnética Nuclear 61
Estado Líquido 66
Logros de estado líquido 67
Limitaciones de estado líquido 70
Estado Sólido 71
El futuro de la Resonancia Magnética Nuclear 72
Discusión 78

CONCLUSIÓN 82

APÉNDICE 87

Apéndice A "Divertimentos Matemáticos" 87
Apéndice B "Operador Densidad" 89
Apéndice C "Dichoso vuestro nombre" 92
Apéndice D "Implementaciones físicas" 93

REFERENCIAS 96

INTRODUCCIÓN

Se introducirá una investigación sobre Computación Cuántica como se sigue en la mayoría de los artículos y publicaciones sobre el tema. Los temas se presentarán como una analogía de la computación clásica o actual. La principal característica de la Computación Cuántica radica en su capacidad de procesamiento para realizar simultáneamente un número exponencial de operaciones.

La Computación Cuántica es un área multidisciplinaria con una fuerte relación que va desde la arquitectura de computadoras hasta la física teórica y experimental, pasando por las comunicaciones, la criptografía, la electrónica, las matemáticas, la microelectrónica y la nanotecnología por citar algunas, y tiene básicamente efectos muy radicales en la tecnología. En términos de hardware, a medida que la información pase a ser representada por partículas subatómicas, los dispositivos deberán tener la capacidad de reconocer los fenómenos cuánticos. En relación con los algoritmos, la computación cuántica abre posibilidades antes no imaginadas, disminuciones exponenciales en el tiempo de procesamiento y realización de operaciones nunca antes realizadas por computadoras actuales.

En la actualidad, la velocidad en el procesamiento de información y la capacidad de almacenamiento de las computadoras se incrementa aproximadamente cerca dos años, además de una evolución tecnológica que permite la miniaturización de los componentes electrónicos como el transistor. Hoy en día, es posible fabricación de circuitos integrados de un cuarto de micra donde (1 micra = 1 millonésimo de un metro, $1\mu m = 10^{-6} m = 10^{-3} mm$), desarrollando estos circuitos con poco mas de 200 millones de transistores.

La computación cuántica hace referencia inicialmente, a los fenómenos que tendrá que enfrentar la tecnología de las computadoras cuando el tamaño de sus componentes, es decir de transistores, circuitos integrados y otros, rebase un límite inferior determinado, frontera para la cual las leyes de la física son fundamentalmente diferentes a las que se aplican en el mundo macroscópico. Al

continuar la tendencia en la reducción del tamaño de los componentes, se tendrá que enfrentar muy probablemente a las leyes cuánticas, cuando el tamaño de éstos alcance niveles atómicos. En este nivel, el transistor quizás pase a ser una pieza de museo y sea sustituido por una molécula.

La idea de “Computación Cuántica” ha inspirado a muchas mentes inquietas simplemente porque las mismas palabras hacen pensar en algo extraño y poderoso, como si los científicos hubieran abierto el camino hacia una revolución en el procesamiento informático, siendo esto el pan de cada día durante este milenio.

Pero, el término “revolución” podría ser una impresión falsa. La computación cuántica no reemplazará a la computación clásica, por las razones similares que la mecánica cuántica no reemplaza a la mecánica clásica: nadie consultó alguna vez al profesor Heisenberg para diseñar una casa y nadie lleva su auto a un taller cuántico para ser reparado. Si las maravillosas computadoras cuánticas llegan a ser posibles en el mundo físico real, se usarán para ocuparse simplemente de las tareas especiales en las cuales nos beneficiaria el poderoso procesamiento de información cuántica, descubriendo por ejemplo: el tiempo de vida de nuestro planeta tierra, el futuro del calentamiento global, el código genético, respuestas al problema de tres o mas cuerpos, etc…, tareas que la computación clásica no puede resolver exitosamente.

Una razón más honesta para investigar sobre la computación cuántica es que es una nueva y profunda manera de pensar en las leyes fundamentales de la física, tanto clásica como moderna. La comunidad de la computación cuántica aún es bastante pequeña en la actualidad, pero con el paso del tiempo y el progreso tecnológico ha ido aumentando y creciendo en los últimos años.

Las ideas sobre la teoría de la información clásica parecen encajar en la mecánica cuántica como una mano en un guante, dándonos el sentimiento de que estamos descubriendo algo muy profundo sobre el comportamiento de la Naturaleza.

Las preguntas de Hilbert con respecto a la estructura lógica de las matemáticas nos alientan a idear e imaginar un nuevo tipo de preguntas acerca de las leyes de físicas. Observando la ecuación de Schrödinger, podemos dejar a un lado si estamos describiendo un electrón o un

planeta, y simplemente preguntarnos por las manipulaciones de partículas y los estados que se aceptan. El lenguaje de información y las ciencias computacionales, así como la informática nos permite idear cosas que se cuestionan de esa manera, incluso una idea tan simple como las compuertas cuánticas viene a ser muy útil, porque nos permite pensar claramente en manipulaciones de estado cuántico que parecerían sumamente complicadas o complejas. Por otra parte, tales ideas abren el horizonte al diseño de algoritmos cuánticos como los desarrollados por Shor, Grover y Kitaev, los cuales muestran que la mecánica cuántica permite el procesamiento de información de una forma diferente de las ya establecidas por leyes de la física clásica. Estos científicos como muchos otros investigadores creen que el comienzo del cómputo cuántico se encuentra en la propagación de un estado cuántico a través de un número exponencialmente grande de dimensiones en el espacio de Hilbert. El resultado de computación proviene de una interferencia controlada entre muchos caminos computacionales que se igualan después de que hemos examinado la descripción matemática, todas estas abstracciones numéricas aún parecen maravillosas y sorprendentes por el simple hecho de que se cumple perfectamente con las teorías de la mecánica cuántica.

La dificultad intrínseca de los problemas en la computación cuántica respecto a la sensibilidad de interferencia a gran escala al ruido e imprecisión es un tema que a menudo es discutido contra la computación cuántica. Esencialmente un dispositivo analógico en lugar de un dispositivo digital tiene muchas limitaciones como resultado. Éste es un concepto erróneo. Es verdad que cualquier sistema cuántico tiene un espacio de estado continuo, pero esto lo tiene cualquier sistema clásico, incluso los circuitos de una computadora digital. Los métodos o modelos de computadoras tolerantes a fallos permitirán la detección y corrección de error, en una computadora cuántica restringida de un conjunto de compuertas cuánticas a un conjunto discreto, por consiguiente las "leyes" de los estados de las partículas en la computación cuántica serán discretos, así como en una computadora digital clásica. La diferencia más importante entre la computación analógica y digital es el incremento de la precisión de un resultado realizado por recursos analógicos o digitales, en base a esto uno debe pensar en re-diseñar una mejor maquina computacional, considerando que con métodos digitales uno necesita meramente un incremento en el número de bits, operaciones y por ende mucho mas recursos, así como mayor procesamiento, más memoria e incluso más espacio. Aún así por el momento se piensa que la computadora cuántica tolerante a

fallos tiene más en común con un dispositivo digital que un dispositivo analógico pero no lo excluye.

El algoritmo de Shor para el problema de la factorización estimuló mucho el interés en la computación cuántica, debido en parte a la relación que tiene con la criptografía de datos. Sin embargo, se cree que este algoritmo no se usará de manera principal para factorizar enteros grandes en el futuro, si así se requiere. Más bien, ha actuado como un estímulo fundamental en este campo de estudio, probando la existencia de un tipo nuevo y poderoso de computación, hecha posible por la evolución cuántica controlada, exhibiendo así, una cierta variedad de nuevos métodos.

Los títulos sobre la computación cuántica seguirán siendo nombres equivocados para cualquier dispositivo experimental por lo menos en los próximos veinte o treinta años. Incluso es un abuso de lenguaje llamar a una calculadora de bolsillo computadora, porque la palabra ha llegado a ser reservada para máquinas de propósito general que más o menos comprenden el concepto de Turing sobre la Máquina Universal. Sin embargo, los pequeños procesadores de información actuales pueden servir para realizar tareas útiles, por ejemplo, la simulación de los conceptos aprendidos en la teoría de la informática cuántica permitirán el descubrimiento de nuevos métodos o modelos espectroscópicos útiles en la Resonancia Magnética Nuclear (NMR).

La mayor satisfacción de la computación cuántica será recompensada por el hecho de crear una máquina de estas características; sin embargo, algunos científicos opinan que tan sólo con investigar y experimentar sobre las teorías propuestas ya merece de un gran mérito por tratar de averiguar lo inalcanzable por el momento, podría ser realidad en un futuro. Uno de los principales usos de la tecnología más avanzada en la actualidad es destinada a la simulación de manipular momentos cuánticos para proporcionarnos una mejor comprensión sobre problemas como la decoherencia en la mecánica cuántica. Esto será fundamental en la investigación experimental durante los próximos años.

Por otro lado, en teoría, hay dos preguntas abiertas sobre la naturaleza de los algoritmos cuánticos y los límites en la fiabilidad de la informática cuántica. No está del todo claro cuál es la

naturaleza esencial de la computación cuántica y qué clase de problemas computacionales son dóciles a una solución eficaz por métodos cuánticos. ¿Hay un mundo lleno de algoritmos cuánticos útiles esperando a ser explorada?, o nos conformaremos con los pocos trozos que hemos descubierto hasta ahora, o bien, ¿El poder de procesamiento con el que se sueña podría lograrse con menos de 100 qubits?. Esto se encuentra limitado por el conocimiento certero que se tiene actualmente, pues hoy en día es difícil simular 10 qubits incluso al utilizar todos los recursos tecnológicos más avanzados.

La fiabilidad matemática y física inmersa en la tecnología a hecho posible el gran avance que se ha realizado hasta el momento para que se pueda tener un pensamiento optimista hacia la informática cuántica ya que con el paso del tiempo se demuestra que no es un sueño imposible lograr. Hoy en día podemos identificar los requisitos suficientes para garantizar una informática cuántica fiable y modelar una computadora cuántica cien veces más poderosa que la computadora clásica actual mas avanzada.

Espero que la información cuántica sea reconocida como una valiosa rama de la física cuántica fundamental y que con el tiempo vaya creciendo la curiosidad de diversas áreas del conocimiento para así lograr una computadora cuántica convencional.

Capítulo I

El azar, la ignorancia y la Mecánica Cuántica

"We have no right to express an opinion until we know all of the answers"

Kurt Cobain (1967-1994)

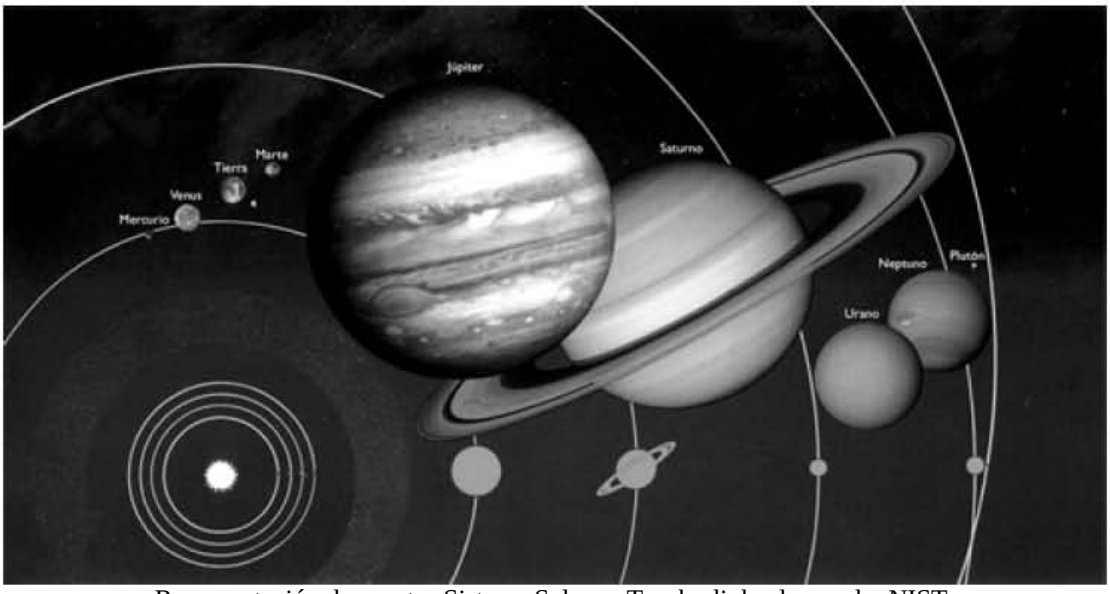
Una extraña forma de pensar.

Muy de vez en cuando aparece alguien que descubre un cierto comportamiento que nadie había visto anteriormente, podría ser por ejemplo que los planetas del Sistema Solar obedecen a reglas precisas y relativamente sencillas o podría ser que las rayas del espectro del Hidrógeno obedecen con una precisión misteriosa a una formula sencilla, tal vez sea una similitud entre la trayectoria de una bala de cañón y la órbita de la Luna lo que atrae la atención de alguien o podría ser una disposición de partículas subnucleares lo que sugiere su funcionamiento interno[2][5].

Observaciones como estas jamás son meras ráfagas de inspiración, son el resultado de interminables trabajos de intentos y fracasos de completos errores y verdades a medias, y que frecuentemente una vez conseguidas se vuelven objeto de amargas controversias sobre a quién le corresponde el mérito, pero hay algo que no se discute una vez que se ha descubierto un nuevo modelo de comportamiento y se ha relacionado una parte del Universo con otra, la conexión jamás será olvidada[1]. Tales acontecimientos nunca son el final de la historia, con frecuencia son precisamente el comienzo, y lo que comienza con ellos puede ser nada menos que revolucionario[6].

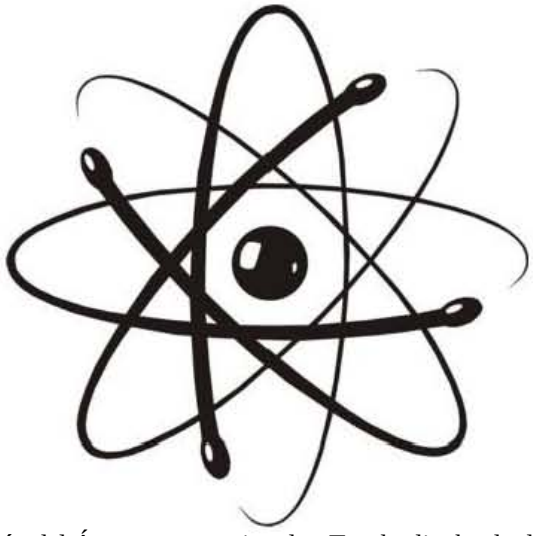
La historia del Universo Mecánico[1][3] comenzó con una revolución científica, cansado de la inmensa complejidad de la astronomía antigua, Copérnico sacó la tierra del centro del Universo y la puso en su lugar, bajo la influencia del Sol, cuando se calmó la agitación provocada por esta teoría el resultado fue una nueva visión del Universo, como una máquina, una máquina

maravillosamente complicada, pero que cumplía unas Leyes Mecánicas precisas, intencionalmente o no, esa idea es el fundamento silencioso de todo el pensamiento occidental desde la época de Newton hasta incluso nuestros días, pero irónicamente ya no es aceptada por la misma gente que la creó, los Físicos



Representación de nuestro Sistema Solar. Teacherlink.ed.usu.edu NIST.

y así el relato del Universo Mecánico finaliza con la historia de la segunda revolución, una revolución que tuvo lugar a inicios del siglo XX y que provocó una incertidumbre que aún no se ha resuelto, al igual que la primera revolución la segunda nación del intento de solucionar un problema, la primera resolvió el problema del sistema solar y la segunda el problema del Átomo[4],

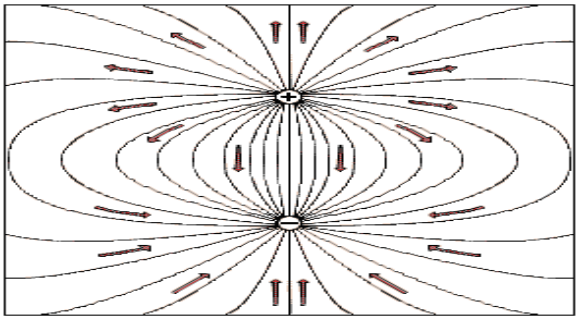


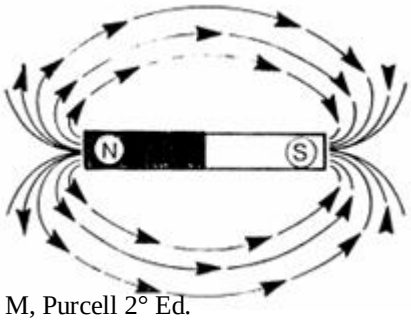
Representación del Átomo convencional. Teacherlinck.ed.udu.edu NIST.

es realmente posible que dos problemas tan similares hayan requerido soluciones tan radicalmente distintas de modo que, ¿Sería necesario una segunda revolución para derribar a la primera?[6][8]. Después de todo, la primera revolución, la invención de la mecánica clásica había resuelto no sólo el problema del Sistema Solar, había logrado mucho más[1].

Para empezar parecía reducir todos los fenómenos de los cielos y de la tierra a la única ecuación $F = ma$, una Ecuación Vectorial, para ser más exactos una Ecuación Diferencial Vectorial $F = m\frac{d^2s}{dt^2}$, pero dentro de su ámbito contenía las respuestas a una asombrosa variedad de preguntas[16][18]. Cuál es el principio para que un reloj vaya bien de hora o el secreto de seguir una trayectoria infalible, por qué las olas del océano rompen en la playa y porque un puente sólido se puede derrumbar, con respuestas a preguntas como éstas, parecía que la propia Mecánica Clásica era una estructura que jamás se derrumbaría, en lugar de eso que inspiraría y guiaría la exploración de nuevos cambios y a la larga ninguna expedición sería mas fructífera o impactaría con mayor fuerza que el estudio de la Electricidad[7].

Benjamín Franklin con un talento aparentemente sin límites para la invención dio la primera descripción útil de la Carga Eléctrica y así proporcionó la primera explicación de un extraordinario invento del siglo XVIII, llamado la Botella de Leyden[13]. Por supuesto una revolución aunque no sea del tipo científico separaba a Michael Faraday de Benjamín Franklin. Sin embargo, Faraday y Franklin tenían mucho en común, compartían una ignorancia casi perfecta de las matemáticas, una insaciable curiosidad por la Naturaleza especialmente la naturaleza de la Electricidad y una participación verdaderamente considerable de genialidad y eso es justo lo que se necesitó para relacionar las Cargas Eléctricas con las Líneas de Fuerza[10][17][18].





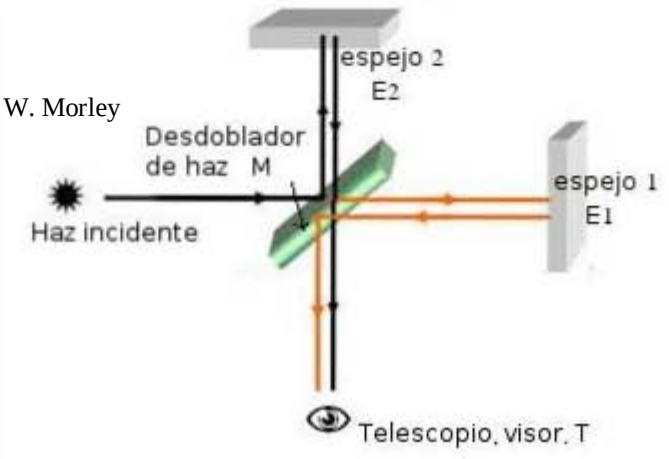
Electricidad y Magnetismo, Líneas de Fuerza, Edward M, Purcell 2° Ed.

El concepto de Líneas de Fuerza incluiría por suerte también el Magnetismo y cuando Michael Faraday se enfrentó a la cuestión de ¿Cómo poder utilizar el Magnetismo para crear la Electricidad?, su respuesta, la Inducción Electromagnética, pondría al mundo bajo un estado constante de Flujo Variable. Nadie captó el significado del Flujo Variable mejor que James Clerk Maxwell[6].

Maxwell tenía un secreto y un dilema a la vez, el secreto era que oculta detrás de las Fuerzas entre Cargas Eléctricas y detrás de la Fuerza Magnética entre Corrientes Eléctricas, estaba nada menos que la propia Velocidad de la Luz esperando ser descubierta, el dilema era que, a pesar de toda la elegancia y la fuerza de las Leyes de la Electricidad y del Magnetismo, las Leyes de Gauss, de Ampere y de Faraday había algo que faltaba, cuando James Clerk Maxwell suministró la pieza que faltaba, la idea de que un Flujo Eléctrico Variable podría producir un Campo Magnético, no sólo había iluminado todo el Espectro Electromagnético, había completado la ciencia de la Electricidad y el Magnetismo. Fue un logro que rivalizó con la invención por parte de Isaac Newton de la propia Mecánica Clásica[9][11][15][17].

Cuando el siglo XIX llegaba a su fin la Mecánica Clásica de Newton y la Teoría Electromagnética de Maxwell parecían ser los cimientos gemelos de un edificio de la Física que permanecería para siempre, pero era un, para siempre, que no estaba destinado a durar mucho tiempo, ¿que podía haber fallado?, ciertamente no parecía que fuera mucho, en ese momento, solamente unos pocos detalles que no encajaban bien en la gran escena, por ejemplo Albert A. Michelson[12][1] había construido un dispositivo maravilloso para medir el movimiento de la Tierra mediante el estudio de los cambios de unas franjas de luz, todo lo que se podía esperar era un pequeño cambio en la figura, pero cuando Michelson giro su interferómetro en el viento del éter, en lugar del pequeño cambio que esperaba, no se produjo absolutamente ninguno.

Interferometro (1887)
Albert A. Michelson y Edward W. Morley



Luego estaba el curioso caso de Max Planck, su problema era explicar el color de un cuerpo caliente brillante, para resolver este problema necesito introducir una nueva constante, era una constante muy, muy pequeña, de hecho Planck tenía la esperanza de que se anularía por completo, pero no se anuló y luego estaba la extraña historia de Ernest Rutherford, cuando bombardeó una fina chapa de oro con rayos alfa ordinarios el experimento funcionó casi perfectamente, casi todos los Rayos Alfa pasaban a través de la chapa justo como se había supuesto solo unos pocos rebotaban, pero, ¿Como podía ser esto?, ni tan siquiera uno debería rebotar[1][3][7].

Partiendo de estos fenómenos extraños surgió la nueva revolución y nadie jugó un papel más importante que el joven Albert Einstein en el mundo de la Física. El año de 1905, año en el que el joven Einstein presentó su tesis doctoral será recordado a la par que en el año 1665, año en el que el joven Isaac Newton huyó a Lincolnshire para escapar de la peste que azolaba a Londres y completó lo que fue quizás su trabajo más importante, pero a diferencia de Newton que utilizaba su pacífico retiro para encontrar las respuestas a las revolucionarias preguntas del pasado[8]. Albert Einstein en 1905 hizo descubrimientos que hicieron poner en marcha la nueva revolución.

El problema del interferómetro de Michelson[12][9] podía resolverse, como demostró Hendrik A. Lorentz, si diferentes observadores medían diferentes tiempos y diferentes distancias, pero Albert Einstein fue más lejos combinando espacio-tiempo en un continuo sin fisuras y la Teoría Especial de la Relatividad de Einstein de 1905 fue solo el primer paso, no el último.

Pretendiendo explicar el viejo misterio de la caída de los cuerpos, Einstein concluiría más tarde que el propio espacio o más bien, el propio espacio-tiempo estaba curvado, dando así un nuevo giro a la Ley de la Inercia, una nueva explicación de la Fuerza de la Gravedad y una nueva Teoría del Cosmos[3][5][2].

Einstein también se dio cuenta de que tenía un modo de explicar algo llamado Efecto Fotoeléctrico, ¿Por qué la luz ultravioleta descargaría una placa metálica cargada eléctricamente?, lo haría si la luz llegaba en paquetes cuya Energía dependiera de la Frecuencia de acuerdo con la

formula de Max Planck, la idea puede haber parecido bastante inocente, pero en realidad no ha habido un manifiesto más revolucionario[10][14].

Un siglo antes, Thomas Young había sido el primero en justificar el fenómeno de la interferencia probando de una vez por todas que la Luz era una Onda. A finales del siglo XIX, la teoría de Maxwell había explicado lo que ocurre cuando Cargas Eléctricas crean Ondas Luminosas que se propagan en el vacío, pero el mundo de la Física apenas se había sentado a descansar para gozar de su triunfo, cuando Albert Einstein negándose a cabalgar sobre la cresta de la ola, dijo que la Luz podría estar formada por Partículas[1].

Esto provocó que la revolución comenzara en serio, provocó a Ernest Rutherford el cual desde el momento en que se dio cuenta de que algunos Rayos Alfa rebotaban en la plancha de metal, eran exactamente revoluciones lo que tenía en mente[11][18]. Copérnico antes que Ernest Rutherford sitúo el núcleo en el centro del Átomo y coloco a los Electrones en movimiento girando a su alrededor.

Hubo una vez mucho tiempo antes en que la pregunta había sido: Si, la Tierra se esta moviendo lanzada a través del espacio, ¿Por qué no salen volando las cosas que están sobre ella?; ahora la pregunta era: Si, el Electrón es acelerado constantemente cayendo eternamente en su órbita alrededor del núcleo, ¿Por qué no irradia su Energía Orbital y cae, al núcleo?.
Niels Bohr se presentó con una nueva visión y una parte de la respuesta, sólo se permitirían ciertas órbitas especiales, aquellas cuyos Momentos Cinéticos fueran múltiplos de "hache con barra $\hbar$" y la Luz sólo podría ser emitida u absorbida en saltos entre Orbitas, eso es exactamente lo que se necesitaba para explicar el tamaño y el espectro del Átomo de Hidrogeno, que se necesitaría para explicar, ¿Por qué se permitían precisamente esas Orbitas y no otras?[13][17]

El príncipe Luis de Broglie era un aristócrata como cualquiera de su época, pero tenía también espíritu democrático y un sentido de la igualdad de oportunidades dijo: Si, la Luz puede estar formada por Partículas, ¿Por qué no pueden los Electrones ser Ondas? Las Ondas del Electrón producirían interferencias constructivas tan sólo en las Órbitas que el Dr. Bohr había organizado y eso, realmente, provocó problemas. Mientras que el mundo de la Física parecía ir de triunfo en

triunfo, su propia estructura se estaba desenmarañando o para expresarlo de otro modo, la dualidad Partícula-Onda parecía una metáfora defectuosamente mezclada, indudablemente las Ondas de diferentes longitudes podrían combinarse en un paquete o en un bulto vagamente parecido a una partícula, pero entonces ésta, ni siquiera tendría una cantidad de movimiento definida. A su debido tiempo esta extraña idea no sólo llegaría a ser aceptada sino que se conocería como el principio de incertidumbre de Heisenberg[2][12][16].
El principio del profesor Heisenberg describía en términos generales las nuevas Leyes de la Física, los detalles se podrían encontrar al resolver una nueva Ecuación dada por Erwin Schrödinger y cuando se resolvió esa Ecuación ofreció una imagen del Átomo que iba más allá de la imaginada por Niels Bohor.

La nueva teoría llamada Mecánica Cuántica explicaría mucho más que los estados del Átomo de Hidrógeno, explicaría también todos los otros Átomos de todos los otros Elementos. La Mecánica Cuántica puede muy bien convertirse en el triunfo definitivo de la Física, pero como muchos triunfos fue adquirido con un costo enorme, desafía la idea más fundamental de todas, la relación entre Causa y Efecto[18][4].

En la Física Aristotélica cada movimiento tenía que tener una causa inmediata, se necesitaba un impulso para mantener en movimiento una bala de cañón. En la Física Newtoniana el movimiento ya no necesitaba de una causa, pero cada cambio en el movimiento sí la necesitaba. Sin embargo, en la Física Moderna dada una causa no siempre se produce el mismo efecto, éste es el verdadero abandono del pasado, los resultados de un conjunto dado de circunstancias no estaban completamente determinados, hay resultados alternativos posibles, sólo están determinadas con precisión las probabilidades de las alternativas, esta falta de determinismo es verdaderamente revolucionaria y no debe confundirse con una situación similar que surgió en la Física Newtoniana.

La Estadística se ha utilizado extensamente para describir el movimiento de las Moléculas en un gas, eso fue solamente un procedimiento práctico, teóricamente se podía calcular la trayectoria de cada bolita sólida, teóricamente se podía predecir el futuro del Universo[8][12], sencillamente no era práctico hacerlo, pero con la Mecánica Cuántica la situación ha cambiado fundamentalmente,

como una cuestión de principios las trayectorias de las Partículas Atómicas no puede predecirse con exactitud y el futuro del Universo no es predeterminado.

En los países como en el campo de la ciencia, tienen lugar revoluciones, vienen y se van y las cosas permanecen más o menos igual, incluso en el Universo Mecánico Cuántico algunas cosas no han cambiado[16].

La Energía se conserva, como siempre lo hace y así la cantidad de movimiento y también el movimiento cinético de hecho esas mismas ideas residen en el propio corazón de la Física Moderna, por ejemplo en la Teoría de la Relatividad se conserva la cantidad de movimiento aún cuando eso signifique que la Masa debe aumentar con la Velocidad y es precisamente por esto, que Energía es igual a Masa por la Velocidad de la Luz al cuadrado $E = mc^2$; Incluso Niels Bohr a pesar de su audacia no desafío la idea de que la Energía se conserva siempre y la idea de Energía sigue siendo fundamental, incluso para las Partículas Fundamentales[1][5][12][6]. Con respecto al momento cinético la idea no sólo guió a Niels Bohr, sino que surgió como un concepto central de la nueva Física en que cada Electrón por no mencionar las otras Partículas Elementales es un tipo de Giróscopo Mecánico Cuántico y sin embargo, es difícil imaginar cambios más profundos que los originados por estas dos grandes revoluciones separadas solamente unos pocos cientos de años, primero las esferas de cristal de los antiguos se transformaron en una máquina racional perfectamente ordenada, el Universo Mecánico y luego en un asombroso cambio de rumbo de los acontecimientos, el Tiempo y el Espacio, la Materia y el Movimiento, los émbolos y engranajes propios de la gran máquina se hicieron irreconocibles, es entonces la entrada al Universo Mecánico Cuántico. Es así como da inicio la mecánica cuántica, como un pensamiento radical sobre el comportamiento de la naturaleza, tratando de resolver los fenómenos curiosos e inexplicables que presenta la materia en un Macro y Micro Universo del cual formamos parte[14][15].

Ondas o partículas, he ahí el dilema.

Uno de los temas principales de la Mecánica Cuántica fue explicar la inexistencia del concepto de Trayectoria de Partículas. A consecuencia del comportamiento dual que presentaban los

Electrones como Onda y como Partícula, la Mecánica Cuántica sugiere la existencia de la indeterminación en la realidad[4][7].

Resulta interesante analizar brevemente el comportamiento de Difracción de la Luz como inicio de este curioso y revolucionario pensamiento. Al pasar un haz de Luz por un cristal, en el haz emergente se observa una figura formada por varias intensidades de Luz y sombras separadas por espacios, análogo a la Difracción por Ondas Electromagnéticas.

Es decir, en ciertas condiciones una Partícula como el Electrón se puede comportar como una Onda. Para explicar esta idea, los Físicos usaron un curioso experimento realizado por Young conocido como Difracción de Electrones mediante doble rendija usando esta vez un haz de Electrones en lugar de un haz de Luz. En este experimento, el comportamiento de los Electrones, debido a la interferencia no se reduce a la simple Superposición de acciones individuales. Tal como lo predice el comportamiento clásico[17][18][13].

Los resultados del experimento demostraron que el torrente de Partículas se separaría en dos, y estos torrentes ahora más pequeños interferirían entre sí, dejando el mismo patrón de luz-oscuridad que se obtuvo con el experimento de Luz. Las partículas se comportaron como Ondas.

Luis de Broglie intentando hacer carrera en el gobierno francés sacó un título en Historia un nuevo enfoque de la Física verdaderamente nuevo, quizás sea esa la razón por la que en la década de 1920 el fue el único que planteó una pregunta crucial. Si las Ondas de la Luz pueden ser Partículas, ¿Es posible que Partículas tales como los Electrones puedan ser también Ondas?

Para empezar las Partículas tienen Energía y cantidad de movimiento, mientras que las Ondas tienen Frecuencia y Longitud de Onda

Partículas	**Ondas**
Energía E	Frecuencia f
$E = mc^2$	$f = \frac{c}{\lambda}$
Momento p	Longitud de Onda λ
$p = mv$	

Evidentemente esas entidades tienen diferentes tipos de propiedades pero Luis de Broglie sospechaba que había algún tipo de conexión y la teoría de Max Planck había dado una pista de cual podía ser.

Max Planck había asociado la Energía de una Partícula de Luz con la Frecuencia de su Onda, dando un paso más.

$$E = hf$$

Luis de Broglie combinó ésto con la Energía de una Partícula de acuerdo con la Teoría de Relatividad de Albert Einstein

$$mc^2 = h\frac{c}{\lambda}$$

$$mc = \frac{h}{\lambda}$$

Esta atrevida combinación de las propiedades de la Onda y de la Partícula sugirió el paso siguiente: ¿Podrían unas Partículas que viajan a menos Velocidad que la Luz, tener su cantidad de movimiento relacionada con la Longitud de Onda?[16][14][11]

$$mv = \frac{h}{\lambda}$$

Luis de Broglie, así lo creía, pensaba que igual que la Energía de una Partícula está relacionada con una Frecuencia, la cantidad de movimiento de una Partícula está relacionada con una Longitud de Onda.

$$p = \frac{h}{\lambda}$$

Era una idea radical, no sólo las Ondas de la Luz pueden comportarse como Partículas, sino que las Partículas pueden comportarse como Ondas, pero antes de un año los experimentos habían verificado que los haces de Electrones podrían ser difractados en forma muy similar a los Rayos de Luz, incluso más…, la idea de Luis de Broglie parecía explicar uno de los aspectos más misteriosos del modelo de Niels Bohr del Átomo[10].

La teoría de Niels Bohr estaba construida sobre la idea de que los Electrones solamente pueden existir en Órbitas de determinados tamaños, sólo en esas Órbitas y en ningún otro lugar entre

ellas. Pero si se consideran los Electrones como Ondas dando vueltas alrededor del núcleo tienen que existir en Órbitas cuya Longitud crezca según Longitudes de Onda enteras, de esa forma cada Órbita consiste en Ondas del Electrón que producen interferencias constructivas y se refuerzan así mismas en cada Órbita, cuando se combinó con las formulas de Luis de Broglie esta idea reprodujo con exactitud las Orbitas del modelo de Niels Bohr del Átomo, porque el momento cinético de cada Órbita sería un número entero multiplicado por $\hbar$ que se define como $\frac{h}{2\pi}$, por lo tanto, la idea de Luis de Broglie había sido brillante, había dado una explicación profunda y elegante del modelo de Niels Bohr del Átomo, se había apoyado en una evidencia experimental sólida y no sorprende que llevara a otros Físicos a profundizar cada vez más en la Naturaleza de la Materia.

En Austria, Erwin Schrödinger, reflexionando sobre las implicaciones del trabajo del científico francés, elaboró una teoría propia extraída de las ideas de Luis de Broglie[11][8][3].

Una Onda tiene una Amplitud y una Longitud de Onda, pero no tiene ni principio ni final, ni nada parecido a la posición determinada de una Partícula, lo que continúa siendo cierto, si se le suma una Onda de la misma Longitud de Onda ya sea en fase o fuera de fase, pero si se suman Ondas de distintas Longitudes se altera la forma de la resultante, si esas Longitudes de Onda son próximas y especialmente si se suman mas Ondas de Longitud próximas, el resultado puede ser un tipo de Onda concentrada en una región limitada del espacio, de manera que con una gama de Longitudes de Onda y por lo tanto, una gama de cantidades de movimiento, se puede construir algo parecido a una Onda situada en un lugar bastante determinado, pero debido a que tiene una gama de cantidades de movimiento se extiende cuando se desplaza, no es verdaderamente una Partícula y no es verdaderamente una Onda, ¿Qué es, realmente?[4]

Es la descripción más clara posible de la Naturaleza de los Fotones y de los Electrones, de la Materia que forma el Universo y todo lo que hay en él y como idea en 1926 fue el corazón y alma de la Mecánica Ondulatoria de Erwin Schrödinger[11].

La Luz al pasar por dos rendijas causa una evidente interferencia de Ondas, la cual se revela claramente como una configuración de franjas luminosas y oscuras. No hay duda de que la Luz es una Onda, pues solamente las Ondas se comportan de este modo, de manera que la pregunta es: ¿Cómo puede la Luz estar formada por Partículas y a pesar de eso producir interferencias como las Ondas?[18], si la Luz está formada por Partículas, Fotones, cosas pequeñas e individuales que no pueden llegar como una estructura extendida, entonces cada Partícula tiene que golpear sobre la pantalla en forma individual, un único punto de Luz por aquí, otro Fotón allí, es imposible predecir con exactitud donde aparecerá un punto, pero es posible ver que lleguen más Fotones a unos lugares que a otros, de hecho hay una probabilidad mayor de que lleguen mas Fotones a ciertas zonas y finalmente debido a esas probabilidades el resultado será una determinada estructura de difracción parecida a una Onda y constituida por Partículas[17].

Esta fue la explicación propuesta por Max Born, los Fotones pueden ser Partículas, dijo, pero las estructuras que producen se rigen por probabilidades que crean interferencias como si se trataran de ondas[4].

Werner Heisenberg, uno de los amigos de Max Born, llevó esta idea un paso más adelante; Dijo: como las Partículas están asociadas con las probabilidades que crean interferencias lo mismo que las Ondas, es imposible conocer tanto la cantidad de movimiento exacta como la posición exacta de cualquier Partícula al mismo tiempo, la idea puede ser un poco difícil de captar, pero ahí esta justamente la cuestión, las Partículas al ser Ondas al mismo tiempo son algo difíciles de captar[6][8].

Es propio de una Onda normal con una determinada Longitud de Onda, el extenderse por el espacio, si esta Onda representa una Partícula entonces su Longitud de Onda se traduce en una cantidad de movimiento determinada, sin embargo no hay nada aquí que explique la ubicación de la Partícula. La posición de la Partícula se puede hacer más determinada sumando una tras otra, Ondas de diferentes Longitudes, pero cada nueva Longitud de Onda significa una nueva cantidad de movimiento, en otras palabras, cuanto más se sabe acerca de la posición de una Partícula menos se puede decir acerca de adónde va y a qué velocidad va, cuanto mas determinada se hace

la posición de la Onda menos determinada se hace la cantidad de movimiento de la Partícula[3][10].

Esa relación recibe el nombre de “Principio de incertidumbre de Heisenberg”

$$\Delta x \Delta p \approx \hbar$$

Werner Heisenberg buscando una verdad científica más profunda había elevado la incertidumbre al nivel de un principio fundamental de la Naturaleza.

Pero la ironía consistió en que Max Planck interesado en buscar algo universal en la Naturaleza de todos los cuerpos brillantes, descubrió que la luz es irradiada en pequeños paquetes de Energía.

$$E = hf$$

Cuando Albert Einstein resolvió el problema del Efecto Fotoeléctrico confirmó que los paquetes de Energía de Planck existen como Partículas en el Campo Electromagnético.

$$K = hf - \phi$$

Combinando los puntos de vista de Max Plank y Albert Einstein; Luis de Broglie sugirió que no sólo las Ondas podrían comportarse como Partículas, sino que las Partículas podrían comportarse como Ondas.

$$p = \frac{h}{\lambda}$$

Erwin Schrödinger pensó que si se suman un numero suficiente de Ondas de diferentes Longitudes el resultado es una Onda que está concentrada en uno u otro lugar como una Partícula, entonces Max Born vio que mientras, que es evidentemente imposible para una Partícula crear una estructura de Onda visible un grupo de Partículas cuyo comportamiento esta determinado por las probabilidades puede desembocar en una estructura que se asemeje muchísimo a una interferencia de ondas[18][17][14].

Y Werner Heisenberg vio en ese mismo hecho el intercambio entre las características de la Luz como Partícula y las características de la Luz como Onda, cuando las incertidumbres de posición y cantidad de movimiento se combinan el producto es aproximadamente igual a la constante de

Max Planck y esto comienza con la constante de Max Planck y cerrando el circuito acaba en la constante de Max Planck, esa es la ironía, la búsqueda de la verdad se convirtió para Planck en un viaje que conducía al corazón de la Física Cuántica, sin embargo, hasta el final nunca aceptó las profundas implicaciones de su propio trabajo y el caso es que tampoco lo hizo Albert Einstein quien dijo: "Parece difícil ver las cartas de Dios, pero no puedo ni por un momento creer que él, juegue a los dados" como pretende la Teoría Cuántica actual.

Harían falta nuevas generaciones de brillantes jóvenes para aceptar completamente las implicaciones asombrosas de la nueva teoría, ellas honran y obedecen a las Leyes de la Mecánica clásica pero adoptan también la Teoría Cuántica, hasta ahora nadie puede negar la perfección teórica de la nueva Física y el hecho de que realmente funciona[6][8][9].

¿Y el gato de Schrödinger?

La Teoría Cuántica genera muchas paradojas, quizá la más importante es la de la Superposición refiriendo a la idea de que un objeto puede estar en un sitio y en otro al mismo tiempo[11].

Erwin Schrödinger propuso un experimento mental para intentar resolver esta incógnita, se trata de un interesante modelo que ilustra la naturaleza aleatoria de la Mecánica Cuántica para ilustrar las diferencias entre interacción y medida en el campo de la Mecánica Cuántica.

Cuando se habla del "Gato de Schrödinger" se está haciendo referencia a una paradoja que surge de un célebre experimento imaginario propuesto por Erwin Schrödinger en el año 1937[2][5].

El experimento mental consiste en imaginar a un gato metido dentro de una caja que también contiene un curioso y peligroso dispositivo. Este dispositivo está formado por una botella de vidrio que contiene veneno y por un martillo sujeto sobre la botella de forma que si cae sobre ella la rompe y se escapa el veneno, con lo que el gato moriría. El martillo está conectado a un mecanismo detector de Partículas *alfa*; si llega una Partícula *alfa,* el martillo cae rompiendo la

botella con lo que el gato muere, por el contrario, si no llega no ocurre nada y el gato continua vivo.

Cuando todo el dispositivo está preparado, se realiza el experimento. Al lado del detector se sitúa un Átomo radiactivo con unas determinadas características: tiene un 50% de probabilidades de emitir una Partícula *alfa* en una hora. Evidentemente, al cabo de una hora habrá ocurrido uno de los dos sucesos posibles: el Átomo ha emitido una partícula *alfa* o no la ha emitido (la probabilidad de que ocurra una cosa o la otra es la misma). Como resultado de la interacción, en el interior de la caja, el gato está vivo o está muerto. Pero no podemos saberlo si no la abrimos para comprobarlo.

Si lo que ocurre en el interior de la caja lo intentamos describir aplicando las Leyes de la Mecánica Cuántica, llegamos a una conclusión muy extraña. El gato vendrá descrito por una función de onda extremadamente compleja resultado de la superposición de dos estados combinados al cincuenta por ciento: "gato vivo" y "gato muerto". Es decir, aplicando el formalismo Cuántico, el gato estaría a la vez vivo y muerto; se trataría de dos estados al mismo tiempo[10][15][16][12].

La única forma de averiguar qué ha ocurrido con el gato es realizar una medida: abrir la caja y mirar dentro. En unos casos nos encontraremos al gato vivo y en otros, muerto. Pero, ¿qué ha ocurrido? Al realizar la medida, el observador interactúa con el sistema y lo altera, rompe la superposición de estados y el sistema se decanta por uno de sus dos estados posibles.
El sentido común nos indica que el gato no puede estar vivo y muerto a la vez. Pero la Mecánica Cuántica dice que mientras nadie mire en el interior de la caja el gato se encuentra en una superposición de los dos estados: vivo y muerto.

Esta superposición de estados es una consecuencia de la Naturaleza de la Materia y su aplicación a la descripción Mecánica Cuántica de los sistemas Físicos, lo que permite explicar el comportamiento de las Partículas Elementales y de los Átomos. La aplicación a sistemas macroscópicos como el gato o, incluso, si así se prefiere, cualquier profesor de Física, nos llevaría a la paradoja que nos propone Schrödinger[11].

Postulados de la Mecánica Cuántica.

La Mecánica Cuántica es el marco matemático para el desarrollo de nuevas Teorías Físicas. De por sí, la Mecánica Cuántica no indica qué ley obedece un Sistema Físico, Químico o Biológico pero sí provee el marco conceptual para el desarrollo de esas leyes.

"La Mecánica Cuántica y el entendimiento de nuestro Universo depende de un conjunto de postulados que conectan al mundo Físico con el formalismo Matemático".

Estos postulados han sido deducidos por un largo proceso de prueba y error, y sus fundamentos siguen siendo sorprendentes incluso para sus múltiples autores. Cuando de aquí en más y en los apartados dedicados a la Mecánica Cuántica mencionemos a la Física, recordemos que ella condiciona a la Química y por ende a la Biología, o sea, toda conclusión que afecte a los sistemas Físicos, impactará sobre los Biológicos en el mundo real[18].

"POSTULADO 1: Asociado con cada Sistema Físico, se encuentra un espacio de Hilbert (H) (Espacio vectorial complejo con producto interno normalizado) conocido como espacio de estados del sistema. El sistema es completamente descrito por su vector de estado, el cual es un vector unitario en dicho espacio de estados."

El sistema más simple de la Mecánica Cuántica y el que más nos interesa desde el punto de vista de la complejidad, es el qubit (***quantum bit***) o unidad elemental de información cuántica[12].

"POSTULADO 2: La evolución de un Sistema Cuántico cerrado (estrictamente aislado, sin intercambio de energía con su medio ambiente) es descrita por una transformación unitaria. Esto es que el estado $|\Psi\rangle$ del sistema al tiempo t_1 está vinculado al estado $|\Psi'\rangle$ al tiempo t_2 por un operador unitario U que depende sólo de t_1 y t_2 tal que $|\Psi'\rangle = U|\Psi\rangle$"

Se define U como operador hermítico, si $U = U^+$ y como *operador unitario* si $U^{-1} = U^+$. Queda claro que si un operador es hermítico y unitario, se cumple que $U^2 = I$ la matriz unitaria. Como

ejemplos de operadores hermíticos y unitarios tenemos las ***matrices de Pauli*** (en H^2*).* En general todo operador es representable por una matriz (o producto vectorial de matrices o vectores)[13]

$$I \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{pmatrix} 0 & -i \\ +i & 1 \end{pmatrix} \quad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

que forman una base ortonormal y permiten escribir a todo vector en H^2 como combinación lineal $|\Psi\rangle = \Sigma_{i=1,X,Y,Z}\alpha_i\sigma_i$ Otro operador con idénticas propiedades y de interés para el procesamiento de información es el operador de Hadamard

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

o como matriz $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Para que se cumpla el postulado 2 se requiere que el sistema no interactúe con su medio ambiente. Estrictamente todo sistema real (que no sea el propio universo) interactúa parcial o totalmente con otros sistemas, sin embargo muchas veces es posible abstraer esa interacción y aplicar este principio[16].

El postulado 2 describe cómo se correlacionan en el tiempo los estados cuánticos de un sistema cerrado. Una versión más refinada de este postulado describe la evolución del sistema en tiempo continuo a través de un sistema de ecuaciones diferenciales ordinarias[12].

"POSTULADO 2': La evolución en el tiempo de un sistema cuántico cerrado es descrita por la Ecuación de Onda de Schrödinger $i\hbar\frac{d|\Psi\rangle}{dt} = H|\Psi\rangle$ donde H es el operador Hamiltoniano (hermítico y unitario), donde $\hbar$ es la constante de Planck ya analizada"

El Hamiltoniano (H) define la energía del sistema (que puede variar de naturaleza) y si se lo conoce se puede predecir la dinámica de ese sistema. En general describir H es un problema

extremadamente complejo y que en muchos casos relativamente simples, llevó buena parte del estudio de la Física de los siglos XIX y XX el comprender esta estructura matemática.

Dado que H es un operador hermético posee descomposición espectral

$$H = \sum_E E \left| E \right\rangle \left\langle E \right|$$

donde E son los *autovalores* y $\left| E \right\rangle$ los correspondientes *autovectores* normalizados. Los estados $\left| E \right\rangle$ son conocidos como los *autoestados de energía* o *estados estacionarios* y E es la *energía* del estado $\left| E \right\rangle$. La energía más baja es conocida como el nivel de base del sistema y el correspondiente autoestado como el estado basal. Los autoestados $\left| E \right\rangle$ evolucionan en el tiempo hasta llegar a un valor estacionario o constante a partir del estado inicial

$$\left| E_t \right\rangle \equiv e^{\frac{-iEt}{\hbar}} \left| E_0 \right\rangle$$

La Ecuación de Schrödinger posee la siguiente solución general

$$\left| \Psi \left(t_2 \right) \right\rangle = e^{\frac{-iH\left(t_2 - t_1 \right)}{\hbar}} \left| \Psi \left(t_1 \right) \right\rangle \equiv U \left(t_2 - t_1 \right) \left| \Psi \left(t_1 \right) \right\rangle$$

Se puede demostrar que el operador $U \left(t_2 - t_1 \right)$ es unitario, por lo cual el postulado 2' coincide con el postulado 2. Además se puede demostrar que para todo operador unitario, existe un operador hermítico K tal que

$$U = e^{iK}$$

La evolución de los sistemas cuánticos cerrados ocurre a través de operadores unitarios, pero a veces los operadores interaccionan con el sistema (***medición***) y alteran su estado, pudiendo eliminar superposiciones. Este proceso se rige por el tercer postulado[17][13][7][10].

"POSTULADO 3: Las Mediciones Cuánticas son descritas por un conjunto $\{Mm\}$ de operadores de medición Estos son operadores que actúan sobre el espacio de estados del sistema medido. El subíndice m se refiere a los resultados posibles del experimento de medición. Si el estado de un sistema cuántico es $|\Psi\rangle$, inmediatamente antes de la medición, la probabilidad de ocurrencia de m es $p(m)=\langle\Psi|M_m^+M_m|\Psi\rangle$ y el estado del sistema después de la medición es $\frac{M_m|\Psi\rangle}{\sqrt{\langle\Psi|M_m^+M_m|\Psi\rangle}}$"

Los operadores de medición satisfacen la condición de completamiento

$$\sum_m M_m^+ M_m = I$$

La condición de completamiento expresa que las probabilidades de los resultados suman uno

$$1=\sum_m p(m)=\sum_m\langle\Psi|M_m^+M_m|\Psi\rangle$$

Supongamos ahora el caso más general en el cual estamos interesados en sistemas cuánticos formados por dos o más sistemas físicos distintos. El siguiente postulado explica cómo describir un sistema compuesto de esta clase[9][15][12].

"POSTULADO 4: El espacio de estados de un sistema físico compuesto es el producto tensorial de los espacios de estado de los componentes. Específicamente, si tenemos los sistemas numerados de 1 a n, si el estado del sistema 1 es $|\Psi_1\rangle$ y así sucesivamente, el estado conjunto del ensamble será $|\Psi_1\rangle\otimes|\Psi_2\rangle\otimes\ldots\otimes|\Psi_n\rangle$"

Hay una aproximación heurística a este principio. Se suele mencionar como el *principio de superposición de la mecánica cuántica* al que plantea que si $|x\rangle$ e $|y\rangle$ son dos estados de un

sistema cuántico, entonces cualquier superposición $\alpha|x\rangle+\beta|y\rangle$ también será un estado válido de otro sistema, específicamente el sistema superpuesto de los dos anteriores.

Además se debe cumplir la condición de renormalización $|\alpha|^2+|\beta|^2=1$. El producto tensorial permite que para el caso de superponer dos sistemas con funciones de estado en los espacios H^n *y* H^m , el espacio resultante será $H^n \otimes H^m = H^{n,m}$ logrando esa multiplicación de combinaciones[18][14].

El Operador Densidad y los Postulados.

POSTULADO 1: A cada sistema físico aislado se le asocia un espacio vectorial complejo con producto interno un espacio de Hilbert conocido como el espacio de estados del sistema. El sistema se describe completamente con un operador positivo de traza unitaria denominado **operador densidad** (o matriz de densidad ρ). Si un sistema cuántico está en el estado ρ_i con probabilidad p_i, entonces el operador de densidad del sistema será $\rho=\sum_i p_i\rho_i$ [2][8]

POSTULADO 2: La evolución de un sistema cuántico cerrado ρ se describe por una **transformación unitaria**. O sea, el estado ρ del sistema al tiempo t_1 está vinculado al estado ρ' del sistema en el tiempo t_2 por un **operador unitario** U que sólo depende de los tiempos t_1 y t_2 según la ecuación $\rho'=U\rho U^+$ [10][12]

POSTULADO 3: Las mediciones cuánticas son descriptas por un conjunto $\{M_m\}$ de **operadores de medición**. El índice m se refiere a los resultados de esa medición. Si inmediatamente antes de una medición el estado del sistema cuántico es ρ , entonces la probabilidad que ocurra el resultado m es $p(m)=tr\left(M_m^+M_m\rho\right)$. Los operadores de medición satisfacen la condición de completamiento $\sum_m M_m^+M_m=I$ y el estado residual del sistema una vez medido m será $\frac{M_m\rho M_m^+}{tr\left(M_m^+M_m\rho\right)}$ [9][3]**POSTULADO 4:** El espacio de estados de un sistema físico

compuesto es el producto tensorial del espacio de estados de los sistemas físicos componentes. Si se tienen n sistemas, el operador densidad conjunto será $\rho = \rho_1 \otimes \rho_2 \otimes \rho_3 \ldots \otimes \rho_n$ [16]

Hemos discutido todos los postulados de la mecánica cuántica. Repasemos brevemente los mismos para ubicarlos en una perspectiva global.

- El primer postulado describe el escenario de la Mecánica Cuántica al fijar el modo de describir los Estados Cuánticos.
- El segundo nos habla de la dinámica de los estados, lo que se resuelve por la ecuación de Schrödinger y los operadores unitarios.
- El tercer postulado nos informa cómo extraer información de un sistema cuántico a través de mediciones.
- El cuarto postulado nos aclara como se combinan estados cuánticos individuales en un ensamble superpuesto.

Lo que es desconcertante en la Mecánica Cuántica, al menos desde el punto de vista de la Mecánica Clásica, es que no se puede observar directamente al estado del sistema. Es una especie de juego de ajedrez en el cual nunca podemos estar seguros en qué casilla se encuentra cada pieza. La Mecánica Clásica nos dice que las propiedades fundamentales de un objeto como la Energía, Posición y Velocidad son directamente observables y medibles. En la Mecánica Cuántica esas magnitudes dejan de ser importantes para ser reemplazadas por un Vector de Estado que no puede ser observado directamente.

Todo se comporta como si en la Mecánica Cuántica existiese un mundo oculto de acceso indirecto e imperfecto. Además observar un sistema clásico no cambia necesariamente el estado del mismo. En cambio en el mundo cuántico y de acuerdo al postulado 3 las mediciones son invasivas y normalmente alteran al sistema bajo estudio. Nos podríamos preguntar cómo siendo tan diferente la Cuántica de la Clásica, ¿por qué en el universo corriente que nos rodea no hay evidencia a favor de la primera? Resulta ser que el mundo clásico puede ser deducido de la Mecánica Cuántica como descripción aproximada del Universo en las escalas de Espacio, Longitud y Masa en las cuales nos desenvolvemos. Vemos que las mediciones cuánticas están vinculadas a distribuciones de probabilidades y por lo tanto son estadísticas o predecibles. El azar

está en la misma esencia del postulado tres, o sea en la verdadera Naturaleza del Universo. **La última respuesta a la naturaleza caótica de la biología es finalmente que desde el punto de vista ontológico la vida es esencialmente estocástica**. Al menos, mientras sobreviva la Mecánica Cuántica

Discusión.

La Mecánica Cuántica surge por la necesidad de comprender fenómenos de la naturaleza inexplicables a la Mecánica Clásica.

A finales del siglo XIX y principios del siglo XX se pensaba que las Teorías Físicas disponibles eran más que suficientes para explicar todos los fenómenos de la Naturaleza. Se creía entonces que toda pregunta hecha sobre el comportamiento de la misma tendría respuestas concretas, correctas y certeras mediante la aplicación de las teorías conocidas. Cuando se intenta utilizar la Mecánica Clásica para explicar fenómenos atómicos, los resultados obtenidos demuestran una clara contradicción con la experiencia. Ningún paradigma científico puede resistir un resultado de confrontación con la realidad.

Se pueden observar estos fenómenos más a detalle en un rango de "macrocosmos y microcosmos". La Mecánica Clásica explica los fenómenos de escala intermedia, los que podemos percibir simplemente con nuestros sentidos. Los objetos, las máquinas, el agua, los ríos, los mares, las olas, las nubes, los rayos, los truenos, el viento, el sol, la luna, las estrellas, etc., procesos con todas sus características y propiedades, de Masa, de Impulso, de Energía, el Calor, la Luz, los Colores y una variedad inmensa de cosas que se demuestran satisfactoriamente con teorías físico-matemáticas que se mencionan en la Mecánica Clásica.

Es interesante saber que todos estos sistemas físicos y procesos son los que han intervenido en el desarrollo y evolución de nuestra intuición, en cuanto a la expectativa que tenemos y que usamos para predecir el comportamiento de las cosas.

Si soltamos un objeto, predecimos con seguridad que va a caer o lo hará en cierto momento, porque eso es lo que hemos experimentado toda la vida. Si dejamos un objeto en un lugar, sabemos que permanecerá allí o que se moverá de acuerdo a causas y efectos conocidos. Si un objeto tiene alguna propiedad como tamaño, volumen, viscosidad, color, velocidad, o cierta posición, sabemos o intuimos que las características que posee un objeto están presentes o ausentes, pero con certeza y afirmación.

De ahí que el mundo que percibimos tal cual es, ha sido debido al desarrollo de la intuición influenciada por nuestro contacto directo e implícito con la Naturaleza, con sistemas que describe correctamente la Mecánica Clásica, decimos entonces que la intuición es clásica pero, aun así, no es de gran ayuda para explicar modelos extremadamente pequeños, es decir a escalas atómicas o el porqué un Electrón Orbital gira con Aceleración Angular y no produce o emite radiaciones, el porqué los Átomos son estructuralmente estables o porqué los Electrones pueden generar difracción y una serie de fenómenos peculiares en este microcosmos.
De igual forma en los modelos extremadamente grandes tampoco nos explica con claridad los fenómenos cosmológicos como la geometría del universo, el big-bang, expansión del Universo, la Gravitación Cuántica, los Hoyos Negros, la Teoría de Supercuerdas, o los modelos de un Universo cíclico, etc.

Estas diferencias entre la teoría y la experimentación señalan que la construcción de una teoría o modelo el cual explique el dominio del tiempo, las longitudes y las masas, extremadamente pequeñas o grandes, exige un cambio radical en las leyes, las ideas y en el pensamiento clásico fundamental que conocemos.
La naturaleza de las concepciones de la mecánica cuántica y el hecho de que estos conceptos no pueden ser visualizados propiamente hace difícil de captar el tema. En verdad algunas de las fallas descansan en la Mecánica Cuántica en sí misma, no sólo porque su alcance está en continua expansión y sus métodos están sufriendo un refinamiento constante, y sabemos que siempre es más difícil escribir acerca de algo que está en estado de cambio y desarrollo, y particularmente un desarrollo tan rápido, que hace dudar de teorías firmemente establecidas. No sólo esto sino también porque los físicos mismos están hasta la fecha todavía argumentando y discutiendo

acerca del significado mismo de la Mecánica Cuántica así como acerca de los aspectos específicos del mundo diminuto que describe.

Entramos en la Era del Espacio, donde de nuevo la Física es llamada para abrir el camino.
La Física del Espacio Cósmico difiere radicalmente de la Física "terrestre" en la que el mundo de lo extremadamente pequeño es de importancia primordial.

La antigua idea de lo pequeño y lo grande encuentra su confirmación en el espacio exterior. Las estrellas enormes y los átomos diminutos no sólo convergen sino también coexisten en unidad integral.

Es imposible escribir popularmente acerca de la ciencia sin recurrir a representaciones visuales. Y así con la Mecánica Cuántica trataremos de encontrar analogías y modelos en la naturaleza. Sin embargo, tales analogías de ninguna manera son exactas y profundas. Simplemente nos ayudan a obtener una concepción general de las cosas.

Por ejemplo, como veremos, en la frase *"los electrones giran alrededor de un núcleo atómico"* difícilmente tiene más significado para nosotros que *"la nieve es algo blanco como la sal y cae del cielo para los habitantes del desierto de Sonora"*.

El movimiento de un Electrón como tal es inconmensurablemente mucho más complejo que lo que sabemos acerca de ellos hoy, mañana y también ¡mil años después!

Ciertamente el desarrollo de la Mecánica Cuántica es una prueba más de la diversidad sin límite, de la inagotabilidad de las propiedades del Electrón.

Todavía hoy tenemos un conocimiento bastante fragmentario del mundo que nos rodea. Sólo estamos comenzando a penetrar en la corteza terrestre, así como en los océanos y en el espacio exterior. Apenas comenzamos a comprender la vida de los campos, de los bosques, de las montañas, de los desiertos, de los ríos y de aquellos atardeceres a la orilla del mar.

Si esto es así, cómo podemos esperar conocer más del mundo de los Átomos, el Núcleo Atómico y las Partículas Elementales, los cuales son mucho más difíciles de comprender. Hay tareas de exploración para la ciencia por cientos y miles de años. Por ahora estamos solamente en la fuente de un poderoso río de conocimientos.

Aún así, cosas maravillosas se revelan al explorador de este mundo recientemente descubierto. Horizontes verdaderamente fantásticos abren esta nueva ciencia a la Tecnología, la Industria, la Agricultura, la Medicina, las estaciones de Energía Nuclear, los Isótopos Radiactivos, las Baterías Solares, los Reactores Nucleares etc…, se encuentran entre algunos de ellos. Estamos en el inicio del control absoluto de las Radiaciones Termonucleares y penetrando más y más en el espacio exterior.

Estos brillantes logros del presente surgieron a partir de las semillas sembradas por varias mentes inquietas de nuestro pasado en un fértil suelo del conocimiento científico y desde entonces cuidadosamente cultivadas por una verdadera galaxia de brillantes científicos.

"No hay límite alguno para la imaginación de una mente febril".

Capítulo II

La esencia del Cómputo Cuántico

"We're so trendy we can't even escape ourselves"

Kurt Cobain (1967-1994)

Motivación para la Computación Cuántica.

La Computación Cuántica pretende ser un nuevo desarrollo Tecnológico para el Procesamiento de Información que depende de los fenómenos de la Naturaleza interpretados por la Mecánica Cuántica.

Para comprender la importancia de este desarrollo es necesario tomar en cuenta que la tecnología actual para el manejo de la información se basa en ideas de la Mecánica Clásica[1].

Los fundamentos de la Computación Moderna fueron establecidos por A. M. Turing en 1936, en su famoso artículo *"On computable numbers, with an application to the Entscheidungsproblem"*. Introdujo una definición matemática de computadora programable, conocido ahora como máquina de Turing. Demostró la existencia de una máquina de Turing Universal, capaz de simular cualquier máquina de Turing, y conjeturó que cualquier tarea que se pueda llevar a cabo sobre un dispositivo (por ejemplo una computadora moderna) también puede realizarse con una máquina de Turing. Este resultado, conocido como tesis de Church-Turing, estableció la base para el espectacular desarrollo de la Computación. Poco después se construyeron las primeras Computadoras Electrónicas. John von Neumann desarrolló un modelo teórico que reunía todos los elementos necesarios para poder construir una computadora tan potente como una Máquina de Turing Universal. El hardware se desarrolló rápidamente a partir del descubrimiento del transistor en 1947, desarrollado por John Bardeen, Walter Brattain y Will Shockley[16][17]. Desde entonces la potencia de las computadoras ha crecido sin cesar, hasta tal punto que Gordon Moore

en 1965 modelizó este crecimiento con la conocida Ley de Moore que originalmente establecía que la potencia de las computadoras se duplica cada dos años, intervalo que posteriormente tuvo que reducirse a 18 meses.

La Ley de Moore se ha cumplido con éxito aproximadamente desde 1960. Sin embargo muchos investigadores esperan que esto no sea así en las primeras décadas del siglo XXI. Los efectos cuánticos empiezan a dificultar el funcionamiento de los dispositivos electrónicos a medida que se miniaturizan.

Una posible solución al eventual fallo o incumplimiento de la ley de Moore consiste en modificar el modelo de computación actual y una alternativa posible es desarrollar un modelo cuántico de computación basado en Mecánica Cuántica[11][3][6].

La idea de superar en eficiencia al modelo de computación clásico no es nueva. Muchos equipos de investigación hicieron notar que ciertos tipos de computación analógica pueden resolver eficientemente problemas que no tienen solución eficiente en una máquina de Turing. Desgraciadamente para la computación, consideraciones realistas sobre la presencia de ruido en las computadoras analógicas hicieron inviable este modelo. Por este motivo, uno de los primeros desafíos del modelo de computación cuántica fue desarrollar las teorías de códigos correctores cuánticos y una computación cuántica tolerante a fallos[17][18].

A diferencia de lo que ocurre con la computación analógica, la computación cuántica puede obtener una cantidad finita de ruido manteniendo sus ventajas sobre el modelo clásico[8].

Para entender el porqué de este desarrollo, es necesario tomar en cuenta que toda la tecnología actual para el manejo de la información está basada en ideas de la mecánica clásica, ideas del siglo XVII, por supuesto que no nos referimos a la tecnología electrónica sino a la del procesamiento de la información así los paradigmas de Turing, Church y Von Neumann bajo los que funcionan actualmente las computadoras y que datan de los años del siglo pasado deberán de ser actualizados y tal vez parcialmente sustituidos por otros[1][3].

La necesidad de una revolución tecnológica es consecuencia de lo que según se ha comenzado a comprender recientemente, la información es una cantidad física análoga a la energía o a la entropía y por ello un sistema cuántico se comportara de manera diferente que un sistema clásico. Todo esto causa una gran curiosidad pues ha hecho necesario revisar las leyes, teorías e ideas clásicas de la computación para generalizarlas a un nivel cuántico. Según las investigaciones y descubrimientos de muchos expertos se esta produciendo un cambio de paradigma y como consecuencia la computación cuántica está destinada a ser una de las tecnologías de punta en desarrollo durante el siglo XXI[11][13][10].

A partir de una idea original de Richard Feynman (1918-1988), en los últimos años se ha desarrollado teorías sobre Computación Cuántica, que es al mismo tiempo un intento de diseñar computadoras más potentes que las conocidas hasta el momento y de comprender a la Mecánica Cuántica de una forma distinta, en los cuales, sistemas cuánticos se piensan como "computadoras" procesando información, con lo que efectos cuánticos aparentemente paradójicos de la Física Cuántica se lograran en un futuro, entender con mayor facilidad[2][5].

Teoría Clásica de Computación.

Ahora recurrimos a la Teoría Clásica de Computación. Esto se encuentra enfocado en su mayoría, en preguntas como: ¿Qué es computable? y ¿Qué recursos son necesarios?[4].

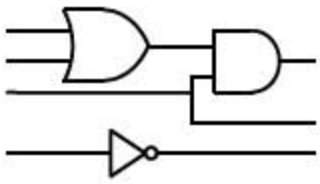
Fundamentalmente los recursos requeridos para computar, son una manera de almacenar y manipular símbolos. Las preguntas elementales son en este caso: ¿Qué tan complicados deben ser los símbolos?, ¿Cuántos símbolos necesitaremos?, ¿Qué tan complejas deben ser las manipulaciones?, y ¿Cuantos símbolos y manipulaciones necesitamos en un computo?[7][15].

En una visión general la computación es considerada difícil o ineficaz si la cantidad de recursos requeridos crecen exponencialmente con respecto al tamaño del problema. El tamaño del problema es dado por la cantidad de información requerida para especificar el problema. Aplicando esta idea en un nivel básico, encontramos que una computadora debe poder manipular

símbolos binarios, no simplemente símbolos unarios de otra manera el número de locaciones de memoria necesarias podría crecer exponencialmente con la cantidad de información a ser manipulada. Por otro lado, no es necesario trabajar en notación decimal (10 símbolos) o con cualquier otra notación con un alfabeto de más de dos símbolos. Esto simplifica significativamente el diseño de la computadora y su análisis[3][7].

Para manipular "n" símbolos binarios, no es necesario manipularlos todos al mismo tiempo, Se pude comprobar que cualquier transformación y operación puede ser manipulada por símbolos binarios, uno a la vez o en pares. En una operación binaria una "compuerta lógica" toma dos bits (x, y) como entradas, y calcula una función $f(x, y)$. Desde que "f" puede ser "0" ó "1", y si hay cuatro posibles entradas, hay 16 posibles funciones de "f". Este conjunto de 16 compuertas lógicas diferentes es nombrado "Conjunto Universal", de esta manera combinando tales compuertas lógicas en serie, cualquier transformación y operación de "n" bits puede ser llevada a cabo. Además, la acción de algunas de las 16 compuertas lógicas puede ser reproducida por la combinación de otras, para que no necesitamos todas las 16 compuertas y de esta manera simplificar el análisis de dichas manipulaciones, de hecho, solo una, la "compuerta lógica *NAND*", es necesaria para representar esta combinación de compuertas lógicas (el "*NAND*" indica *Not AND*, para que la salida sea "0" si y sólo si, ambas entradas son "1")[7][8][9].

Encadenando compuertas lógicas, podemos manipular símbolos de "$n-bit$".



"Una Computadora Clásica puede ser construida por redes de compuertas lógicas"[10]

Este acercamiento en general es conocido como un modelo de computación y es útil para nuestros propósitos porque sugiere como pensar en un modelo de computación cuántica, que en la actualidad es muy factible experimentalmente. En este modelo "clásico", los componentes

esenciales de una computadora son un conjunto de bits, varias copias y combinaciones de compuertas lógicas universales, unidas entre sí por alambres[12][15].

El Quantum contra la Física Clásica.

Para pensar sobre la teoría cuántica de información, primero mencionaré los siguientes principios de la Mecánica Cuántica, como indica. (Shankar 1980)[14].

1. El estado de un sistema aislado "Q" es representado por un vector estado $|\psi\rangle$ en un espacio de Hilbert.

2. Las variables como posición y momento son llamados observadores y son representadas por operadores Hermitianos. Los operadores de posición y momento "X, P" tienen los siguientes elementos de la matriz en el eigenbasis de "X":

$$\langle x|X|x'\rangle = x\delta(x-x')$$

$$\langle x|P|x'\rangle = -i\hbar\delta'(x-x')$$

3. El vector estado obedece la ecuación de Schrödinger.

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

Donde "$\mathcal{H}$" es el operador cuántico Hamiltoniano.

4. Postulado de la medida.

El cuarto postulado no ha sido explicado claramente, pues a menudo es un tema en discusión, desde que diferentes interpretaciones llevan a las mismas predicciones o conclusiones, puesto

que, el concepto de la “medida” está repleto de ambigüedades en la Mecánica Cuántica [Wheeler y Zurek 1983, Bell 1987, Peres 1993][14][19].

Sea $\mathbb{C}^{m\times n}$, donde "$\mathbb{C}$"es el campo de los números complejos, y el espacio de matrices de orden "$m\times n$", es decir, de matrices con "m" renglones y "n" columnas, con entradas de números complejos.

Para una matriz $M=(m_{ij})_{i,j}\in\mathbb{C}^{m\times n}$ su transpuesta hermitiana es:

$$M^{H}=(m_{ji}^{H})_{ji}\in\mathbb{C}^{n\times m}$$

donde para cada pareja de índices $(i,j)\in[\![0,m-1]\!]\times[\![0,n-1]\!]$

$$m_{ji}^{H}=\overline{m_{ij}}$$

Si $z=a+ib\in\mathbb{C}$ es un número complejo, entonces se tiene $\overline{z}=a-ib\in\mathbb{C}$ en su forma conjugada.

Una matriz $M=(m_{ij})_{i,j}\in\mathbb{C}^{m\times n}$ se dice ser *unitaria* si $M^{H}M=1_{nn}$, donde 1_{nn} denota a la matriz identidad de orden "$n\times n$".

Al subconjunto de vectores columnas unitarias en $\mathbb{C}^{m\times 1}$ (es decir, el espacio de vectores columnas de dimensión "m") se le llama conjunto de estados de un sistema físico cerrado, y la dimensión "m"se le conoce como el grado de libertad del sistema.
En $\mathbb{C}^{m\times 1}$ cada estado es un vector en la esfera euclidiana unitaria de $\mathbb{C}^{m}$.

Así pues $E_m=\left\{v\in\mathbb{C}^m\,\middle|\,1=v^{H}v=:\langle v|v\rangle\right\}$ el conjunto de estados.

Sea $e_j=(\delta_{ij})_{i<m}$ el j-ésimo vector de la base canónica de $\mathbb{C}^{m}$. Por lo tanto se tiene que todo vector de la base canónica es un estado.

Se dice que un estado $v=(\upsilon_{i1})_{i<m}$ produce la salida "i"con una probabilidad $\left|\upsilon_{i1}{}^2\right|=\mathrm{Re}(\upsilon_{i1})^2+\mathrm{Im}(\upsilon_{i1})^2$. [16][12]

Por lo tanto se obtiene el siguiente **Postulado de Medición:**

Si el estado actual es $v=(\upsilon_{i1})_{i<m}$ entonces, para cada "$i<m$", con probabilidad $\left|\upsilon_{i1}\right|^2$ se realiza lo siguiente: Se emite la respuesta "i"y se transmite al estado "e_i"; es decir este último será el estado actual en el paso siguiente[2][5].

De hecho el proceso de medición se realiza al final de cualquier algoritmo cuántico, así que el último estado actual al que se refiere en su enunciado es el estado final.

Ahora bien, sea $U\in\mathbb{C}^{m\times m}$ una matriz unitaria cuadrada de orden "$m\times m$".

"U" determinara una transformación ortogonal $\mathbb{C}^m\to\mathbb{C}^m : v\mapsto Uv$.

Además, al restringirla a "E_m" se obtiene una transformación $E_m\to E_m$.
"U" se dice ser una "compuerta cuántica". Un "algoritmo cuántico" es la composición de un número finito de compuertas cuánticas.

Una declaración que es válida para la mayoría de los propósitos prácticos es que, ciertas interacciones físicas son "mediciones" reconocibles. Su efecto en el vector estado $|\psi\rangle$ es cambiado a un eigenstate $|k\rangle$ de la variable medida, el valor de "k" es escogido al azar con probabilidad $P\propto\left|\langle k|\psi\rangle\right|^2$. El cambio $|\psi\rangle\to|k\rangle$ puede ser expresado por el operador de proyección $\left(|k\rangle\langle k|\right)/\langle k|\psi\rangle$. [6][18]

De acuerdo con las ecuaciones anteriores, la evolución de un sistema cuántico aislado siempre es unitario, es decir $|\psi(t)\rangle = U(t)|\psi(0)\rangle$ dónde $U(t) = \exp\left(-i\int \mathcal{H}\, dt/\hbar\right)$ es un operador unitario $UU^{\dagger} = I$.

"Esto es verdad, pero hay un problema, no existe tal cosa como un sistema completamente aislado". Es decir, que no experimenta interacciones con cualquier otro sistema, incluyendo, posiblemente el universo entero. Por lo tanto, siempre hay alguna aproximación involucrada usando la ecuación de Schrödinger para describir los sistemas reales[3].

Una manera de ocuparse de esta aproximación es hablar de un sistema "Q" y su entorno "T". La evolución de "Q" principalmente es obtenida por la ecuación de Schrödinger, pero la interacción entre "Q" y "T" tiene, en parte, el carácter de una medida de "Q". Esto produce una contribución no-unitaria a la evolución de "Q" (desde que las proyecciones no son unitarias) este fenómeno ubicuo se llama "decoherencia". He mencionado estas ideas porque son elementales en la mecánica cuántica y son principales herramientas para comprender mejor la posible computación cuántica[18][4][15].

Ahora podemos comenzar reuniendo ideas de Física y el Procesamiento de Información. Pues es claro que muchos fenómenos maravillosos de la Naturaleza observados a nuestro alrededor podrían ser comprendidos como una forma de procesamiento de información e inversamente nuestras computadoras podrían simular y analizar muchos patrones o comportamientos de la Naturaleza por su poderoso procesamiento[7][9].

Inevitablemente, si algo es impreciso, las preguntas son:

1. ¿Puede la Naturaleza considerarse útil como esencialmente un procesador de información?[6]

2. ¿Podría una computadora simular completamente a la Naturaleza?[2]

Los principios de mecánica cuántica sugieren que la respuesta a la primer pregunta sea: "Si". Pues, el vector estado $|\psi\rangle$ es elemental para la Mecánica Cuántica, un concepto como muchos aquéllos de ciencia de la información: Una entidad abstracta que contiene exactamente toda la información sobre el sistema "Q". La palabra "exactamente" aquí, es un recordatorio que no sólo es $|\psi\rangle$ una descripción completa de "Q", es también una que no contiene cualquier información extraña que no pueda asociarse significativamente con "Q". [14]

La segunda pregunta puede hacerse más precisa convirtiendo la tesis de Church-Turing en un principio de física.

"Todos los sistemas físicos finitos comprensibles pueden ser simulados por una máquina de computación universal que funcione en pasos finitos"[10]

Esta declaración es fundamentada por Deutsch (1985). La idea es proponer que un principio como éste, no es derivado de la Mecánica Cuántica, mejor aún, podría ser señalado como otros principios, por ejemplo, el de Conservación de la Energía.

Deutsch afirma que la tesis de Church es demasiado general en comparación con algunos de los principios físicos conocidos[19]. Deutsch propone referirse a las *"funciones que de manera natural sean consideradas computables"* como *"funciones que puedan ser computadas por un sistema físico real"*, ya que de esta forma lo que se quiere expresar es mucho más concreto. Todo esto le permitió introducir la concepción del diseño de una máquina de Turing[12].

La idea anteriormente expuesta es innovadora e interesante ya que para nosotros no es fácil entender que algo "considerado computable de forma natural" no pueda ser computado por la naturaleza. De esta manera, Deutsch convierte la tesis en un principio llamado "Principio de Church-Turing-Deutsch"[10].

La nueva versión de la tesis de Church-Turing (ahora llamado "Principio de Church-Turing-Deutsch") no se refiere a las máquinas de Turing. Esto es importante porque hay diferencias

fundamentales entre la misma naturaleza de la máquina de Turing y los principios de Mecánica Cuántica. Uno se describe por lo que se refiere a las operaciones clásicas con bits, y el otro por lo que se refiere a la evolución de estados cuánticos qubits[7].

Por otro lado existe la posibilidad en la que una máquina universal de Turing y por ende todas las computadoras clásicas, no pudiesen simular algún fenómeno o comportamiento de la Naturaleza. Recíprocamente, esto puede ser físicamente posible, es decir, que no fuera regido estrictamente por las leyes de Naturaleza comprender un nuevo tipo de computación esencialmente diferente de la informática clásica. Es el objetivo más importante de la Informática Cuántica[19].

Bit's y Qubit's

Actualmente, los microprocesadores, como los desarrollados por Intel y AMD, se componen por millones de chips. El material es un semiconductor como el silicio del cual aprovechamos sus propiedades eléctricas. La información se almacena en "bits", que no es más que, si pasa o no, corriente eléctrica: se le asigna un "1" si, "Si" pasa la corriente y un "0" si, "No" pasa la corriente o viceversa, no es más que un simple convenio. El significado del "1" ó del "0" es otra cuestión, en la computación actual una cadena de bits generalmente representa información numérica[8].

En los microprocesadores cuánticos estamos hablando de partículas en las cuales aprovechamos sus propiedades físicas basándonos en teoría cuántica. Estas propiedades cuánticas nos permiten almacenar la información no en bits, sino en lo que se llama **qubits** o **quantum bits**[17].

Las propiedades cuánticas nos permiten almacenar la información en qubits. La idea es que una partícula puede encontrarse, por ejemplo en dos estados (los mencionados "1" y "0", ó en una superposición de ambos estados "1,0"). Esta peculiaridad de las partículas permite alcanzar velocidades de procesamiento extremadamente más grandes. En la escala atómica la materia obedece las reglas de los mecanismos del quantum, que son absolutamente diferentes de las reglas clásicas que determinan las características de las compuertas lógicas convencionales[1][6].

El Bit

Bit es el acrónimo de **B**inary dig**it**. (dígito binario). Un bit es un dígito del sistema de numeración binario.

Mientras que en nuestro sistema de numeración decimal se usan diez dígitos, en el binario se usan sólo dos dígitos, el 0 y el 1. Un bit o dígito binario puede representar uno de esos dos valores, 0 ó 1.

$$\mathbb{Z}_2 = \{0,1\}$$

Podemos imaginarnos un bit como un foco que puede estar en uno de los siguientes dos estados:

Apagado,  o bien, encendido. 

El bit es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información. Con él, podemos representar dos valores cualesquiera, como verdadero o falso, abierto o cerrado, blanco o negro, norte o sur, masculino o femenino, amarillo o azul, etc. Basta con asignar uno de esos valores al estado de "apagado" (0), y el otro al estado de "encendido" (1).

"Los bits siempre han constituido el elemento básico de la computación actual"[17].

El Qubit

Un qubit (quantum bit), es la unidad elemental en la Computación Cuántica. Esta unidad puede representarse mediante el estado de un sistema cuántico binario, como ejemplo, el spin de un electrón. Matemáticamente, puede describirse por un vector estado en un sistema cuántico de dos niveles que equivale formalmente a un espacio vectorial de dos dimensiones sobre números complejos. Los dos estados básicos de un qubit son $|0\rangle$ y $|1\rangle$, se nombran: ket cero y ket uno,

que corresponden al "0" y "1" del bit clásico. Pero además, el qubit puede estar en un estado de Superposición Cuántica, la combinación de esos dos estados $\alpha|0\rangle+\beta|1\rangle$. Es en esto donde difiere completamente al estado de un bit clásico, ya que puede tomar probablemente alguno de los valores "0" ó "1". [14][8][3]

La unidad elemental de información cuántica qubit puede entenderse como un sistema de dos estados, como un spin "1/2" o un átomo de dos niveles, pero cuando medimos la información cuántica en qubits, realmente estamos haciendo algo mucho más abstracto, se dice que un sistema cuántico tiene "n" qubits, si, se tiene un espacio de Hilbert de "2^n" dimensiones, de esta manera se tiene disponibles "2^n" estados cuánticos mutuamente ortogonales[19].

Un qubit se representa por un vector estado en el espacio de Hilbert. Sea una base ortonormal (ortogonal y de norma unitaria).

$$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix} \quad ; \quad |1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$$

Y por lo tanto se suele representar de la siguiente manera:

$$|\Psi\rangle=\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\alpha|0\rangle+\beta|1\rangle$$

Donde "α" y "β" son complejos.

Cuando "α" y "β" no se anulan, se dice que los estados cero y uno están en superposición. Es decir un qubit se encuentra de manera simultánea en el estado clásico "0" y "1", sólo se define por una "medición o interacción"[18].

La condición de normalización del vector estado $|\Psi\rangle$ para que se comporte como vector unitario responde a:

$$\langle\Psi|\Psi\rangle=1$$

Lo equivalente a decir:

$$|\alpha|^2+|\beta|^2=1$$

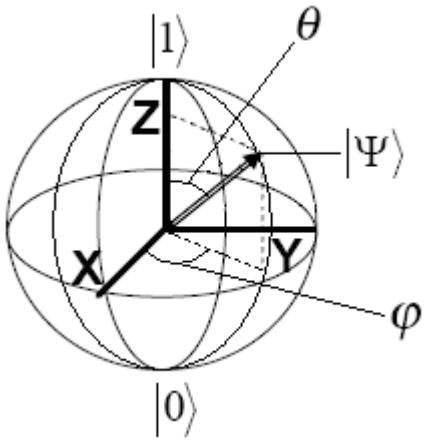
En donde, si $\alpha = r_1 + r_2 i$, entonces $|\alpha|^2 = \alpha$, por lo que tiene: $\alpha^* = r_1^2 + r_2^2$

Se ha comprobado que está ecuación solamente asegura que en la medición se obtenga uno de los dos estados. Debido a su naturaleza cuántica, cualquier medición del qubit altera inevitable su estado[12].

Un qubit puede existir en un estado de superposición, pero la medición del qubit ocasiona que la superposición colapse a sólo uno de los estados base, según las probabilidades.

El espacio de estados del qubit se puede representar mediante un espacio vectorial complejo bidimensional de módulo 1[16][9].

Equivalentemente, se puede representar geométricamente por la esfera de Bloch[19].



Los polos de la esfera de Bloch representan los estados clásicos "0" y "1", Cada estado del qubit corresponde a un punto de la superficie de la esfera, es decir que cada punto sobre la esfera "θ" ó "φ" representa la superposición entre ambos estados. Esto esencialmente significa que un qubit tiene dos grados de libertad. Estos grados de libertad podrían ser longitud y latitud, o bien dos ángulos[11][15].

Bit's vs Qubit's

La unicidad de las propiedades del mundo clásico con respecto al cuántico puede ser mejor comprendida si observamos sus características esenciales, de esta manera se resumen algunas de dichas características de la computación comparando las diferencias entre las unidades elementales de cada máquina[4][5][15].

Características esenciales	**Bit**	**Qubit**
Estado s de n (qu) bits	$s \in \{0,1\}^n$	$s = \Sigma_{x\in\{0,1\}^n} \lvert x\rangle$, si: $c_x \in \mathbb{C}$ y $\sum_x \lvert c_x\rvert = 1$
Evolución de un estado	Función Booleana $f:\{0,1\}^n \to \{0,1\}^n$	Matriz Unitaria U de $2^n \times 2^n$
N° de transformaciones	Muchas finitamente	Muchas incontablemente
Se obtiene por Medida	El estado s	Algunos estados clásicos (n bit's)
Estado después de la Medida	Inalterado	Alteración irreversible
Naturaleza de la Media	Deterministico	Estocastico
Composición de subsistemas	Producto Cartesiano $\times$	Producto Tensor $\otimes$
Tamaño de $n-(qu)$ bits	n	2^n
Universalmente es lograda	Exacta	Con arbitraria precisión
El estado de subsistemas	Siempre definida	Indefinido por los estados "entangled"

Compuertas cuánticas.

Para "$n=1$", consideraremos las siguientes *compuertas básicas*, llamadas también *operadores cuánticos*:

Identidad.

$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad I=\mathrm{H}_1\to\mathrm{H}_1 \text{ es el operador identidad.}$$

Negación.

$$N=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad \text{Se tiene } N:\begin{pmatrix}z_0\\ z_1\end{pmatrix}\mapsto\begin{pmatrix}z_1\\ z_0\end{pmatrix}$$

"N" es unitaria y tiene como función *permutar señales*, es de hecho "una reflexión a lo largo de la diagonal principal".

Hadamard.

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad \text{Se tiene } H:\begin{pmatrix}z_0\\ z_1\end{pmatrix}\mapsto\frac{1}{\sqrt{2}}\begin{pmatrix}z_0+z_1\\ z_0-z_1\end{pmatrix}$$

"H" es unitaria y tiene como función reflejar el plano respecto al eje "x" y rotar luego un ángulo de "$\pi/4$" radianes, en sentido opuesto a las manecillas del reloj.

Naturalmente, $N^{\otimes n}$ y $H^{\otimes n}$ son sendas compuertas en "H_n". Las matrices que las representan, respecto a la base producto "B_{H_n}", pueden ser calculadas mediante la relación siguiente relación.

Observamos que "$N^{\otimes n}$" actúa como el "complemento a 2^n-1", es decir, en los vectores básicos se tiene:

$$N^{\otimes n}(e_{\varepsilon_{n-1}\ldots\ldots\varepsilon_1\varepsilon_0})=e_{\delta_{n-1}\cdots\cdots\delta_1\delta_0}$$

En donde $(\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0)_2 + (\delta_{n-1}\cdots\delta_1\delta_0)_2 = 2^n - 1$

Observamos también que

$$H^{\otimes 1}(e_0) = \frac{1}{\sqrt{2}}(e_0 + e_1)$$

$$H^{\otimes 2}(e_{00}) = \frac{1}{\left(\sqrt{2}\right)^2}(e_{00} + e_{01} + e_{10} + e_{11})$$

y de manera general

$$H^{\otimes n}(e_{0\cdots 0}) = \frac{1}{\left(\sqrt{2}\right)^n}\left(\sum_{\varepsilon\in\{0,1\}^n} e_\varepsilon\right)$$

Es decir, el operador "$H^{\otimes n}$" aplicado al primer vector básico "$e_{0\cdots 0}$" produce el estado que promedia a todos los demás con valores uniformes[15][13][18].

Discusión

La idea de "Informática Cuántica" ha inspirado a muchas mentes inquietas simplemente porque las mismas palabras hacen pensar en algo extraño y poderoso, como si los científicos hubieran abierto el camino hacia una revolución en el procesamiento informático, siendo esto pan de cada día durante este milenio.

Pero, el término "revolución" podría ser una impresión falsa. La Informática Cuántica no reemplazará a la informática clásica, por las razones similares en que la Mecánica Cuántica no reemplaza a la mecánica clásica: nadie consultó alguna vez al profesor Heisenberg para diseñar una casa y nadie lleva su auto a un taller cuántico para ser reparado. Si las maravillosas computadoras cuánticas llegan a ser posibles en el mundo físico real, se usarán para ocuparse simplemente de las tareas especiales en las cuales nos beneficiaria el poderoso procesamiento de información cuántica, descubriendo por ejemplo: el tiempo de vida de nuestro planeta tierra, el

futuro del calentamiento global, el código genético, etc…, tareas que la computación clásica no puede resolver exitosamente.

Una razón más honesta para investigar sobre la informática cuántica es que es una nueva y profunda manera de pensar en las leyes fundamentales de la física. La comunidad de la informática cuántica aún es bastante pequeña en la actualidad, pero con el paso del tiempo y el progreso tecnológico ha ido aumentando y creciendo en los últimos años.

Las ideas sobre la teoría de información clásica parecen encajar en la Mecánica Cuántica como una mano en un guante, dándonos el sentimiento de que estamos descubriendo algo muy profundo sobre Naturaleza. El teorema silencioso de codificación de Shannon llevó a los científicos Schumacher y Josza a pensar en el teorema cuántico de codificación y la importancia del qubit como una medida útil de información. Esto nos permite seguirle la pista a la Información Cuántica y para estar seguro de que es independiente de los detalles del sistema en el que se almacene.

Esto es necesario para mencionar conceptos como: códigos detectores de error y correctores de error de la teoría clásica de computación, estos códigos clásicos llevaron a un descubrimiento análogo, el de códigos detectores error y correctores de error cuántico. Esto deja que en un proceso físico el cual antes fue pensado imposible se pueda obtener la recuperación casi perfecta de un estado cuántico general, deshaciendo así los procesos irreversibles como relajación por emisión espontánea. Por ejemplo, durante un largo proceso de detección y corrección de error en el computo cuántico usando métodos o modelos algorítmicos tolerantes a fallos, ya que cada qubit en la computadora podría corromperse un millón de veces y aun así la coherencia de la información cuántica se debe preservar.

Las preguntas de Hilbert con respecto a la estructura lógica de las matemáticas nos alientan a idear e imaginar un nuevo tipo de preguntas acerca de las leyes de físicas. Observando la ecuación de Schrödinger, podemos dejar a un lado si estamos describiendo un electrón o un planeta, y simplemente preguntarnos por las manipulaciones de partículas y los estados que se aceptan. El lenguaje de información y las ciencias computacionales así como la informática nos

permite idear cosas que se cuestionan de esa manera. Incluso una idea tan simple como las compuertas cuánticas viene a ser muy útil, porque nos permite pensar claramente en manipulaciones de estado cuántico que parecerían sumamente complicadas o complejas. Por otra parte tales ideas abren el horizonte al diseño de algoritmos cuánticos como los desarrollados por Shor, Grover y Kitaev. Estos algoritmos muestran que la Mecánica Cuántica permite el procesamiento de información de una forma diferente de las ya establecidas por leyes de la física clásica. Estos científicos como muchos otros investigadores creen que el comienzo del cómputo cuántico se encuentra en la propagación de un estado cuántico a través de un número exponencialmente grande de dimensiones en el espacio de Hilbert. El resultado de computación proviene de una interferencia controlada entre muchos caminos computacionales que se igualan después de que hemos examinado la descripción matemática, todas estas abstracciones numéricas aún parecen maravillosas y sorprendentes por el simple hecho de que se cumple perfectamente con las teorías de la Mecánica Cuántica.

La dificultad intrínseca de problemas en la Computación Cuántica respecto a la sensibilidad de interferencia en gran escala al ruido e imprecisión es un tema que a menudo es discutido contra la Computación Cuántica. Esencialmente un dispositivo analógico en lugar de un dispositivo digital tiene muchas limitaciones como resultado. Éste es un concepto erróneo. Es verdad que cualquier sistema cuántico tiene un espacio de estado continuo, pero esto lo tiene cualquier sistema clásico, incluso los circuitos de una computadora digital. Los métodos o modelos de computadoras tolerantes a fallos permitirán la detección y corrección de error, en una computadora cuántica restringida de un conjunto de compuertas cuánticas a un conjunto discreto, por consiguiente las "leyes" de los estados de las partículas en la computación cuántica serán discretos, así como en una computadora digital clásica. La diferencia más importante entre la computación analógica y digital es el incremento de la precisión de un resultado realizado por recursos analógicos o digitales, en base a esto uno debe pensar en re-diseñar una mejor máquina computacional, considerando que con métodos digitales uno necesita meramente un incremento en el número de bits, operaciones y por lo tanto mucho mas recursos como mayor procesamiento, mas memoria e incluso mas espacio. Aun así por el momento se piensa que la Computadora Cuántica tolerante a fallos tiene más en común con un dispositivo digital que un dispositivo analógico pero no lo excluye.

El algoritmo de Shor para el problema de la factorización estimuló mucho el interés en la Informática Cuántica, debido en parte a la relación que tiene con la encriptación de datos. Sin embargo, se cree que este algoritmo no se usará de manera principal para factorizar enteros grandes en el futuro, si así se requiere. Más bien, ha actuado como un estímulo fundamental en este campo de estudio, probando la existencia de un tipo nuevo y poderoso de computación, hecha posible por la evolución cuántica controlada, exhibiendo así, una cierta variedad de nuevos métodos.

Los títulos sobre la Computadora Cuántica seguirán siendo nombres equivocados para cualquier dispositivo experimental por lo menos en los próximos veinte o treinta años. Incluso es un abuso de lenguaje llamar a una calculadora de bolsillo computadora, porque la palabra ha llegado a ser reservada para máquinas de propósito general que más o menos comprenden el concepto de Turing sobre la Máquina Universal. Sin embargo, los pequeños procesadores de información actuales pueden servir para realizar tareas útiles. Por ejemplo, la simulación de los conceptos aprendidos en la teoría de la informática cuántica permitirán el descubrimiento de nuevos métodos o modelos espectroscópicos útiles en la Resonancia Magnética Nuclear (NMR).

La mayor satisfacción de la Computación Cuántica será recompensada por el hecho de crear una máquina de estas características. Sin embargo, algunos científicos opinan que tan sólo con investigar y experimentar sobre las teorías propuestas ya merece un gran mérito por tratar de averiguar que lo inalcanzable por el momento, podría ser realidad en un futuro. Uno de los principales usos de la tecnología más avanzada en la actualidad es destinada a la simulación de manipular momentos cuánticos para proporcionarnos una mejor comprensión sobre problemas como la decoherencia en la Mecánica Cuántica. Esto será fundamental en la investigación experimental durante los próximos años.

Por otro lado en teoría, hay dos preguntas abiertas sobre la naturaleza de los algoritmos cuánticos y los límites en la fiabilidad de la Informática Cuántica. No está del todo claro cuál es la naturaleza esencial de la Computación Cuántica y qué clase de problemas computacionales son dóciles a una solución eficaz por métodos cuánticos. ¿Hay una mina llena de algoritmos cuánticos útiles esperando a ser explorada?, o nos conformaremos con los pocos trozos que

hemos descubierto hasta ahora, o bien, ¿El poder de procesamiento con el que se sueña podría lograrse con menos de 100 qubits?. Esto se encuentra limitado por el conocimiento certero que se tiene actualmente, pues hoy en día es difícil simular 20 qubits incluso al utilizando todos los recursos clásicos más avanzados.

La fiabilidad Matemática y Física inmersa en la tecnología ha hecho posible el gran avance que se ha realizado hasta el momento para que se pueda tener un pensamiento optimista hacia la Informática Cuántica, ya que con el paso del tiempo se demuestra que no es un sueño imposible de lograr. Hoy en día podemos identificar los requisitos suficientes para garantizar una informática cuántica fiable y modelar una computadora cuántica cien veces más poderosa que la computadora clásica actual mas avanzada.

Espero que la Información Cuántica sea reconocida como una valiosa rama de Física Cuántica fundamental y que con el tiempo vaya creciendo la curiosidad de diversas áreas del conocimiento para así lograr una computadora cuántica convencional.

Capítulo III

Criptografía Cuántica

"I really haven't had that exciting of a life. There are a lot of things I wish I would have done, instead of just sitting around and complaining about having a boring life. So I pretty much like to make it up. I'd rather tell a story about somebody else…"

Kurt Cobain (1967-1994)

Despertando la curiosidad.

La Criptografía Cuántica es una aplicación muy importante de la Mecánica Cuántica y la primera con interés comercial en la Computación Cuántica.

La Computación Cuántica comenzó a desarrollarse en la década de los ochenta a raíz de las propuestas de Deutsch y principalmente de R. Feymann, que sugirieron independientemente que la propia evolución de los sistemas cuánticos se podría utilizar como herramienta de cálculo.

En 1994 aparece el primer resultado verdaderamente importante en computación cuántica. Se trata de los algoritmos polinomiales para la factorización de números enteros y cálculo de logaritmos discretos propuestos por P. Shor[4][12], que abren la posibilidad de que las computadoras cuánticas puedan romper los criptosistemas de clave pública.

Sabemos que la codificación usando claves privadas aleatorias de un solo uso como el caso del cifrado de Vernam, permite llevar a cabo una comunicación segura. Pero presenta la dificultad práctica de la distribución segura de las claves. Afortunadamente, las leyes de la Mecánica Cuántica proporcionan las herramientas necesarias para abordar este problema. La aportación cuántica a la seguridad del proceso de distribución de claves consiste esencialmente en que un

espía no puede extraer información sin revelar su presencia, ya que por las leyes de la Mecánica Cuántica no es posible copiar estados[1][3].

Existen diversos protocolos para la distribución cuántica de claves privadas. El más sencillo fue propuesto en 1984 por C.H. Bennett y G. Brassard[1] y se conoce como *BB*84. Después se propusieron diversas modificaciones que dan lugar a otros protocolos esencialmente equivalentes[10][11].

Criptografía.

La Criptografía es el arte de convertir un mensaje a una forma indescifrable de tal manera que no cualquier persona sea capaz de interpretarlo. El origen de la palabra criptografía proviene del griego “cripto”(oculto, secreto) y “grafos”(escritura.). Para lograr esto es necesario hacer uso de algún algoritmo, también conocido como criptosistema, para que combine o mezcle el mensaje con alguna información adicional y de esta forma generar un criptograma, es decir un mensaje cifrado. La información adicional utilizada para alterar dicho mensaje se conoce como clave[8].

Hay que distinguir también entre clave y cifra. Con la clave cambiamos una palabra o letra del mensaje original por otra, un buen ejemplo de código es la traducción de un idioma a otro. Mientras que la cifra actúa sobre los carácteres, un ejemplo de cifrado puede ser “eliminar los espacios en blanco y cambiar el orden de los caracteres de dos en dos”[9][13][6]. Con esto, si yo digo una frase, por ejemplo “emprender la guerra”, y la pasamos por el código inglés obtendríamos “to go to war” y con el cifrado anterior obtendríamos “merpneedlrgaeurra”.[8]

Hay dos tipos de clave, simétrica y asimétrica. La primera consiste en usar la misma clave para cifrar que para descifrar. La segunda emplea claves distintas para cifrado y descifrado[7][15].

Resulta evidente que para un criptosistema sea lo suficientemente seguro, debe ser imposible descifrar un mensaje si no se conoce la clave. Por esta razón es que nos debemos concentrar en mantener la clave segura y evitar que ésta sea interceptada. Sin embargo, los actuales

mecanismos clásicos de encripción aún presentan debilidades en este aspecto, pues en varias ocasiones muchos intrusos han conseguido obtener sus claves causando serios problemas a los sistemas de comunicación y a la información[2][5][14][17].

Un tipo de ataque clásico en criptografía se conoce como "Man-in-the-Middle Attack" el cual consiste básicamente en ubicar un dispositivo en el medio de una comunicación, y así éste puede recibir la información del transmisor para procesarla, interpretarla y finalmente reenviarla al receptor, sin que las partes lo detecten. Además este tipo de ataques es común gracias a que las claves se intercambian generalmente por redes públicas[9][16].

Es por esto que surge la gran necesidad de crear un mecanismo de encripción que no sea vulnerable a esta forma de ataques y es en este escenario donde tiene protagonismo la Criptografía Cuántica[16][18].

Distribución de claves.

Por años, se creyó que la única posibilidad para solucionar el problema de la distribución de claves fuese la de enviar la clave por algunos medios físicos por ejemplo en un disco. En la era digital, esta solución es claramente inusual e impráctica. Además, no es posible saber con seguridad si el medio que llevaba la clave fuera interceptado copiado o no[4][13].

La Distribución Cuántica de Claves, QKD (Quantum Key Distribution), es una tecnología que se propuso como solución a los problemas de distribución de claves en los criptosistemas clásicos. Basado en las leyes de la Mecánica Cuántica, la distribución cuántica de claves permite que las partes involucradas en una comunicación puedan intercambiar las claves de forma segura, las cuales de hecho se pueden utilizar en la criptografía clásica[17][18].

Debido a que la Criptografía Cuántica está fundamentada en la Mecánica Cuántica, obedece a las siguientes propiedades:

- No se pueden hacer medidas sin perturbar el sistema. (A menos que el estado sea compatible con la medición)[9].

- No se puede determinar simultáneamente y con un alto grado de precisión la posición y el momento de la partícula[3].

- No se puede medir la polarización del fotón en la base vertical/horizontal y en la base diagonal simultáneamente[7].

- No se puede duplicar un estado cuántico desconocido[13].

La primera regla puede ser interpretada como un punto de vista negativo de la Mecánica Cuántica comparada con la Mecánica Clásica. Sin embargo al ver el lado positivo debido a nuevos hitos en las concepciones de la información, permite pasar de una etapa de inconvenientes, a las aplicaciones potencialmente útiles, desprendiéndose el teorema de la no clonación: La copia perfecta en el mundo cuántico es imposible[15]. El hecho de que los estados cuánticos, también conocidos como información cuántica, no pueden ser copiados es uno de los atributos específicos de esta nueva clase de información tan diferente y por tanto tan atractiva, haciendo a la criptografía cuántica potencialmente segura. [10][19]

La idea principal de la distribución cuántica de claves consiste en explotar el hecho de que un estado cuántico no se puede copiar y que no es posible realizar una medición sin tener que alterar dicho estado cuántico. Es posible establecer un canal de comunicaciones seguro si la información clásica se transmite codificada en estados cuánticos únicos. Esto no quiere decir que se va a evitar que un espía extraiga información valiosa del canal, sino que será posible detectarlo inmediatamente[15][4]. En un canal de transmisión ideal, sin pérdidas y sin ruido, es posible detectar intrusos mediante el análisis del ruido introducido a los estados transmitidos. En canales reales, la situación es un poco más complicada pero sin embargo también es posible detectar la presencia de intrusos o de alteraciones en la comunicación[12][1].

Principio básico.

El principio básico de Criptografía Cuántica nos expresa lo sensible que es un sistema con características cuánticas al intervenir personas ajenas o no deseadas[2]. De acuerdo con la Física Cuántica, el solo hecho de observar un objeto cuántico lo cambia en una forma irreparable[19].

El impacto de partículas de luz lo calentará ligeramente y por lo tanto lo cambiará. Este efecto es muy pequeño en una hoja de papel, lo cual es un objeto macroscópico. Sin embargo, la situación es radicalmente diferente con un objeto microscópico. Si uno codifica el valor de un bit en un objeto cuántico solo, su intercepción necesariamente realizará una corrupción, porque la persona que escucha clandestinamente se ve forzada a observarla. Esta perturbación causa errores en la secuencia de los bits intercambiados por el remitente y el destinatario. Revisando en busca de la presencia de tales errores, los dos lugares distantes pueden saber si su mensaje fue interceptado o no. Es importante para hacer énfasis en que esta verificación tiene lugar después del cambio de bits, uno se entera a posteriormente si la comunicación fue escuchada a escondidas o no. Por esto es que esta tecnología se usa para intercambiar una información crucial y no valiosa. Una vez que la clave es validada, puede usarse para encriptar datos. La Física Cuántica permite demostrar que la intercepción de la clave sin corrupción es imposible[10][13][16][5].

Comunicación.

Uno de los problemas de mayor dificultad práctica a la hora de llevar a cabo una comunicación segura mediante un sistema de clave privada es la distribución segura de las claves[6].

La Criptografía Cuántica resuelve el problema de la "key distribution" o "distribución de claves" permitiendo el intercambio de una clave criptográfica entre dos lugares distantes con seguridad absoluta, respaldado por las leyes de Física. Esta clave puede ser usada con algoritmos criptográficos convencionales. Se podría decir, entonces, que, la distribución de claves cuánticas sería el titulo mas adecuado para la Criptografía Cuántica[5][1].

La criptografía segura requiere que las claves con que se cifran y descifran los mensajes no puedan ser descubiertas por terceros. La criptografía de clave pública es una forma de proveer claves secretas de manera que la encriptación efectuada por una de las partes sólo pueda ser desencriptada por la otra y por nadie más; y ello, pese a que parte de la información pertinente sea el dominio público. La seguridad del procesamiento depende de la dificultad inherente a ciertos problemas matemáticos; en especial, el de factorizar un número[11][14]. Es fácil calcular el producto de dos números grandes, pero extremadamente difícil volverlo a factorizar en números primos. En esa asimetría se basa el algoritmo de cifrado RSA, muy usado en la criptografía de clave pública. El mensaje confidencial que se transfiere entre el remitente y el receptor, previamente convertido por un procedimiento estándar en un número, se encripta mediante operaciones matemáticas en la que intervienen números extremadamente grandes relacionando factores primos entre ellos[5][17][3].

Precisamente una de las razones del éxito obtenido por el sistema de clave pública es que permite prescindir de acordar y distribuir la clave secreta. Sin embargo la seguridad de este sistema nunca ha sido probada matemáticamente. No se sabe si factorizar un número entero puede hacerse en tiempo polinomial, simplemente no se ha encontrado un algoritmo que lo haga[8][18]. Hacer un "crack informático" a un cifrado de clave pública resulta tan difícil, que el secreto de las claves se puede mantener durante poco más de una docena de años. Pero el advenimiento de la era de la Información Cuántica, y en particular de computadoras cuánticas capaces de realizar con rapidez factorizaciones mounstrosas, supondría seguramente el declive final del RSA y de otros métodos criptográficos[13].

Las leyes de la Mecánica Cuántica permiten abordar el problema de la distribución segura de claves privadas. Los usuarios pueden transmitir la clave privada a través de un canal cuántico. Por ejemplo, un cable de fibra óptica o como es el caso del uso de láser. En este caso, los estados de polarización de un fotón se pueden usar para diseñar un protocolo criptográfico cuántico para la distribución de una clave aleatoria de un solo uso[1][12].

En un proceso de distribución cuántica de claves, intervienen un emisor, un receptor, un espía y dos canales de comunicación, uno cuántico, para enviar fotones, y otro clásico para reconciliar y

depurar la información. El espía puede acceder al canal clásico y también puede acceder al canal cuántico y usar todos los medios que desee, con la única restricción de que sean compatibles con las leyes de la Mecánica Cuántica[13][19]. Los dos usuarios tanto emisor como receptor usan un trozo de su clave para detectar la presencia de espías y sólo en el caso de que no se detecten o que la información de éstos sea muy pequeña, dan por válida la clave.

El espacio de Hilbert $\mathcal{H}$ consideraremos las siguientes bases ortogonales:

$$\psi_0 = \left(|0\rangle, |1\rangle\right) \quad ; \quad \psi_1 = \left(|+\rangle, |-\rangle\right)$$

En los protocolos cuánticos de distribución de claves la idea será enviar una cadena de bits, usando para codificarla fotones polarizados en dirección horizontal o vertical $90°$, cuando se use "ψ_0" o en las direcciones de $\pm 45°$ cuando se use "ψ_1".

A grandes rasgos las fases de un protocolo de generación de claves son: generación y distribución de la clave, análisis y corrección de errores y amplificación de la privacidad. A continuación, se describe cada una de ellas para el *BB*84.

El Algoritmo BB84.

En la Criptografía Cuántica, los codificadores son quienes definen como se representa la información clásica mediante estados cuánticos. Una forma para codificar información clásica por medio de fotones polarizados, consiste en representar un '0' lógico como un fotón polarizado horizontalmente $|\leftrightarrow\rangle$, y un '1' lógico como un fotón polarizado verticalmente $|\updownarrow\rangle$. Este esquema de codificación por polarización lineal sería suficiente para poder transmitir datos entre el emisor y el receptor, pero no para ofrecer un canal de comunicaciones seguro. El hecho de codificar información en una sola base "rectilínea" hace que sea más fácil la detección de la información[13].

Este protocolo fue presentado por Bennet y Brassard en la "International Conference on Computers", en Bangalore, en el año 1984. Poalrizaremos fotones en la base + y elegiremos los ejes X e Y para polarizarlos. Podremos escribir entonces un vector polarización[8]

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

Donde se denotan los estados de base como $|\rightarrow\rangle$ y $|\uparrow\rangle$. No obstante la elección es totalmente arbitraria, y podríamos haber considerado la base $\times$, el mismo estado tiene su representación en esta base, mediante las ecuaciones de cambio de base.

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

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

Por convenio representaremos el bit 0 por el vector $|\rightarrow\rangle$ en la base $+$ y por $|\nearrow\rangle$ en la base $\times$.

El proceso entonces consiste en comparación de bases, empleadas al emitir y al medir. En los procesos en que han compartido base, tanto emisor como receptor tienen el mismo bit, en los que no ha habido coincidencia los bits serán aleatorios. Si consiguen eliminar esos bits aleatorios, tendrán una clave de un sólo uso. ¿Cómo pueden eliminar esos bits erróneos? Pues basta en que emisor y receptor hagan públicas las secuencias de bases empleadas para prepara y medir los estados. Comparando las dos listas, ambos sabrán que resultados deben desechar[4][16].

La pregunta obvia es, ¿No es esto peligroso? No mientras el emisor no diga que bits han codificado ni que el receptor muestre que resultado ha obtenido[15][2].

Alicia, Bob y alguien más.

El protocolo BB84 es uno de los esquemas más sencillos de generación y distribución cuántica de claves y se puede describir del siguiente modo:

Alicia y Bob intentan mantener en secreto una clave de criptografía cuántica. Para ello, la transmiten en forma de fotones polarizados, procedimiento ideado por Charles Bennett, de IBM y Gilles Brassard, de la Universidad de Montreal, durante los años ochenta y ahora materializado en algunos incipientes productos comerciales[10][18].

1. Para crear una clave, Alicia envía un fotón a través de la rendija 0 o de 1 de unos filtros polarizantes rectos o diagonales; mientras, anota las distintas orientaciones.

2. Para que cada bit que llega, Bob elige aleatoriamente qué filtro utiliza para la detección y anota tanto la polarización como el valor del bit.

3. Eva quiere espiar el tren de fotones, pero la Mecánica Cuántica le prohíbe usar a la vez ambos filtros para detectar la orientación de cada fotón. Se elige el filtro incorrecto, modificará su polarización y creara errores.

4. Una vez que todos los fotones han llegado a Bob, éste le dice a Alicia, por un canal público, quizá por el teléfono o con un correo electrónico, la secuencia de modos de medición que utilizó para los fotones entrantes, pero no el valor del bit de los fotones.

5. Alicia le dice a Bob, durante la misma conversación, en que casos eligió correctamente. Los correspondientes bits formarán la clave que Alicia y Bob utilizarán para cifrar mensajes.

Al contrarío que la criptografía de clave pública, la criptografía cuántica seguiría siendo segura, aunque existieran computadoras cuánticas[4][3].

Una forma de enviar una clave criptográfica cuántica entre el remitente y el receptor consiste en que el láser transmita fotones, cada uno polarizado de una de dos maneras. En la primera, la polarización es vertical u horizontal lo denominaremos "modo recto"; en la segunda, se orienta 45 grados hacia la izquierda o derecha de la vertical "modo diagonal". En cualquiera de los modos, las polarizaciones opuestas de los fotones representan un 0 o un 1 digitales[2][11][19].

El remitente, a quien los criptógrafos acostumbran llamar Alicia, envía una cadena de bits; para cada fotón, que codificará uno de esos bits, elegirá aleatoriamente si lo envía en el modo recto o en el diagonal. El receptor, al que se llama Bob, decide al azar qué les medirá a los bits entrantes, si el modo recto o el diagonal. El principio de incertidumbre de Heisenberg dicta que podrá medir los bits nada más que un modo. Bob sólo obtendrá con toda certeza el valor correcto cuando mida un bit del mismo modo en que lo envió Alicia[8][6].

Después de la transmisión, Bob se comunica con Alicia, intercambio que no tiene ya por qué ser secreto, para decirle cuál de los dos modos le midió a cada fotón. Sin embargo, no revela el valor, 0 ó 1, que obtuvo en cada caso[7][19]. Alicia le dice entonces a Bob cuáles se midieron en el modo que correspondía; ambos descartan los demás. Los modos medidos correctamente constituyen la clave que introducirá en el algoritmo empleado para encriptar o descifrar el mensaje.

Si alguien llamémosle Eva (espía), intenta interceptar esta serie de fotones, no podrá medir ambos modos, gracias a Heisenberg. Si Eva mide en el modo incorrecto, aunque reenvíe los bits a Bob en el mismo modo en que los midió, introducirá errores. Alicia y Bob pueden detectar la presencia de la espía comparando bits seleccionados y comprobando si hay errores[9][14].

En la actualidad y un futuro en desarrollo

El futuro desarrollo de la Criptografía Cuántica se enfocará en concreto en el incremento de seguridad en el intercambio de mensajes cifrados. Varios experimentos han sido propuestos para aumentar el intercambio de claves procurando proteger la integridad de los mensajes[3][8].

Actualmente, la BBN Technologies de los Estados Unidos está construyendo múltiples enlaces de distribución de claves cuánticas para consolidar lo que sería una red cuántica de distribución de claves. Así, si un enlace fallara, ya sea porque lo estén interceptando frecuentemente o porque este presentando niveles de ruido muy altos, se procedería a hacer uso de otro enlace de distribución de claves cuánticas en la red. La idea es que si algunos de los enlaces de la red

cuántica no están ocupados, estos se podrán utilizar no sólo para el envío de claves sino también para transportar mensajes de los usuarios ya encriptadas[19][14][8].

Desde el 2003 ya es posible encontrar equipos de distribución de claves cuánticas y generadores de números cuánticos aleatorios. Entre las marcas que se pueden encontrar en el mercado están: id Quantique, de Ginebra y MagiQ Technologies, de Nueva York, quienes han presentado productos comerciales que envían una clave de criptografía cuántica a más de los 30 cm recorridos en el experimento de Bennett. Tras exhibir una distancia de transmisión de 150 kilómetros la mayor conseguida hasta la fecha, se espera que NEC presente un producto en el mercado durante la siguiente década. IBM, Fujitsu y Toshiba trabajan en lo mismo[12][18].

Los productos ya comercializados pueden enviar claves por un enlace de fibra óptica a decenas de kilómetros. Un sistema de MagiQ cuesta de 70.000 a 100.000 dólares. El número de clientes es aún pequeño; el sistema no se ha implementado en ninguna red a gran escala[2].

Ciertos organismos gubernamentales e instituciones financieras temen que un mensaje cifrado espiado hoy se guarde hasta el día en que una computadora cuántica pueda descifrarlo. Entre los posibles clientes de los sistemas de criptografía cuántica se hallan también los abastecedores de servicios de telecomunicaciones que prevén ofrecer a sus clientes un servicio ultraseguro[15][17].

Están en Marcha los primeros intentos denotar con criptografía cuántica, no a conexiones punto a punto, sino a verdaderas redes. DARPA la Agencia de Proyectos de Investigación Avanzados para la Defensa de los Estados Unidos, el organismo estadounidense que patrocinó los inicios de lo que luego se llamaría Internet, ha financiado una conexión en red de seis nodos pertenecientes a la Universidad de Harvard, la Universidad de Boston y BBN Technologies, empresa de Cambridge, Massachussets, que también desempeñó un papel fundamental en aquellos orígenes de Internet. Las claves cifradas se envían por enlaces reservados, por Internet los mensajes cifrados con ellas. Es la primera red de criptografía cuántica que opera sin interrupción fuera de un laboratorio. Se ha creado sólo para demostrarla viabilidad del procedimiento; no transmite informaciones confidenciales[8][3].

El pasado otoño 2006, id Quantique, junto con Deckpoint, proveedor de servicios de Internet, exhibió una red que un grupo de servidores de Ginebra utilizó para almacenar sus a datos a 10 kilómetros de distancia. Un enlace con encriptación cuántica repartida se trata de una serie de operaciones para generar nuevas claves[2].

La actual criptografía cuántica está destinada a aplicarse a redes de alcance geográfico limitado. En su mayor virtud que al espiar un mensaje o clave encriptados cuánticamente se cambie sin remedio, está su peor defecto: los dispositivos que restauran en la red las señales debilitadas para que se las pueda transmitir hasta el repetidor siguiente, no podrían ejecutar esa tarea con las señales que codificaran las claves cuánticas. Un amplificador óptico corrompería los bits cuánticos, es decir los qubits[5].

Para que pueda haber una mayor distancia entre enlaces, se persigue que un medio diferente de la fibra óptica distribuya las claves cuánticas. Se ha subido a montañas donde la altitud reduce al mínimo la turbulencia atmosférica para probar la viabilidad de enviar los fotones a través del aire. Un experimento, realizado en el año 2002 en el Laboratorio Nacional de los Alamos, estableció un enlace de 10 kilómetros de esta manera[9].

Otro ensayo, ese mismo año, de QinetiQ, en Farnborough, y la Universidad Ludwing Maximilian de Munich, cubrió 23 kilómetros entre dos cumbres de los Alpes meridionales. Optimizando esta técnica con mayores telescopios para la detección y mejores filtros y recubrimientos antirreflectantes, se podría construir un sistema capaz de transmitir y recibir señales a más de 1000 kilómetros; bastaría para llegar a los satélites situados en una órbita terrestre baja. Una red de satélites de ese tipo ofrecería una cobertura mundial[6][18].

Es posible intercambiar mensajes cifrados usando criptografía cuántica entre una estación terrestre y un satélite de baja órbita, la atmósfera en este caso jugaría el papel principal sobre todo en los primeros kilómetros, si la longitud de onda es la adecuada, correctamente seleccionada y si el clima es limpio el mensaje viajaría sin problema alguno. Por ejemplo el satélite se mueve con relación a la superficie terrestre y al pasar sobre una segunda estación localizada a miles de kilómetros de la primera, podría retransmitirse el mensaje. El satélite entonces, es directamente

considerado como una estación intermediaria y segura por sus características. Esta tecnología apenas es una propuesta experimental basada en el comportamiento de la fibra óptica. Algunos grupos de investigación de la NASA ya han realizado pruebas preliminares de esta propuesta en su mayoría, teórico-practicas, muchos del los científicos creen que es viable el intercambio de claves cuánticas mediante un satélite para cubrir extensas distancias entre distintos puntos[2][7][19].

La Agencia Espacial Europea ha empezado a proyectar un experimento que conectaría un satélite a tierra. En abril del año pasado 2006, La Unión Europea puso en marcha también planes para desarrollar la encriptación cuántica en redes de comunicaciones; la ha movido a ello, en parte, el deseo de prevenir el espionaje de "echelon", sistema que intercepta mensajes electrónicos para los servicios de inteligencia de los Estados Unidos, Gran Bretaña y otras naciones[1].

En última instancia, los criptógrafos desean algún tipo de repetidor cuántico, que vendría a ser una forma elemental de computador cuántico capaz de superar las limitaciones de la distancia. Funcionaría gracias a las que Albert Einstein llamo "spukhafte fernwirkungen" "fantasmagóricas acciones a distancia". Un equipo del Instituto de Física Experimental de Viena, dirigido por Antón Zeilinger, ha dado un primer paso hacia un repetidor así: en el número de "Nature del 19 de agosto del 2004 informaron de que habían tendido bajo el Danubio, por un conducto del alcantarillado, un cable de fibra óptica con un fotón "entrelazado" en cada extremo. La medida de polarización de uno de esos fotones establecía inmediatamente en el otro un estado de polarización correlacionado con el primero, justo en eso consiste el entrelazamiento[16][3][1].

Pese a que el entrelazamiento cuántico le pareciese fantasmagórico a Einstein, les valió a Zeilinger y su equipo para que la conexión por fibra óptica entre los dos fotones entrelazados "teletranportación" la información contenida en un tercer fotón al otro lado del Danubio, a 600 metros de distancia. Se podría extender el montaje mediante repetidores múltiples, hasta que los qubits de una clave se transmitiesen a través de continentes o de océanos. Pero ese cambio de escala requeriría la creación de componentes muy peculiares, memorias cuánticas, por ejemplo, que almacenen los qubits sin corromperlos antes de que se los reenviara al enlace siguiente. Falta mucho para siquiera acercarse a la fabricación de elementos de esa especie. Acerca de un

experimento un poco anterior, en que se comprobó que el entrelazamiento de fotones transmitidos por el aire se mantenía entre ambas orillas del Danubio, pero sin que se teletransportase a un estado, véase "Experimento en el Danubio", [de Gabriel Molida Terriza, Investigación y ciencia, agosto 2004].

Quizá se realizaría mejor una memoria cuántica con átomos que con fotones. Un experimento, publicado en el número del 22 de octubre de 2004 de Science, ha mostrado una manera de hacerlo. Basándose en una idea de Lu Ming Duan, Mikhail Lukin, Ignacio Cirac y Meter Zoller, dos investigadores del instituto de Tecnología de Georgia, Alex Kuzmich y Dzmitry Matsukevich, entrelazaron un par de nubes de átomos de rubido ultraenfriados para inscribirles un qubit, las nubes los almacenan mucho más tiempo que los fotones y transferirlo después a un fotón. Transportaron, información de la Materia a la Luz, y una memoria cuántica entregó un qubit. Esperan crear mediante ese procedimiento repetidores que transmitan qubits a largas distancias.

Existen varias propuestas teóricas para construir repetidores cuánticos buscando retransmitir qubits sin ser corrompidos. En un principio los repetidores podrían ser usados para extender el intercambio de mensajes a largas distancias. En la práctica los repetidores cuánticos no existen aún, ni en laboratorios, son meras ideas universitarias y de bastante investigación teórica. No obstante es interesante notar que un repetidor cuántico podría funcionar como una computadora cuántica básica dedicada exclusivamente al envío y recepción de datos. El desarrollo de computadoras cuánticas permitirá implementar criptografía cuántica a la información capaz de viajar alrededor del globo terráqueo mediante redes especiales.

Discusión.

Hoy en día, la Criptografía Cuántica ha recorrido un largo camino desde aquella precaria exhibición. Ya hay dos pequeñas empresas que venden sistemas criptográficos cuánticos; otros productos semejantes vienen en camino. Con este método de encriptación, la ciencia de la Información Cuántica, que combina la Mecánica Cuántica y la Teoría de la Información, llega al

mercado. El dispositivo supremo que podría darnos sería una computadora cuántica tan potente, que no hubiese otra protección contra su prodigiosa capacidad de descifrar mensajes que la criptografía cuántica.

La supuesta inviolabilidad de la criptografía cuántica se apoya sobre un conjunto de hipótesis que quizá no se cumplan en el mundo real. Según una de ellas, cada qubit está representado por un fotón y sólo uno. Para efectuar un encriptado cuántico, se disminuye la energía de un láser que funciona a impulsos hasta que sea poco probable que más de uno de cada diez impulsos contenga un fotón el resto son "oscuros"; por esa razón es el ritmo de transmisión de datos tan bajo. Pero sólo se trata de una probabilidad estadística. El pulso puede contener más de un fotón. Un espía podría, en teoría, robar los fotones adicionales y descifrar con ellos un mensaje. Un algoritmo de programación, una "amplificación de la intimidad" protege de esta posibilidad enmascarando los valores de los qubits.

Los criptógrafos quisieran contar con mejores detectores y fuentes de fotones. El Norteamericano Instituto Nacional de Pesos y Medidas (NIST) es una de muchas organizaciones que investigan en esa línea. Tienen interés en construir detectores que distingan entre la llegada simultánea de uno, dos o mas fotones. Allí también intentan paliar el problema de la lenta velocidad de transmisión mediante la generación de claves cuánticas a un ritmo de megabit por segundo, cien veces más deprisa que hasta ahora. Bastaría para distribuir las claves en aplicaciones de vídeo.

La criptografía cuántica, con todo, seguiría siendo vulnerablemente a cierto tipo de ataques. Un espía podría sabotear un detector que recibe los fotones haciendo que los qubits que le llegan pasasen a una fibra, donde se los interceptaría. Y contra la defección interna, contra la mera traición, no hay defensa cuántica que valga.

Capítulo IV

Una propuesta real, Resonancia Magnética Nuclear (NMR)

"I'm so happy because today I found my friends – they're in my head"

Kurt Cobain (1967-1994)

Computación Cuántica y la Resonancia Magnética Nuclear (NMR)

La Resonancia Magnética Nuclear proporciona las bases experimentales para investigar las implementaciones físicas del procesamiento cuántico de información y hacer posible la computación cuántica en el mundo real. Aquí se introducirán los elementos básicos para comprender las aplicaciones de la Resonancia Magnética Nuclear en el procesamiento cuántico de información y explicar sus éxitos actuales, sus limitaciones y su potencial[1][3].

La espectroscopia en la Resonancia Magnética Nuclear es muy conocida por la variedad de manipulaciones dinámicas sobre el comportamiento del spin en las partículas. Las ideas y las herramientas de la espectroscopia en la Resonancia Magnética Nuclear en estado líquido se han utilizado para experimentar con el procesamiento cuántico de información[2][6][11]. Este método nos ha llevado a entender una complejidad de casi 10 qubits, un número pequeño para el cómputo cuántico pero bastante grande para observar, mejorar y comprender la complejidad de un mundo cuántico[5].

Por ahora la Resonancia Magnética Nuclear en estado líquido es la única tecnología actual que ha llegado a alcanzar este número de qubits, pues mientras más incrementos en la complejidad del comportamiento de las partículas a estudiar, requerirán nuevos métodos de estudio[13][7].

¿Cómo podríamos convertir sistemas cuánticos en dispositivos útiles y prácticos para el procesamiento cuántico de información?

Actualmente no se conoce alguna implementación o método detallado, aunque la mayoría de los científicos continúan desarrollando e investigado métodos importantes tanto teórico como experimentalmente para resolver esta pregunta[3]. Por consecuencia tal dispositivo será parte fundamental para lograr una computadora cuántica, y aunque tales dispositivos están más allá del alcance experimental en nuestros días, he relacionado los dispositivos actuales que podrían ser capaces de realizar un procesamiento cuántico de información[4][5][7].

Los procesadores cuánticos destinaran las leyes de la mecánica cuántica para la computación, comunicación, y almacenamiento de información. La diferencia principal entre los procesadores cuánticos y los procesadores clásicos consiste en la habilidad para manipular el "quantum" mecánicamente observando el fenómeno de la superposición en estados cuánticos y utilizar los efectos resultantes. Para aprovechar el procesamiento cuántico de información se requiere de una mecánica cuántica controlable mediante dispositivos físicos[16][21].

La dificultad de construir los dispositivos convenientes requiere de un esfuerzo aun mayor pues la fragilidad extrema de un sistema de información cuántico comparada con sistemas clásicos hace las manipulaciones a gran escala mucho más difíciles. Además, son exactamente estos estados cuánticos lo que necesita ser implementado para lograr un procesamiento cuántico de información[9][10].

Para convertir un procesamiento cuántico de información en una tecnología útil es indispensable explorar e investigar nuevos territorios de la mecánica cuántica, proponiendo nuestra comprensión y control de estos sistemas[20].

Evaluar, comparar y medir el éxito de dispositivos cuánticos para el procesamiento cuántico de información requiere de una dirección certera en el largo camino hacia la construcción una computadora cuántica. Un procesador cuántico es un dispositivo físico que opera mediante leyes de la mecánica cuántica, es aquel cuya evolución puede manejarse adecuadamente, con ruido y el fenómeno de la "decoherencia" bajo control. Finalmente este control conducirá a sistemas escalables, aceptando una computación tolerante a fallos como el algoritmo de factorización de

Shor o simulaciones de la mecánica cuántica. Los procesadores cuánticos pueden ser comparados en base a su manejo, fiabilidad, escalabilidad y eficiencia[18][15].

La mayoría de las propuestas para crear dispositivos de procesamiento cuántico de información incluyen ideas para un control adecuado, la aplicación del conocimiento sólo puede ser realizado a través del descubrimiento teórico de una computación cuántica tolerante a fallos. Antes de este descubrimiento, se sugirió que los problemas computacionales interesantes nunca fuesen solucionados usando computadoras cuánticas, Sin embargo, sin métodos adecuados para un control de errores las computadoras cuánticas pierden todo su potencial. La computación cuántica tolerante a fallos se basó en la existencia de correctores de código de error cuántico[17][8].

El resultado principal es el teorema del umbral de exactitud que demuestra que los errores en el control pueden ser susceptibles. Una computación eficiente tan exacta como lo deseado proporcionada por la precisión de un dispositivo cuántico excede del umbral. Por consiguiente, errores en dispositivos reales no son un obstáculo fundamental en el procesamiento cuántico de información. El umbral de exactitud depende de los tipos de ruido que puede afectar a un dispositivo y las estimaciones máximas admisibles se encuentran entre un rango de 10^{-6} a 10^{-3} probabilidades de error. La fidelidad de control es quizá el estándar de comparación más útil de los procesadores cuánticos, siendo así directamente relacionados con la escalabilidad de dispositivos cuánticos[15][20].

La relación entre la teoría de información y la Resonancia Magnética Nuclear comienza con experimentos e investigaciones desde el nacimiento de la misma en 1946, cuando los jóvenes científicos E. M. Purcell y F. Bloch observaron por primera vez la variación del campo magnético y su influencia en el spin nuclear. Esto abrió un nuevo campo de investigación desarrollando varias aplicaciones importantes como: Imágenes por Resonancia Magnética (MRI) y la determinación de la estructura molecular; estas dinámicas son estudiadas a detalle en ambos estados: líquido y sólido[9].
Quizá, el más claro ejemplo de la relación para una teoría de información cuántica posible, es el "eco de spin" donde Hahn demostró que las interacciones No-homogéneas podrían ser redirigidas a la extensión de fase en la que los spins nucleares retienen información acerca del campo local.

Esta técnica en la Resonancia Magnética Nuclear permite crear una polarización local no-homogénea y posteriormente detectar su evolución[22][12]. El fenómeno de eco mágico fue utilizado en el estado sólido, siendo posible invertir el signo del Hamiltoniano dipolar a fin de que el sistema pueda ser devuelto a un estado anterior y así revertir una dinámica aparentemente difusiva, generando un eco de spin almacenando los efectos en una matriz de densidad[14].

La idea de usar el spin nuclear para el almacenamiento de información fue propuesta por: A. G. Anderson y E. L. Hahn en 1955. Recientemente, la Resonancia Magnética Nuclear se propone como una tecnología viable para el procesamiento cuántico de información[19][20].

Los experimentos hechos con la Resonancia Magnética Nuclear han dado como resultado la única forma conocida de crear la primera generación de dispositivos cuánticos basado en estado liquido, manipulando sistemas de hasta 7 qubits utilizando la tecnología comercial. El logro principal de este avance tecnológico ha sido convertir algoritmos cuánticos teóricos en experimentales[10][5][16].

La Resonancia Magnética Nuclear es una tecnología donde se puede probar las suposiciones de la teoría y dónde se aprende a resolver las imperfecciones o fallas de los dispositivos físicos actuales. Los experimentos también han inspirado a crear nuevas ideas e investigaciones teóricas para lograr un procesamiento cuántico de información[12][20][22][3].

Los experimentos de estado sólido en la Resonancia Magnética Nuclear son los precursores ideales para la manipulación controlada de un orden muy alto de coherencia cuántica. Por ejemplo, A. Pines y sus colegas J. Baum, M. Munowita, A. Garroway han demostrado que sistemas cuánticos de cientos de partículas de 1/2 de spin pueden ser controlados coherentemente. En el estado sólido la tasa de decoherencia puede reducirse promediando una coherencia directa logrando así el tiempo de la fase de coherencia en segundos. Como el tiempo para las operaciones cuánticas básicas es de un orden de $100\mu s$, la exactitud operacional está en el umbral cerca de lo necesario para lograr una escalabilidad tolerante a fallos[9][10].

Una de las conclusiones más importantes de espectroscopia en la Resonancia Magnética Nuclear y el procesamiento cuántico de información en las últimas cuatro décadas es que los sistemas nucleares de 1/2 de spin son sistemas cuánticos extremadamente robustos. Su coherencia puede ser manipulada con precisión y la decoherencia puede ser obtenida lentamente en el período de las interacciones del qubit[6][17].

Los esfuerzos en el presente para crear a un procesamiento cuántico se basa en el spin nuclear, con pasos firmes para:

- Desarrollar métodos bien fundamentados en estado líquido y sólido en la Resonancia Magnética Nuclear para un control coherente.

- Explorar el estado sólido en la Resonancia Magnética Nuclear, desarrollando métodos para lograr una alta polarización.

- Diseñar sistemas con la meta de incrementar la tasa de reloj y la complejidad de los sistemas cuánticos aplicados.

Uno de los obstáculos principales para la lograr el procesamiento cuántico de información consiste en el problema de la decoherencia, que causa la pérdida del caracter unitario y la reversibilidad del sistema en algoritmo cuántico aplicado.

Los tiempos de decoherencia para los sistemas propuestos, en particular el tiempo de fase en la Resonancia Magnética Nuclear y en las Imágenes por Resonancia Magnética se encuentra normalmente entre nanosegundos y segundos, a temperaturas bajas. Las tasas de error son comunmente proporcionales a la razón entre tiempo de operación y el tiempo de decoherencia, de forma que cualquier operación debe ser resuelta en un tiempo mucho más corto que el tiempo de decoherencia. Si la tasa de error es lo bastante baja, es posible usar eficazmente la corrección de errores cuánticos, con lo cual sí sería posible tiempos de cálculo más largos que el tiempo de decoherencia y, en principio, arbitrariamente largos. Se menciona con frecuencia una tasa de

error límite de 10^{-4}, por debajo de la cual se supone que sería posible la aplicación eficaz de la corrección de errores cuánticos[21][20][14][5].

Otro de los problemas principales es la escalabilidad, especialmente teniendo en cuenta el considerable incremento en qubits necesarios para cualquier cálculo que implica la corrección de errores. Para ninguno de los sistemas actualmente propuestos es trivial un diseño capaz de manejar un número lo bastante alto de qubits para resolver problemas computacionalmente interesantes hoy en día[7][18].

Estado Líquido

La Resonancia Magnética Nuclear proporciona un importante soporte experimental de ideas para lograr un procesamiento cuántico de información; Los análisis matemáticos como el método Hamiltoniano y sus operadores son bien conocidos además de fiables para controlar la dinámica del spin nuclear. Ninguna otra tecnología ha conseguido la capacidad de controlar un número accesible de qubits, en la actualidad se ha logrado manipular hasta siete de ellos exitosamente. Además, hay cuarenta años de experiencia utilizando la Resonancia Magnética Nuclear para explorar las dinámicas, reacciones y estructuras químicas de estas partículas[6][19]. Tal experiencia ha llevado a la construcción de máquinas e instrumentos a gran escala capaces de realizar experimentos más complejos y a una riqueza de métodos prácticos para comprender la dinámica, estructura y comportamiento del spin[7][10].

Aunque las metas de los experimentos de la Resonancia Magnética Nuclear estándar y el procesamiento de información cuántica son bastante diferentes, los requisitos de la instrumentación son muy similares y el mismo dispositivo puede usarse para ambos propósitos. La espectroscopia de la Resonancia Magnética Nuclear en estado líquido consiste en estudiar la química y dinámica de una solución que contiene las moléculas conocidas o desconocidas mediante una serie de experimentos bien definidos para sacar componentes específicos de las ecuaciones hamiltonianas, en un estado de cierta relajación es fácil interpretar valores numéricos como la moda. En la Resonancia Magnética Nuclear y especialmente en el procesamiento

cuántico de información, la meta es caracterizar la transformación total y eficaz de una serie compleja de operaciones. Finalmente la meta es aplicar una serie de transformaciones suficientemente complejas para estar más allá de la capacidad de una computadora clásica[8][11][16].

Logros de estado líquido

Una razón del por qué la Resonancia Magnética Nuclear y el procesamiento cuántico de información han tenido tal ventaja por encima de otros dispositivos, es definitivamente el uso de la espectroscopia y se ha utilizado para realizar las manipulaciones coherentes durante ya mas de 2 décadas. De hecho, mucho del trabajo de la investigación en la Resonancia Magnética Nuclear se dirige hacia el control coherente de los estados cuánticos para extraer la información química de los sistemas más complejos. Esto ha llevado a la comunidad de científicos dedicados a esta área a desarrollar las herramientas analíticas más poderosas para una mejor comprensión del spin de las partículas[4][22].

En el límite de acoplamiento débil dónde se llevan a cabo los qubits en la espectroscopia, fácilmente por lo que se refiere al spin nuclear, es el formalismo de los operadores matemáticos del producto que proporciona una descripción completa de la dinámica del qubit. No sólo es experimentalmente, si no que, esto es sumamente útil, así como también describe las dinámicas que se desean en una computadora cuántica. Claro que para la espectroscopia de la Resonancia Magnética Nuclear el enfoque está en las operaciones únicas del spin y para el procesamiento cuántico de información, está en las operaciones del qubit y el comportamiento de las compuertas cuánticas[3][14][22]. En el caso de sistemas de spin más complejos, las dinámicas son a menudo complementadas con un spin ficticio, qué es esencialmente una asignación del sistema físico en el que los qubits se comportan de la manera sugerida para la simulación cuántica deseada. Más allá de una cierta complejidad está extremadamente difícil asignar una dinámica en el que los qubits son confusos y el enfoque empieza a discutir las propiedades termodinámicas del sistema del spin mediante los conceptos de temperatura. Un desafío mayor en el procesamiento cuántico de

información, es usar estos sistemas para lograr un fiable procesamiento computacional físicamente controlable.

Hemos visto en capítulos anteriores, ejemplos de la estructura matemática, en especial el de las ecuaciones hamiltonianas que se relaciona a la simulación cuántica y es sumamente útil para seleccionar aplicaciones específicas de posibles compuertas cuánticas. Aunque el espacio experimental es limitado no ha permitido establecer una discusión detallada sobre que estructuras matemáticas puedan llegarse a establecer[18][11][17]. En general, la computación cuántica es comprendida a través de bases meramente teóricas donde sistemas muy complejos se combinan simplemente con las ideas sobre el procesamiento cuántico de información. Interesantemente los conceptos como el de corrección del error cuántico no parecen haber sido previstos, ni si quiera en un sentido primitivo. Éste es quizá un ejemplo de dónde sólo pueden tocarse ideas complejas a través de un acercamiento de la teoría de información formal tal cual la conocemos hasta ahora[15][19].

Las mismas características que hacen posible el procesamiento cuántico de información para saber la capacidad de controlar la dinámica del spin se usan en muchas de las técnicas experimentales que se han hecho en las aplicaciones de la Resonancia Magnética Nuclear. Hay métodos muy robustos para crear los pulsos selectivos y éstos han tocado con una precisión muy alta los propósitos exclusivos de las imágenes por resonancia magnética. Hoy en día cada experimento realizado en la Resonancia Magnética Nuclear se distingue por el siguiente formulario, de la manera física más coherente posible:

- Para transferir la polarización y para la mejora de sensibilidad
- Transferir la coherencia para la correlación experimental.
- Suprimir la coherencia selectivamente para la eliminación de la señal solvente y limitar el rango dinámico de la señal.
- Para seleccionar las sendas cuánticas múltiples para observar los subsistemas específicos producidos por el spin.
- Para eliminar los spin no deseados.
- Para analizar el spin cuyas diferencias del desplazamiento químicas son mayores

que el acoplamiento entre ellos.

- Para borrar el efecto dipolar selectivamente o el quadrupolar al igual que las interacciones.

La mayoría de estos métodos han encontrado las aplicaciones y la precisión del control requerido por el procesamiento cuántico de información, que implica que tendremos que hacer uso de todos los posibles recursos de que se disponen en la actualidad para lograr el mejor control coherente.

La espectroscopia de la Resonancia Magnética Nuclear no se ha centrado exclusivamente en los procesos químicos y en las aplicaciones médicas, también se ha usado como una forma de comprender la dinámica del comportamiento cuántico. Este campo de estudio se ha esforzado con la incertidumbre de los límites que puede alcanzarse en la eficacia de las transformaciones, así como también de la transferencia de la polarización y en encontrar los recursos necesarios para lograr esto experimentalmente[12][9][20]. Las investigaciones en el procesamiento cuántico de información incluyen la medida interferométrica de las dinámicas del spin, es decir, la creación de estados pseudo-puros lógicamente reconocidos y el entendimiento de su fase geométrica. Se sabe también que existen aplicaciones en la Resonancia Magnética Nuclear para controlar la fase geométrica, exactamente de como se comportaría una compuerta cuántica.

Han realizado también una serie de investigaciones de la complejidad cuántica para los sistemas dipolares acoplando el spin dirigido en ambos cristales, líquido y sólido, son los resultados obtenidos en la experimentación de la Resonancia Magnética Nuclear los que hicieron posible acoplar bipolarmente el spin y que provee un soporte de prueba a la complejidad cuántica, además bajo estos resultados se puede ir pensando en la próxima generación de dispositivos de procesamiento cuántico de información[2][13][10]. El estado sólido también ofrece un soporte de prueba ideal para los estudios más grandes de la dinámica del spin y de la transición del comportamiento clásico al cuántico, para lograr una mejor adaptación dentro de los laboratorios.

Claramente sin el conocimiento acumulado y en constante avance en los métodos producidos por la espectroscopia e instrumentación en el campo de la Resonancia Magnética Nuclear no habría tanto adelanto como hasta el día de hoy. Hay descripciones excelentes y extremadamente

detalladas en el tema de la informática cuántica, afortunadamente sólo tratare de resumir a grandes rasgos algunos aspectos que pueden hacer posible una computadora cuántica. La tabla siguiente resume los experimentos realizados y publicados por científicos de renombre.

N° de qubits	**Algoritmos**	**Año**
2	Gates	1996
	Database Search	1998
	Deutsch-Josza	1998
	Quantum Simulation	1999
	Quantum Detecting Code	1999
	Quantum Fourir Transform	1998
	Dense Coding	1998
	Quantum Detecting Code	1999
3	GHZ State	1997
	Quantum Error Correction	1997
	Quantum Teleportation	1997
	Deutsch-Joza	1998
	Quantum Simulation	1999
	Quantum Fourier Transform	1998
	Quantum Eraser	1999
4	C-Not Gate	1999
5	Deutsch-Josza	1999
6	Decoupling	1998
7	Benchmark	1999

Limitaciones de estado líquido

La Resonancia Magnética Nuclear en estado líquido es sumamente útil para demostrar un control coherente y fiable de lo que es el comienzo de la computación cuántica, es decir hablando de llevar la teoría directamente al laboratorio y mientras tanto se tiene las siguientes limitaciones:

1) La preparación no-escalable de un estado pseudo-puro. Como el número de incremento en los qubits, en otras palabras es la señal que resulta de la preparación del estado pseudo-puro esta señal se disminuye exponencialmente, este decaimiento hace ineficaz una posible corrección del error cuántico[9][17].

2) La proporción del tiempo tan corto en la decoherencia. Esto es suficiente para que los experimentos puedan llevarse a cabo y computacionalmente que los algoritmos funcionen correctamente[6].

3) La dificultad de restablecer los qubits. Para integrar la corrección del error cuántico, los qubits deben proporcionar una estabilidad adecuada, esto se establece mediante una fina polarización desde el inicio al final de las pruebas la Resonancia Magnética en estado líquido no parece proveer un mecanismo para restablecer los qubits a voluntad propia[8].

La primera generación del procesamiento cuántico de información se basó en el estado líquido de la Resonancia Magnética Nuclear y ha sido muy útil como un primer paso en el paradigma de la computación cuántica[15].

Estado Sólido

Las Resonancia Magnética Nuclear en estado sólido tiene cuatro ventajas principales que pueden ser aprovechadas en el procesamiento cuántico de información. El primero, consiste en que el sistema puede ser aumentando y muy polarizado, mientras la sensibilidad nos permita tener lo necesario para leer los resultados que involucren muchos qubits[13][22]. El segundo, respecto al tiempo de la decoherencia ya que pueden hacerse más lentos. El tercero, los acoplamientos entre el spin son más altos, mientras se va permitiendo que las operaciones sean más rápidas y más exactas y que puedan llevarse a cabo algoritmos de una complejidad mucho mayor. Hay mecanismos que pueden usarse para restablecer los qubits dinámicamente y finalmente obtener una precisa corrección del error cuántico eficazmente[10][16].

Desde el un punto de vista de la espectroscopia las diferencias principales entre el estado líquido y sólido en la Resonancia Magnética Nuclear son los siguientes:

1) Los acoplamientos del efecto dipolar están resueltos.

2) La difusión del spin contribuye significativamente a las dinámicas propuestas.

3) El desplazamiento químico necesita ser descrito por un tensor.

4) Los tiempos de relajación del spin normalmente son en muy poco tiempo.

5) El tiempo de la decoherencia transversal (fase) es dominado por interacciones del spin-spin que pueden ser reenfocadas por propósito especial de un láser pulsando las sucesiones de qubits.

6) Se conocen los métodos por crear y controlar la polarización de la luz.

El futuro de la Resonancia Magnética Nuclear

El primer gran adelanto para la comunidad científica en las posibles ideas de construir computadoras cuánticas llego a mediados de los años 90, cuando descubrieron como realizar cálculos usando la técnica de la Resonancia Magnética Nuclear. La idea clave fue que una sola partícula puede actuar como una diminuta computadora. La información es almacenada en la orientación en que los spin son manipulados[7][20][5]. La interacción entre el spin fue entonces conocida como "spin - spin coupling" y sirve para controlar las operaciones lógicas básicas. En un campo magnético tan fuerte, estos qubits son puestos a girar alrededor de la dirección del campo magnético en las frecuencias de las que dependieron en su medio ambiente químico.

Las ideas más extrañas pueden venir de los lugares más ordinarios. Una idea en la construcción de computadoras cuánticas viene de Texas. En el año de 1981, cuando John A. Wheeler, el padre

de los agujeros negros y físico teórico de la Universidad de Texas en Austin, organizó una fiesta donde la mayoría de los invitados eran estudiantes jóvenes de física de esa universidad, con el interés común en los fundamentos de la computación, un tópico que Wheeler creía que comenzaría a aumentar en las siguientes décadas[13][17].

Fue en esa fiesta en una conversación con Charles Bennett, un físico de la IBM, donde se produjo una idea en la mente del investigador de la Universidad de Oxford David Deutsch pues le llamó la atención que la teoría de la computación estuviera basada en las leyes de Newton, no en la teoría más fundamental de la descripción del universo proporcionada por el quantum[19].

Con el tiempo, la industria de las computadoras fue empezando a preocuparse sobre el futuro de la microelectrónica cada día más y más pequeña además de que, ¿Cuantos cálculos por segundo sería finalmente posible realizar y cuanto calor produciría esto directamente en los circuitos integrados y podría el silicon sobrevivir al constante e intenso calor?. Para ayudarlos, los científicos expertos en las computadoras pensaron y recordaron la teoría desarrollada en los años 30 por el pionero de la computación, Alan Turing. Pero en la fiesta de Wheeler, dijo Deutsch, "Yo podría ver inmediatamente que usando las leyes de la Mecánica Cuántica podría dar una respuesta diferente".[22][10]

Deustch tomo el lápiz, el papel y empezó el mejor trabajo de su vida, escribiendo en un documento que hasta ahora generalmente es considerado como un artículo principal para la introducción del cómputo cuántico. Publicado en 1985, que describe como una computadora podría funcionar usando las extrañas reglas de la Mecánica Cuántica y porque tal computadora se distingue fundamentalmente de las computadoras clásicas. Quince años después, la revolución que Deustch comenzó, ha alcanzado proporciones globales. Las computadoras cuánticas no son vistas como extrañas curiosidades en el ambiente científico, pero si como el poderoso futuro de la industria de las computadoras, y el debate esta moviéndose desde preguntas como: ¿Estas computadoras serán alguna vez una realidad, y cuando lo serán?. La sorpresa no es debido a su poder, aunque indudablemente serán, por mucho, más poderosas que las computadoras actuales. Su gran ventaja por lo menos teórica que se tiene, es que pueden resolver problemas y llevar a cabo simulaciones que son básicamente imposibles en las computadoras convencionales[13].

Tal es el atractivo de esta clase de dispositivos que hay una lista de compañías financiando y patrocinando varios programas de investigación por todo el mundo algunas compañías que conforman la lista son: Microsoft, IBM, Lucent Technologies, Hewlett-Packard y AT&T y algunas empresas como, MagiQ Technologies actualmente ya vende y da soporte a dispositivos usados en la criptografía cuántica y se espera desarrollar más propiedades en este campo[5][17].

Uno de los más recientes problemas que ha sido un obstáculo en el desarrollo de las computadoras cuánticas es el temor a que con su poder podría romper con extrema facilidad los códigos mayormente secretos y que son impenetrables para otras computadoras. Las alarmas empezaron a sonar cuando en 1994, Peter Shor, un distraído físico de los Laboratorios Bell demostró que las computadoras cuánticas eran extraordinariamente más rápidas efectuando operaciones como la factorización de números grandes, encontrar los factores de grandes números es tan difícil para las computadoras convencionales que los programadores usan estas debilidades para proteger datos sensibles. Con el desarrollo de las computadoras cuánticas, estos códigos serán sencillamente obsoletos[13][4][2].

La Resonancia Magnética Nuclear se propone como la solución soñada por todo investigador para llevar a cabo la construcción de una poderosísima computadora, solamente vista en películas de acción. Los núcleos están naturalmente aislados del ruido del mundo exterior y por lo tanto pueden mantener una coherencia estable por muchos segundos y estoy representa suficiente tiempo para ejecutar cientos de operaciones lógicas extremadamente rápido. Además, la Resonancia Magnética Nuclear es una tecnología madura, habiendo sido usada desde hace ya casi 50 años para el análisis de imágenes y químicos.

Tan pronto como la primera computadora cuántica sea exitosamente encendida, los gobiernos y sus militares serán forzados a admitir que muchos, si no es que todos, sus códigos son inseguros. Comprensiblemente, toda la industria de la tecnología esta ansiosa por descubrir todo lo que una computadora cuántica podría realizar, varios laboratorios y universidades en todo el mundo han empezado programas de investigación y en particular institutos como el: Instituto Nacional de Estándares y Tecnología NIST, el Instituto Nacional Los Alamos EUA, son de las entidades de investigación que mas promueven el estudio del quantum aplicado a la computación cuántica.

En la carrera hacia el desarrollo constante en la velocidad de las computadoras, la gigantesca industria de los microprocesadores se estrella contra impedimentos Físicos, propios de los materiales utilizados. Por eso los científicos están abocados a buscar nuevas maneras de computar que permitan aumentar la capacidad de procesamiento hasta límites que parecían imposibles e inimaginables. Tareas consideradas sin solución en tiempos razonables podrían ser resueltas en un par de milésimas de segundo si los científicos logran desarrollar las computadoras cuánticas.

La falta de velocidad para el procesamiento de datos no es un problema nuevo. Para solucionarlo se intenta, desde mediados de los años 60, diseñar arquitecturas de hardware, modelos que indican cómo interconectar componentes y microcircuitos en el CPU, periféricos etc., compuestas por procesadores en paralelos es decir, que ejecutan instrucciones de forma independiente y que analizan datos de forma simultánea, sería como poner a todos los "superhéroes" a trabajar al mismo tiempo, sobre el mismo tema. Sin embargo, hoy en día dichas computadoras paralelas son muy costosas y tienen usos extremadamente específicos, procesamiento de imágenes, cálculos científicos, sistemas de control, genética, medicina nuclear, biomédicas, computo simbólico etc. Como en muchos otros casos, los neurólogos creen que gran parte del poder expresivo del cerebro humano se debe al procesamiento simultáneo que permite la evaluación de miles de combinaciones o posibles soluciones al mismo tiempo y que permite resultados nuevos e imprevisibles.

Frente a este cúmulo de dificultades los especialistas están buscando múltiples salidas. Una de ellas surge de la Física Cuántica. Esta teoría que explica el curioso comportamiento de las partículas a nivel subatómico no parece coincidir con lo que el sentido común dice acerca del mundo cotidiano en el cual estamos involucrados. La Física Cuántica predice fenómenos que sólo pueden explicarse diciendo cosas como, "una partícula es capaz de estar en dos lugares al mismo tiempo".

En los años 80's tres Físicos llamados Feynman, Benioff y Deutsch fueron aún más lejos y concibieron una máquina que aprovechara los fenómenos cuánticos para aumentar la capacidad de procesamiento de una computadora. Si una partícula puede estar en dos estados al mismo

tiempo, se le puede utilizar para codificar, a su vez, dos datos al mismo tiempo; en caso de una computadora binaria, en 0 y 1. Si un qubit puede estar en dos estados al mismo tiempo, dos pueden representar cuatro estados al mismo tiempo (00, 01, 11, 10), tres qubits pueden representar 8 y así sucesivamente.

A pesar de lo interesante de la teoría, la curiosidad científica no dejaba de ser una construcción útil sólo para amenizar las charlas de café entre jóvenes científicos. Es que no se le encontraba ninguna utilidad práctica.

Pero a mediados de los años 90's un científico de la Bell Labs, Peter Shor, demostró que las Computadoras Cuánticas podrían ser utilizadas de manera eficiente para resolver un problema de gran interés práctico: factorizar números enteros, una de las necesidades básicas de las empresas de seguridad informática que utilizan estos complejos cálculos matemáticos para crear claves de seguridad. Apareció una utilidad práctica y detrás de ella los que podían llegar a obtener un beneficio, la poderosa industria de la seguridad informática abrió los ojos y las carteras, y el dinero comenzó a llegar a los laboratorios que se dedicaron a estudiarlas.

El funcionamiento de una Computadora Cuántica, como de la Física Cuántica, tiene sus bemoles, y esos bemoles exigen el no poco complejo proceso de quitarse de encima el sentido común. La idea básica es utilizar los estados cuánticos de algún objeto para representar la información. En las computadoras comunes también la información se representa en estados físicos de ciertos materiales que se codifican como 1 ó 0 y para manipularla se usan circuitos que dejan pasar electricidad o no. Pero nuestras actuales computadoras almacenan la información utilizando un enorme número de partículas, casi cien mil millones de átomos son modificados para escribir un 0 o un 1 en un disco magnético ordinario. En cambio, al usar un único átomo por cada bit, las Computadoras Cuánticas tendrán otra ventaja enorme frente a las computadoras clásicas. Así, en las Computadoras Cuánticas se conjuga la posibilidad de ocupar poco espacio y aprovechar las características de los qubit de representar dos estados al mismo tiempo.

La Computadora Cuántica local funciona en el interior de un gran espectrómetro de Resonancia Magnética Nuclear (RMN) que consta de un imán superconductor muy poderoso, enfriado dentro

de un tanque de helio y nitrógeno líquidos. En su interior se encuentra el verdadero "cerebro informático", un tubito con un compuesto químico que es manipulado para codificar ceros y unos y hacerlos actuar para procesar información. En una Computadora Cuántica es necesario controlar el estado cuántico de la computadora a nivel de obligar a cada bit a ser 0, 1 o cualquier otra cosa intermedia que uno quiera. Pero es difícil decir "quiero cambiar un átomo de lugar, sentido o forma" e incluso hacer algo que afecte a un único átomo. Lograr que los átomos se queden quietos y fríos es el Premio Nobel de hace algunos años.

Así planteadas las cosas, las Computadoras Cuánticas generan problemas prácticos sobre los que se avanza muy lentamente. Cualquiera que haya intentado armar alguno de los regalitos que vienen en los huevos de chocolate, sabe que manipular las cosas pequeñas no es tarea fácil. Mucho menos si se trata de átomos. Sin embargo, los pacientes obreros de la Física no se rinden. La cosa es así: la información se codifica en una de las características de los átomos "el spin" que se comporta de esa manera particular que le permite estar en dos estados al mismo tiempo. Para codificarlos utilizamos un aparato de resonancia magnética (RMN) que tiene un imán gigante. Introduciendo pulsos de radio frecuencia puedo hacer que los 0 se vuelvan 1 u otra opción, para cada uno de los tres átomos de nuestra computadora cuántica. De ninguna manera se piensa en escribir un programa en algún lenguaje de programación, lo que hace es que tener que manipular directamente el qubit número 1 de tal manera, sobre el 2, o de tal otra para que se genere un encadenamiento lógico que me dé el resultado que busco, explica Paz con paciencia.

Cómo manipular una sola molécula es algo muy complejo y difícil de medir, incluso en las supercomputadoras más exactas, se utilizan muchas moléculas a las que se hace interactuar en conjunto para que las señales magnéticas sean lo más fuerte posible. "Estas moléculas son manipuladas y todas ellas actúan de tal manera que les indico. Luego se observa que los qubits interactúan entre sí". En esta interacción se pueden crear funciones lógicas que son las que le dan la verdadera utilidad a la información acumulada en los qubits. Modificando los primeros eslabones de la cadena manipulada y sobre el último que arroja el resultado. Cuando termina el procesamiento se mide la magnetización, es decir, se obtienen resultados finales.

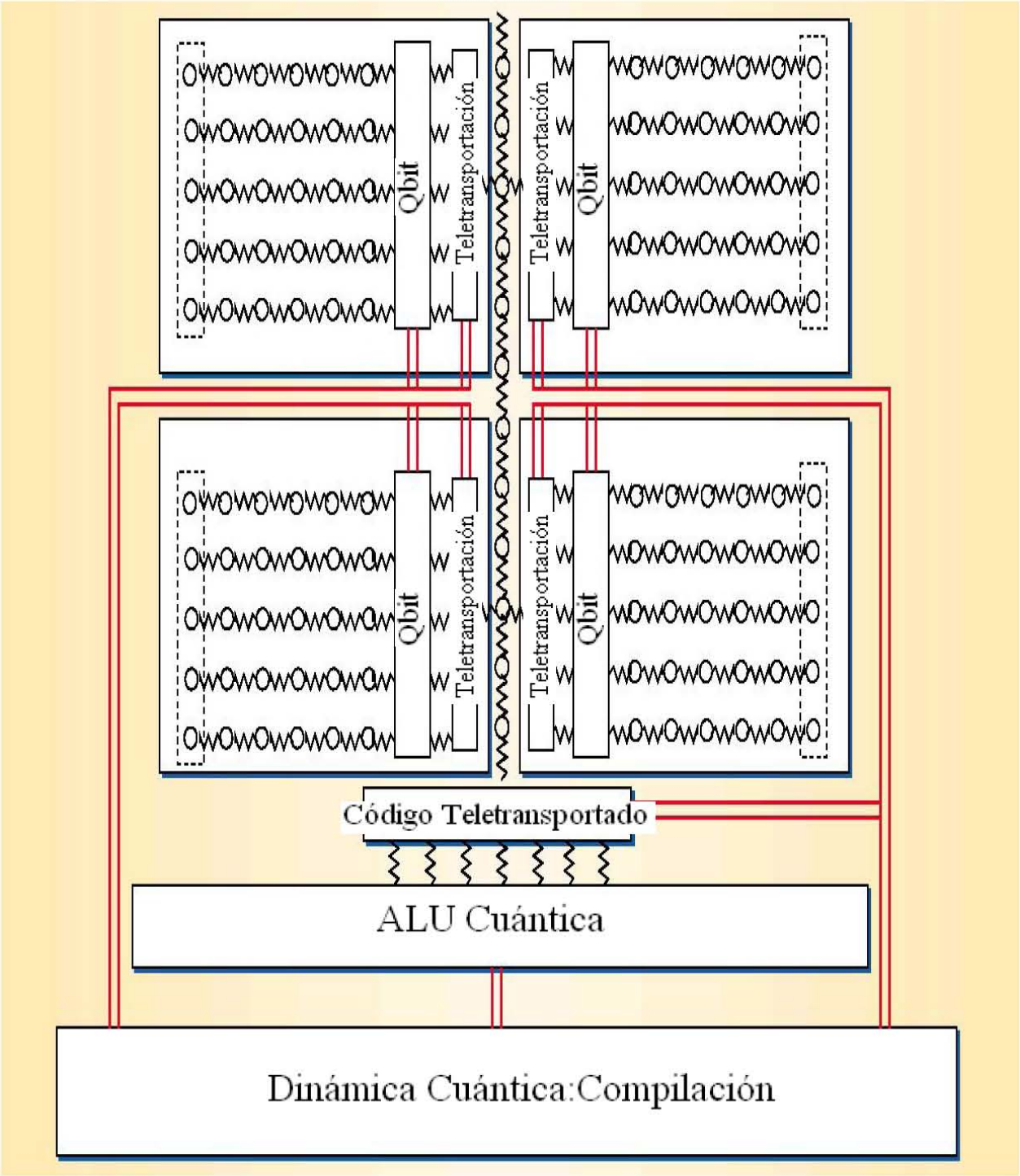
Así funciona el corazón de esta Computadora Cuántica. ¿Pero dónde está el programa que le indica qué hacer? "En este sentido la Computadora Cuántica es bastante similar a las comunes. Se crea un programa en una computadora que indica cómo debe ser la posición inicial de los átomos para procesar la información que se desea obtener, se provoca esa posición inicial mediante pulsos de radiofrecuencia y filtros especiales, se deja que el espacio cuántico de procesamiento elabore un resultado. Podríamos decir que un aparato de Resonancia Magnética Nuclear (RMN) es una interfaz que me permite comprender lo que sucede en el interior de la máquina, de la misma manera que un monitor me permite entender lo que en el interior de una PC está codificado como unos y ceros."

Hasta ahora, lo que se logró es que una computadora de dos bits encuentre, en un intento, un dato escondido entre otros tres falsos: con dos átomos se cubren las cuatro posiciones al mismo tiempo. En realidad, "la potencialidad real de la Computación Cuántica no se conoce" y además "No se sabe qué es lo que se puede hacer con una Computadora Cuántica." Lo cierto es que, si una parte de lo que prometen llega a cumplirse, pueden llegar a redefinir lo que se entiende por calcular. De la misma manera que hace un siglo debía parecer imposible utilizar información acumulada en forma de 0 y 1 electrónicos, en la actualidad el futuro de la Computación Cuántica es todavía incierto, pero posible. Es más, se podría decir que el futuro mismo es cuántico, ya que en este momento todas las posibilidades son reales. Cuando una de ellas se concrete, de acuerdo con la limitada lógica cotidiana, va a haber tenido que elegir inclusive, si las Computadoras Cuánticas sirvieron para algo o no.

Discusión

Aplicando las manipulaciones más fiables en la informática cuántica, la Resonancia Magnética Nuclear ofrece un soporte muy útil para el desarrollo del procesamiento cuántico de información. Los elementos esenciales para la informática cuántica se han demostrado, no sólo teóricamente, sino también experimentalmente, es decir, ya es una realidad. Se han desarrollado técnicas muy avanzadas y completas en la Resonancia Magnética Nuclear, en especial por la comunidad de científicos dedicados a la espectroscopia para tratar con la mayor gama de errores coherentes

solucionables, aún cuando la tecnología para desarrollar una computación cuántica no pueda parecerse a lo que podemos imaginar hoy, el conjunto de técnicas que se han desarrollado se necesitan para el perfeccionamiento de esta nueva tecnología.



Arquitectura: KRONOS Oswaldo Camargo Vidals 2007 UNAM, F.I

Otra contribución importante de la Resonancia Magnética Nuclear ha sido cuestionar algunas explicaciones ingenuas del poder tan sorprendente de una computación cuántica como la necesidad por los estados puros y enredos sobre los qubits. Como resultado, se ha comprendido que el procesamiento cuántico de información es el tema esencial de la informática cuántica y el poder computacional relativo de dispositivos que no encajan en el modelo estándar está empezando a ser explorado en distintas partes del mundo.

A pesar de las limitaciones en estado líquido de la Resonancia Magnética Nuclear, es probable controlar 10 qubits, un éxito enorme por ser de las primeras tecnologías para la manipulación del quantum. Muchas de estas limitaciones serán superadas por una segunda generación de la Resonancia Magnética Nuclear basado en dispositivos que tienen el potencial necesario para exceder del predecible reino clásico. La propuesta de un estado sólido en la Resonancia Magnética Nuclear inició directamente con una polarización muy alta, así como también, permito un mejor entendimiento de la corrección del error cuántico. El uso y desarrollo de la Resonancia Magnética Nuclear es una esperanza tecnológica que permitirá comprender las investigaciones en la simulación cuántica y en la decoherencia. Cuando el procesamiento cuántico de información tiene un aumento en los qubits, incrementa la complejidad de simularlos usando las computadoras clásicas y es casi imposible tratar de hacer cálculos e investigaciones de unos 30 ó 40 qubits al mismo tiempo. Esto debe considerarse como una oportunidad para investigar un nuevo territorio inaccesible a las simulaciones clásicas. Por otro lado, el número de qubits disponible en el estado sólido en la Resonancia Magnética Nuclear es todavía pequeño comparado a lo que se necesita para llevar a cabo los cálculos algorítmicos más elementales que se tienen a hasta el día de hoy. Se tiene que desarrollar métodos Físicos y Matemáticos para investigar los espacios de Hilbert extremadamente grandes y que se puedan controlar, el trabajo de la Resonancia Magnética Nuclear contribuye en todo aspecto a este tipo de desarrollos.

Los recientes descubrimientos en la Mecánica Cuántica permiten manipulaciones más poderosas de la información que en su contraparte clásica, cuando se habla sobre una posible computadora cuántica se tiene el potencial meramente para revolucionar el procesamiento de información a niveles nunca antes imaginados. En principio, la estructura matemática de muchos artículos y libros sobre el tema muestran diversos teoremas del umbral de exactitud, pero…, las limitaciones

de sistemas cuánticos son en gran parte debido al ruido y decoherencia, hablando ya en términos tecnológicos éstos pueden superarse siempre en base al desarrollo científico, esto no significa que el camino del procesamiento cuántico de información conceptualmente pensando en la "escalabilidad de un sistema" se encuentre libre de dificultades. La exactitud requerida será difícil de lograr en la práctica y en la actualidad, puesto que hoy en día, sólo podemos explorar una pequeña y mísera parte de lo que es la informática cuántica.

Con el avance tecnológico actual, es claro que no podremos alcanzar un umbral de exactitud aceptable, tampoco podemos decir que nunca se llevará a cabo una tecnología de computación cuántica. Sin embargo, muchos científicos, universidades y laboratorios así como también empresas de renombre, que ya han alcanzado a manipular, controlar y comprender a más de 8 qubits y se ha observado que en el estado sólido de la Resonancia Magnética Nuclear la preocupación principal es la capacidad para mantener la información en los qubits eficazmente. Esto es un problema actual que intenta resolver la complejidad y la estabilidad de los futuros sistemas cuánticos.

Y mientras científicos y tecnólogos están esforzándose día a día en la prometedora tecnología cuántica, estamos acercándonos a la situación dónde podemos preguntar si hay alguna ley de la Naturaleza que prohíba las manipulaciones como sólo Dios puede hacer.

Conclusión

Veamos a la ciencia de dos formas. La primera tiene que ver con nuevas ideas, concepciones, leyes y fórmulas. La segunda con su traslado al mundo real a través de la tecnología, a herramientas, instrumentos y máquinas prácticas para el ser humano.

No importa cuán abstractos sean los giros de la mente científica, siempre hay un retorno al mundo real de los seres humanos y sus necesidades. Las famosas palabras de Marx, de que la filosofía sólo explicaba al mundo y, que la cuestión era, sin embargo cambiarlo, no sólo se refería a la filosofía. Contenían el verdadero sentido de la existencia y desarrollo de cualquier ciencia.

Cada nuevo descubrimiento es una adición al almacén del conocimiento humano. Pero no es sólo eso, el hombre se vuelve más fuerte en su lucha por comprender la naturaleza. Si se rastrean los descubrimientos a través de la historia, se verá que en cada periodo, se acorta la divergencia entre uno de ellos y su aplicación a las necesidades humanas.

La ciencia percibe futuros problemas antes de que la práctica humana los capte. Esta previsión no es una gracia de los dioses o de los genios ultraterreneos, es una realidad objetiva, que se encuentra en el razonamiento mismo de la cual se encuentran las leyes del desarrollo social. La ciencia no espera que un problema vital e importante madure. Ya sea que se perciba su magnitud o no atacan nuevos problemas antes que se tornen problemas vitales.

La ciencia es la avanzada más distante de la sociedad humana, el explorador del futuro, y el defensor más confiable del presente.

El descubrimiento y desarrollo de la mecánica cuántica puede servir como una buena ilustración. El núcleo atómico fue concebido alrededor de 1912. Veinte años después, esa concepción tomó trazos bien definidos y las fuerzas que operan entre las partículas nucleares se descubrieron y explicaron. La inaccesibilidad del núcleo atómico, tanto la física como conceptualmente, no detuvo a los físicos e ingenieros. Trece años después se vio el advenimiento de la era atómica.

Cierto que fue en la forma de las horribles bombas atómicas que los americanos tiraron en Hiroshima y Nagazaki produciendo muerte y destrucción en vez de abundancia. Entonces pasaron algunos años más, y en 1954 la entonces Unión Soviética puso a operar la primera estación atómica. Los científicos soviéticos distrajeron el poder del átomo de la guerra y la destrucción hacia la paz y la construcción.

La mecánica cuántica encontró su primera aplicación técnica en el infierno del reactor atómico, en donde se dividen los núcleos de los átomos pesados y se genera calor y electricidad.

Entonces los científicos se fijaron en el núcleo de la luz, los isótopos de hidrógeno, en intentos de extraer más energía. En ese entonces naciones poderosas propusieron la utilización de las reacciones termonucleares para la paz, para generar electricidad. Éste es el noble propósito de los científicos, dar energía a la humanidad para los próximos mil años.

Aquí también la mecánica cuántica tiene cosas importantes que decir. Calcula el curso de las reacciones atómicas y predice la energía que generarán.

¿Qué vendrá después? Nuevos problemas. Problemas que serán mucho más difíciles de los que conocemos en la actualidad. Pero entonces los científicos del futuro estarán mejor equipados que los actuales.

Hasta hace pocos años, los investigadores raramente pensaban en las consecuencias de sus descubrimientos Young. A. Ioffo, quien a principios del siglo XIX se interesaron en los llamados materiales de desperdicio, difícilmente se imaginaban el futuro de los semiconductores.

Pero sin la mecánica cuántica, los semiconductores estarían muertos. La mecánica cuántica no sólo explicó sus notables propiedades, sino sugirió cambios radicales para las mejoras. Actualmente, el departamento de la mecánica cuántica que se conoce como la teoría de bandas de los sólidos se convirtió en la estrella polar de muchos miles de investigadores e ingenieros que trabajan en la electrónica. Estos dispositivos diminutos pero poderosos forjaron cambios fundamentales en la industria y la tecnología.

No hay una sola fábrica, vehículo o instalación de comunicaciones que no funcione con ellos. Difícilmente e inexistente hay alguna esfera de la actividad humana que no experimente los efectos de la electrónica.

Los científicos trabajan ya desde hace tiempo en uno de los proyectos más audaces: el uso de los semiconductores para extraer electricidad de la energía solar que generosamente cae sobre la tierra y sustituir así las casi exhaustas fuentes de energía de combustibles fósiles. Las primeras baterías solares de semiconductores están funcionando ya en la generación de rayos solares. Los diseñadores de estos aparatos trabajan en proyectos de baterías solares para dar energía eléctrica a las primeras colonias de la luna y de los planetas del sistema solar.

Un hecho interesante en este aspecto es que las instalaciones de semiconductores en la tierra cubren grandes áreas para captar los suficientes rayos solares que interferirían con el crecimiento de las plantas y la ganadería. En la luna no existe ese problema.

Entonces, ¿cómo se transmitirían estas grandes cantidades de energía a la tierra? Las líneas de transmisión que conocemos en la tierra estarían naturalmente fuera de cuestión, serían inútiles. Es más, las pérdidas son muy grandes en estos modos convencionales de transmisión de la energía.

Hace cerca de 10 años, un prominente físico V. Fabrikant, propuso un amplificador cuántico de las ondas electromagnéticas. Y la mecánica cuántica, primero se trasladó hacia el instrumental de un amplificador cuántico, y luego a un oscilador cuántico, trajo la vida a una serie de instrumentos y herramientas, los masers que son amplificadores y generadores de ondas de radio y los lasers, amplificadores de rayos de luz. Esto se podría llamar ciencia ficción de la realidad.

En el comienzo de este trabajo hablamos de los postulados de la mecánica cuántica que gobiernan la radiación electromagnética de los átomos. Estas leyes fueron firmemente establecidas hace mucho, tanto como en el primer tercio del siglo XX. Lo cual es bastante en la historia de la mecánica cuántica, y con tal firmeza, que en 1970, pocas personas se preocupaban por criticarlas.

Pero entonces algunos investigadores inquisitivos enfocaron nuevamente la cuestión desde un ángulo diferente, y estos postulados sobresalieron inesperadamente, dando lugar a un nuevo conjunto de poderosas y maravillosas herramientas. A partir de personajes como Richard Feynman se han desarrollado algunos logros técnicos más excepcionales debidos a las ideas y concepciones acerca del mundo de las cosas que dio a conocer la mecánica cuántica.

La mecánica cuántica continúa realizando incursiones en la ciencia y la tecnología. El número de herramientas creadas por ella continúa aumentando. Este fenómeno científico de la mecánica cuántica es excepcionalmente rico y diverso. Presenciamos su nacimiento históricamente y el futuro sobrepasará por sus realizaciones las predicciones más audaces de la ciencia ficción.

Sabemos que en una escala muy pequeña el mundo esta gobernado por las leyes de la mecánica cuántica y también sabemos que a escala cósmica muy grande el mundo esta gobernado por la teoría general de la relatividad, cuando esas dos grandes teorías se examinan muy cuidadosamente se encuentra que no son completamente compatibles entre sí, y esto significa que aún no conocemos las ultimas reglas del juego, pero los científicos son muy optimistas y presienten que muy pronto tendremos las ecuaciones definitivas que describan todo lo que ocurre en el universo. La verdadera tarea de los seres humanos no es descubrirlo todo, la verdadera tarea es entenderlo, es averiguar como unas cosas están relacionadas con otras, es desarrollar una forma de intuición adiestrada que nos permita entender en cualquier fenómeno dado lo que es importante y lo que no lo es, lo que queremos saber es porqué las cosas funcionan del modo que lo hacen.

En la ciencia, la mayor parte del trabajo no consiste en encontrar cómo funciona todo, consiste en hacer lo contrario exactamente, en ir separando lo sencillo de lo complicado, en hacer aproximaciones, en hacer estimaciones, en profundizar a través de las dificultades para llegar a dominar las características esenciales de cualquier fenómeno dado.

Me alegro que no me diesen las conclusiones ni la hoja de resultados, sino sólo me planteasen las preguntas adecuadas... de todo aquello que no me explicaron convenientemente, de lo que me explicaron sin darlo por cierto, bien seguro, sino que seguramente he tenido que averiguarlas,

probar para obtener mis propias y posibles respuestas, y generar nuevas dudas... De todo aquello que podía resultar o no, obligándome a probar, para comprobarlo.

Sé que resulta confuso, obtuso, disperso y difuso lo que he escrito... Quizás no sea ésta la mejor forma de aproximarme a lo que quiero decir, pero es la única manera para expresar lo que pienso.

FIN

Oswaldo Camargo Vidals
Noviembre 2007

Apéndice A

"Divertimentos Matemáticos"

Considerar los espacios vectoriales finito-dimensionales sobre el campo de números complejos $\mathbb{C}$. Denotar el conjugado de los números complejos $c \in \mathbb{C}$ como c^*[3].

Adoptamos la notación de Dirac[2][6][7]: *ket's* y *bra's.*

Donde un vector genérico ψ en un espacio es denotado por un ket: $|\psi\rangle$.

Se puede pensar en $|\psi\rangle$ como vector de columna.

El espacio *dual* del vector $|\psi\rangle$ es representado por el bra $\langle\psi|$, que indica el vector fila.

Bases estándares ortonormales. En un espacio vectorial *n-dimensional*, una base estándar ortonormal es representada por los siguientes vectores[8]:

$$|0\rangle, |1\rangle, \ldots, |n-1\rangle$$

Así, cada vector $|\psi\rangle$ en el espacio puede ser expresado como una combinación lineal[1]:

$$|\psi\rangle = \sum_{i=0,\ldots,n-1} c_i |i\rangle \quad \text{donde, } c_i \in \mathbb{C} \text{ para toda } i.$$

Productos internos: El producto interno entre dos vectores como:

$$|\psi\rangle = \alpha_0 |0\rangle + \ldots + \alpha_{n-1} |n-1\rangle \qquad \text{y} \qquad |\varphi\rangle = \beta_0 |0\rangle + \ldots + \beta_{n-1} |n-1\rangle$$

es definido como : $\langle\psi|\varphi\rangle = \alpha_0^* \beta_0 + \ldots + \alpha_{n-1}^* \beta_{n-1}$

Por medio del producto interno, se define la *norma* de un vector $|\psi\rangle$ como $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$. Se llamará *vector unitario* a cualquier vector con norma unitaria[5].

Operadores Lineales: Las *transformaciones lineales* en vectores son representados por matrices con números complejos[4][12]. Si A es un operador lineal (es decir, una matriz), se expresará lo siguiente: A^* como conjugado de una matriz, A^{T} como la transpuesta de una matriz y $A^\dagger$ como la matriz adjunta, en otras palabras $A^\dagger = \left(A^*\right)^{\mathrm{T}}$. Las mismas operaciones están definidas en los vectores y particularmente en la equivalencia $\left|\psi\right\rangle^\dagger = \left\langle\psi\right|$[1].

Producto Tensorial: El *producto tensorial* entre dos vectores *n-dimensiónales*[11]

$$\left|\psi\right\rangle = \alpha_0\left|0\right\rangle + \ldots + \alpha_{n-1}\left|n-1\right\rangle \qquad \text{y} \qquad \left|\varphi\right\rangle = \beta_0\left|0\right\rangle + \ldots + \beta_{n-1}\left|n-1\right\rangle$$

es representado en los textos de varias maneras como:

$$\left|\psi\right\rangle \otimes \left|\varphi\right\rangle, \quad \left|\psi\right\rangle\left|\varphi\right\rangle, \quad \left|\psi,\varphi\right\rangle, \quad \text{o simplemente } \left|\psi\varphi\right\rangle$$

esto se define como un vector n^2 *-dimensional* por lo tanto se tiene:

$$\left|\psi\right\rangle \otimes \left|\varphi\right\rangle = \sum_{\substack{i=0,\ldots,n-1 \\ j=1,\ldots,n-1}} \alpha_i \beta_j \left|ij\right\rangle$$

Unitario y Hermitiano: Un operador lineal U es *unitario* cuando se satisface lo siguiente:

$$U^\dagger U = UU^\dagger = I, \qquad \text{donde } I \text{ es la matriz identidad[3].}$$

Es simple demostrar que un operador unitario asigna los vectores de la unidad a los vectores de la unidad[10].

Un operador lineal H se dice que es *Hermitiano* cuando se cumple $H^\dagger = H$. Cualquier operador Hermitiano puede ser escrito como la suma de proyecciones sobre los subespacios ortonormales como: $H = \sum_i h_i P_i$, donde P_i es la proyección sobre el subespacio (*eigenspace*) con un *eigenvalue* h_i[8].

Espacio de Hilbert: En el caso finito-dimensional, un *esapcio de Hilbert* es un espacio vectorial complejo con un producto interno. No se considerarán en este trabajo casos infinito-dimensionales[3][5][10].

Apéndice B

"Operador densidad"

Una formulación más general que nos permita describir sistemas cuánticos sobre los cuales sólo poseemos cierta información, es posible con una herramienta alternativa conocida como *operador de densidad* o *matriz de densidad*[1][4][3].

En mecánica cuántica se llama *operador densidad* a un objeto matemático operador lineal que codifica todas las propiedades estadísticas de un sistema cuántico en la situación más general concebible, en particular, cuando la descripción de un vector estado no resulta posible[1].

El lenguaje del *operador de densidad* brinda un medio conveniente para describir sistemas cuánticos cuyo estado no es totalmente conocido, mediante una estructura estadística formalizada en mecánica cuántica[3].

Consideremos que un sistema cuántico se encuentra en uno de entre varios de estados.

Información parcial sobre el sistema:

$$p_i \rightarrow |\psi_i\rangle \qquad i = 1, 2, 3, \ldots m$$

donde p_i es la probabilidad de que el sistema este en el estado $|\psi_i\rangle$ cuyos valores respectivos son:

$$0 \leq p_i \leq 1 \qquad \sum_i p_i = 1$$

Un sistema físico que se halla en el estado mezcla no se describe con un único vector de estado[11] por lo que se considera una mezcla de estados puros al conjunto $\{p_i, |\psi\rangle\}$ y definimos entonces como un operador densidad a:

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

La explicación intuitiva de esto es que estamos mezclando deliberadamente o no, poblaciones estadísticas que podrían considerarse como estados puros completamente determinados y diferentes[5][7].

En la literatura este operador también es conocido como *matriz de densidad* y se pueden reformular todos los principios de la mecánica cuántica con esta herramienta matemática.

Por ejemplo la evolución de un sistema cuántico cerrado se representado por un operador unitario U. Si el sistema inicialmente se encontraba en el estado $|\Psi_i\rangle$ con probabilidad p_i entonces después de la evolución el sistema se encontrará en un estado $U|\Psi_i\rangle$ con igual probabilidad p_i. Por lo tanto la evolución del operador de densidad puede describirse de la siguiente manera:[1][12]

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^+ = U\rho U^+$$

De igual manera, las medidas también pueden ser fácilmente expresadas[13]. Por ejemplo, se realiza una medida representada por operadores de medición M_m. Si el estado inicial era el i-ésimo, entonces la probabilidad de obtener el resultado m sería la probabilidad condicional

$$p(m|i) = \langle\psi_i|M_m^+ M_m|\psi_i\rangle = tr\left(M_m^+ M_m|\psi_i\rangle\langle\psi_i|\right)$$

Ahora bien, aplicando la ley de probabilidades totales se obtiene la probabilidad absoluta de obtener el resultado m

$$p(m) = \sum_i p(m|i)\, p_i = tr\left(M_m^+ M_m \rho\right)$$

así el estado que se obtiene después de la medición sería[8][1]:

$$|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^+ M_m|\psi_i\rangle}}$$

Por lo tanto después de la medición que genera el resultado m tenemos una mezcla de estados $\left|\psi_i^m\right\rangle$ con respectivas probabilidades $p\left(i\middle|m\right)$. El operador de densidad respectivo $\left(\rho_m\right)$ será

$$\rho_m = \sum_i p\left(i\middle|m\right)\left|\psi_i^m\right\rangle\left\langle\psi_i^m\right| = \sum_i p\left(i\middle|m\right)\frac{M_m\left|\psi_i\right\rangle\left\langle\psi_i\right|M_m^+}{\left\langle\psi_i\middle|M_m^+M_m\middle|\psi_i\right\rangle}$$

por último, al relacionar: $p\left(m\middle|i\right) = p\left(m,i\right)/p\left(m\right) = p\left(m\middle|i\right)p_i/p\left(m\right)$ obtenemos:

$$\rho = \sum_i p_i \frac{M_m\left|\psi_i\right\rangle\left\langle\psi_i\right|M_m^+}{tr\left(M_m^+M_m\rho\right)} = \frac{M_m\rho M_m^+}{tr\left(M_m^+M_m\rho\right)}$$

Se define como ***estado puro***[7] a la mezcla formada por un único estado, en este caso $\rho = \left|\Psi\right\rangle\left\langle\Psi\right|$. En caso contrario ρ sería un ***estado mixto***[6]. Una prueba simple para averiguar si se tiene un estado puro o mixto es la siguiente:

Un estado puro cumple con $tr\left(\rho^2\right)=1$, mientras que, para un estado mixto se cumple que $tr\left(\rho^2\right)<1$.

Por ejemplo a partir de una mezcla de $\left\{p_{ij,}\left|\psi_{ij}\right\rangle\right\}$ se prepara un sistema cuántico tal que se encuentre en el estado ρ_i con probabilidad[4] p_i, entonces la matriz de densidad resulta:

$$\rho = \sum_{ij} p_i p_{ij}\left|\psi_{ij}\right\rangle\left\langle\psi_{ij}\right| = \sum_i p_i\rho_i$$

Un operador ρ es el operador de densidad de una mezcla de $\left\{p_i,\left|\psi_i\right\rangle\right\}$ si y sólo si, se satisfacen las siguientes condiciones[1][4].

Traza unitaria $\quad tr\left(\rho\right) = \sum_i p_i tr\left(\left|\psi_i\right\rangle\left\langle\psi_i\right|\right) = \sum_i p_i$

Definida positiva $\quad \forall\left|\varphi\right\rangle \in H^n \Rightarrow \left\langle\varphi\middle|\rho\middle|\varphi\right\rangle = \sum_i p_i\left|\left\langle\varphi\middle|\psi_i\right\rangle\right|^2 \geq 0$

Al cumplir las condiciones y dado que ρ es positivo, entonces se tiene descomposición espectral

$$\rho = \sum_j \lambda_j \left|j\right\rangle\left\langle j\right|$$

donde λ_j es el eigenvalue[8] (reales y no negativos) y $\left|j\right\rangle$ el eigenvector de ρ [11].

Apéndice C

"Dichoso vuestro nombre"

Aunque el campo de la computación cuántica es relativamente nuevo, ya se han desarrollado un gran número de artículos relacionados con distintas áreas de estudio. Reflejando el conocimiento han aparecido varios nombres diferentes representando el novedoso campo a estudiar. Los significados de estos nombres están estrechamente relacionados unos con otros, sin embargo, no son totalmente sinónimos. Se reflexionará sobre algunos nombres diferentes para la computación cuántica y brevemente se describirán los aspectos que normalmente los identifican[2].

Computación Cuántica: probablemente es el título generalmente más usado en la documentación científica para representar todo el conjunto de conocimientos sobre este campo de estudio. Bajo un significado más específico, representa temas como: algoritmos, topología, modelado teórico, modelos computacionales avanzados, complejidad computacional, opuestos siempre a los aspectos clásicos conocidos.

Información Cuántica: Refiere a los aspectos teóricos de la información como la codificación de información con sistemas cuánticos, modelos como detección y corrección de error, representación de qubits[2][9].

Ciencias de la Computación Cuántica: Usualmente representa el campo de estudio como un todo, algunas ocasiones se encuentra como Tecnologías de la información cuántica.

Procesamiento Cuántico de Información: A menudo se refiere a las implementaciones experimentales como los modelos para implementaciones en sistemas físicos, modelos de ruido, dispositivos, etc.

Quantum y algo más: Cada vez que uno representa el paradigmático mundo de la física moderna específicamente el "quántum" en algunos aspectos o disciplinas, uno lo suele escribir con la palabra cuántica. Así, por ejemplo, tenemos: algoritmos cuánticos, autómatas cuánticos,

circuitos cuánticos, complejidad cuántica, mecánica cuántica (teoría), teoría de juegos cuántica, etc.

Aunque las diferencias anteriores en los significados son meramente conceptuales, no son estrictos y el nombramiento comúnmente es libre[2].

Apéndice D

" Implementaciones físicas"

Uno de los desafíos actuales de la tecnología, es la construcción de dispositivos con características cuánticas. Debido a los problemas de la creación, control y corrección de errores en la superposición de estados cuánticos.

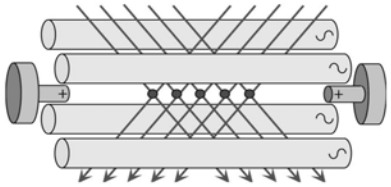
A pesar de todo se han construido compuertas experimentales como control-not de dos qubits y también se han usado algunas técnicas simples de corrección de errores.

Para construir una computadora cuántica es necesario resolver varios problemas como: elección adecuada de dispositivos físicos para la representación de qubits, control de compuertas cuánticas, control de los errores con la posibilidad de crear sistemas escalables para la solución de problemas de distinto tamaño, etc[9].

Con la variedad de requerimientos para la construcción de una máquina con características cuánticas se estudian diferentes modelos, sistemas y dispositivos físicos que pueden ser clasificados dependiendo de su comportamiento o sus características.

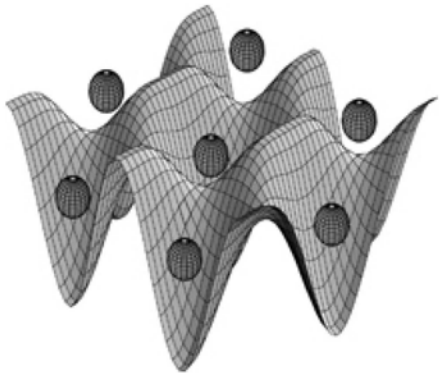
Entre los dispositivos experimentales viables para la implementación de dichos dispositivos se encuentran en investigación y prueba los siguientes candidatos[2][9].

- **Trampas de iones:** Es una tecnología de uso común en la ciencia de materiales, adaptada a la necesidad del cómputo del cuántico. Se puede generar un potencial donde se atrapen una serie de átomos cargados. Se usan como qubits dos estados de energía de los iones atrapados.



A cada qubit se accede usando un láser de la frecuencia apropiada a la transición sobre el ión correspondiente es decir las compuertas individuales. Compuertas de varios qubit's requieren un mediador como un bus de fonón.

- **Optical Lattice:** *(enrejado óptico de átomos)* Esta tecnología es semejantemente al de los iones atrapados. Es constituido por rayos láser para crear un patrón periódico en la intensidad, el efecto es logrado por radiación electromagnética. El potencial periódico resultante se utiliza para atrapar átomos neutrales[9].



Este sistema es semejante a un cristal en el sentido que los átomos están localizados periódicamente en el espacio. La mayor parte de la experimentación con estos dispositivos se basa en los gases condensados de Bose-Einstein[6][7].

- **Tecnologías de estado sólido:** Algunos de los métodos de la física de estado sólido consiste en los llamados puntos cuánticos, que son una clase de "átomos artificiales" donde los electrones son atrapados como impureza de materia artificial. La ciencia de

materiales se ocupa principalmente de las propiedades de los sólidos como su estructura y transformación de fase. Las ventajas principales de esta tecnología en comparación a otras consiste en la gran velocidad de realizar operaciones unitarias, y su perfecto control. La desventaja se encuentra relacionada con el tiempo de la decoherencia y sus efectos[9].

- **Dispositivos ópticos:** Consiste en manipular fotones como un sistema cuántico. Es la mejor tecnología hasta el momento que se tiene para implementar dispositivos cuánticos de comunicación, los fotones viajan a la velocidad de la luz permitiendo así que la interacción con el ambiente es muy reducida[6]. Por otro lado, es difícil realizar las tareas computacionales con dispositivos ópticos, como el realizar operaciones unitarias parece ser un proceso complejo y bastantemente complicado[7].

- **Electrodinámica cuántica de cavidades:** En esta tecnología, los átomos o los iones se unen a los fotones por medio de cavidades. Esto se considera una excelente forma de intercambiar información cuántica entre la óptica y los qubits, materiales que se desean para poder construir una computadora cuántica capaz de realizar algunas tareas hechas por la tecnología óptica como la comunicación y algunas otras como el concepto de memoria por medio de las tecnologías de estado sólido, explotando así las ventajas de cada uno[9][2]. Estudiando el comportamiento de estos átomos y fotones en este entorno protegido, los científicos han podido comprender aspectos fundamentales de la teoría cuántica, tales como la superposición, la complementariedad y la decohernecia que permitirían hacer viable la comunicación por medio del desarrollo de nuevos sensores, entre otras aplicaciones.

- **Resonancia magnética nuclear (NMR):** Esta tecnología consta de grandes cantidades de átomos idénticos que se colocan en un estado coherencia resonante por medio de pulsos magnéticos extremadamente fuertes. Históricamente, la resonancia magnética nuclear (NMR) ha sido la cuna experimental mas importante para muchas de las ideas como el procesamiento cuántico de información y varias implementaciones de algoritmos cuánticos[2][6].

Referencias

Capítulo I: El azar, la ignorancia y la Mecánica Cuántica

[1] Cropper, William H. ***The Quantum Physicists and an Introduction to their Physics***, Oxford University Press, New York, 1970.

[2] C. J. Davisson and L. H. Germer, ***Diraction of Electrons by a Crystal of Nickel***, Physical Review 30, 705 (1927).

[3] R. P. Feynman, R. B. Leighton y M. Sands, Física. Vol. III: Mecánica Cuántica. Addison-Wesley Iberoamericana, S.A., 1987.

[4] French, A. P. ***Vibrations and Waves***, The M.I.T. Introductory Physics Series. W.W. Norton & Company, New York, 1971.

[5] Goswami, Amit. ***Quantum Mechanics***. Wm. C. Brown Publishers, Dubuque, Iowa, 1992.

[6] Jammer, Max. ***The History of QM***.

[7] Libor, Richard. ***Introductory Quantum Mechanics***. Addison-Wesley Publishing Company, Inc., Reading, Massachusetts, 1980.

[8] Bohm, David. ***Quantum Theory. Dover Publications***, Inc., New York, 1959.

[9] J. Preskill, Lecture ***Notes for Physics*** 229 (1998).
http://www.theory.caltech.edu/people/preskill/ph229

[10] Baggott, Jim. ***The Meaning of Quantum Theory***. Oxford University Press, Oxford, 1992.

[11] Schrödinger E., ***What is life?***, Cambridge University Press, (1992)

[12] Semat, Henry and Harvey E. White. ***Atomic Age Physics***. Rhinehart & Company, Inc., New York, 1959.

[13] Ikenberry, Ernest. ***Quantum Mechanics for Mathematicians and Physicists***. Oxford University Press, Oxford, 1962.

[14] Landauer R 1995 ***Is quantum mechanics useful?*** Philos. Trans. R. Soc. London Ser. A. 353

[15] Kafatos, Menas and Robert Nadeau. ***The Conscious Universe***. Springer-Verlag, New York.

[16] Albert, David Z. ***Quantum Mechanics and Experience***. Harvard University Press, Cambridge

[17] W. Pauli, Pauli Lectures on Physics. Vol. 5. ***Wave Mechanics***. Dover Publications, Inc., 2000.

[18] S. Weinberg, ***The Quantum Theory of Fields***. Vol. I. Fundations. Cambridge University. 2001.

Capítulo II: La esencia del Cómputo Cuántico

[1] American Mathematical Society Short Course 2000, Samuel L. Lomonaco, ***Quantum Computation***, AMS, (2002)

[2] Brylinski r. K., ***Mathematics of Quantum Computation***, CRC Press, (2002)

[3] Brown University, USA ***Information Theory***, http://www.dam.brown.edu/people/yiannis/info.html

[4] Barenco, A., ***Quantum Physics and Computers***. quant-ph/9612014, 3 Dec 1996.

[5] Charles Day in Physics Today, ***Devices Based on the Fractional Quantum Hall Effect May Fulfill the Promise of Quantum Computing***. Vol. 58, pages 21–24; October 2005.

[6] Lloyd, S. ***Quantum-mechanical computers***. Scientific American, 140-145. (1995)

[7] Steane, A., ***Quantum computing***, quant-ph/9708022, 24 Sep 1997.

[8] Deutsch D 1985 ***Quantum theory, the Church-Turing principle and the universal quantum computer***, Proc. Roy. Soc. Lond. A 400 97-117

[9] Deutsch D 1989 ***Quantum computational networks***, Proc. Roy. Soc. Lond. A 425 73-90

[10] Deutsch D and Jozsa R 1992 ***Rapid solution of problems by quantum computation***, Proc. Roy. Soc. Lond A 439 553-558

[11] D.P. DiVincenzo. ***Quantum computation***. Science, 270:255–261, 1995.

[12] V. Vedral & M.B. Plenio, Prog. ***Quant. Electron***. 22, 1 (1998); A. Steane, Rep. Prog. Phys. 61, 117 (1998);

[13] Ekert, P. Hayden & H. Inamori, ***Basics Concepts in Quantum Computation***, Les Houches summer school 1999.

[14] Landauer R 1991 ***Information is physical***, Phys. Today May 1991

[15] Landauer R 1996 ***The physical nature of information***, Phys. Lett. A 217 188

[16] Hoi-Kwong L., ***Introduction to Quantum Computation and Information***, World Scientific Pub., (2001)

[17] Kitaev Y. A. et al., ***Classical and Quantum Computation***, AMS, (2002)

[18] Nielsen, M.A.,Chuang, I.L:, ***Quantum Computation and Quantum Information***, Cambridge University Press, (2002)

[19] Pittenger A. O., ***An Introduction to Quantum Computing Algorithms***, Birkhauser, Boston

Capítulo III: Criptografía Cuántica

[1] Ardehali, M., H. F. Chau, and H.-K. Lo, 1998, ***Efficient quantum key distribution***, preprint quant-ph/9803007.

[2] Aspect, A., J. Dalibard, and G. Roger, 1982, ***Experimental test of Bell's inequalities using time-varying analyzers***, Phys. Rev. 49, 1804–1807.

[3] Bechmann-Pasquinucci, H., and N. Gisin, 1999, ***Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography***, Phys. Rev. A 59, 4238–4248.

[4] Bechmann-Pasquinucci, H., and A. Peres, 2000, ***Quantum cryptography with 3-state systems***, Phys. Rev. 85, 3313–3316.

[5] Bechmann-Pasquinucci, H., and W. Tittel, 2000, ***Quantum cryptography using larger alphabets***, Phys. Rev. A 61, 062308.

[6] Bell, J. S., 1964, ***On the problem of hidden variables in quantum mechanics***, Rev. Phys.

[7] Bell, J. S., 1987, ***Speakable and Unspeakable in Quantum Mechanics*** (Cambridge University, Cambridge, England).

[8] Bennett, C. H., 1992, ***Quantum cryptography using any two nonorthogonal states***, Phys.

[9] Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, 1992, ***Experimental quantum cryptography***, J. Cryptology 5, 3–28.

[10] Bennett, C. H., and G. Brassard, 1984, in ***Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing***, Bangalore, India, (IEEE, New York)

[11] C.H. Bennett and P.W. Shor. ***Quantum information theory***. IEEE Trans. Inf. Theory, 1998.

[12] L. Chuang, N. Gershenfeld, and M. Kubinec. ***Experimental implementation of fast quantum searching***. Phys. Rev. Lett., 1998.

[13] L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, and S. Lloyd. ***Experimental realization of a quantum algorithm***. Nature, 1998.

[14] B. Schumacher. ***Sending entanglement through noisy quantum channels***. Phys. Rev. A, 1996.

[15] P. W. Shor. ***Scheme for reducing decoherence in quantum computer memory***. Phys. Rev. A,23

[16] P. W. Shor. ***Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer***. SIAM J. Comput., 1997.

[17] Lütkenhaus, N., 1996, ***Security against eavesdropping in quantum cryptography***, Phys. A23

[18] Lütkenhaus, N., 2000, ***Security against individual attacks for realistic quantum key distribution***, Phys. Rev. A 61.

[19] Marand, C., and P. D. Townsend, 1995, ***Quantum key distribution over distances as long as 30 km***, 1695–1697.

Capítulo IV: Una propuesta real, Resonancia Magnética Nuclear

[1] Abragam. ***Principles of Nuclear Magnetism***. Clarendon Press, Oxford, England, 1961.

[2] Abragam and M. Goldman. ***Nuclear Magnetism: Order and Disorder***. Oxford Scientific Pub., New York, 1982.

[3] D. Aharonov and M. Ben-Or. ***Fault-tolerant quantum computation with constant error***. In Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC), 176-188, New York, New York, 1996. ACM Press.

[4] Ambainis, L. J. Schulman, and U. Vazirani. ***Computing with highly mixed states***. Quant ph/0001066, 2000.

[5] G. Anderson and E. L. Hahn. ***Spin echo storage technique***. US Patent # 2,714,714, 1955.

[6] A.G. Anderson, R. Garwin, E. L. Hahn, J. W. Horton, and G. L. Tucker. ***Spin echo serial storage memory***. J. App. Phys., 1955.

[7] E.R. Andrew, A. Bradbury, and R.G. Eades. ***Removal of dipolar broadening of Nuclear Magnetic Resonance spectra of solids by specimen rotation***. Nature, 1959.

[8] W. P. Aue, E. Bartholdi, and R. R. Ernst. ***2-dimensional spectroscopy: Application to Nuclear Magnetic Resonance***., 1976.

[9] J. Baum, M. Munowita, A. Garroway, and A. Pines. ***Multiple-quantum dynamics in solid-state NMR***. J. Chem. Phys., 1985.

[10] H. Bennett and D. P. DiVincenzo. ***Quantum computing: Towards an engineering era***. Nature, 1995.

[11] N. Bloembergen. ***On the interaction of nuclear spins in a crystalline lattice***. Physica, 1949.

[12] N. Bloembergen and R. V. Pound. ***Radiation damping in magnetic resonance***. Phys. Rev., 1954.

[13] G. Bodenhausen, H. Kogler, and R. R. Ernst. ***Selection of coherence-transfer pathways in NMR pulse experiments***., 1984.

[14] L. Chuang, N. Gershenfeld, M. Kubinec, and D. Leung. Bulk ***Quantum computation with Nuclear Magnetic Resonance: Theory and experiments***. Proc. R. Soc. Lond. A, 1998.

[15] D. Collins, K. W. Kim, W. C. Holton, H. Sierzputowska-Gracz, and E. O. Stejskal. ***NMR quantum computation with indirectly coupled gates***. quant-ph/9910006, 1999.

[16] D. G. Cory, A. F. Fahmy, and T. F. Havel. ***Nuclear Magnetic Resonance spectroscopy: An experimentally accessible paradigm for quantum computing***. In T. Toffoli et al., editor, Proceedings of the 4th Workshop on Physics and Computation, pages 87–91, Boston, Massachusetts, 1996. New England Complex Systems Institute.

[17] D. G. Cory, W. Maas, M. Price, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo. ***Experimental quantum error correction***., 1998.

[18] D. G. Cory, M. D. Price, and T. F. Havel. ***Nuclear Magnetic Resonance spectroscopy: An experimentally accessible paradigm for quantum computing***. Physica D, 1998.

[19] D. P. DiVincenzo. ***Real and realistic quantum computers***. Nature, 1998.

[20] D.P. DiVincenzo. ***Two-bit gates are universal for quantum computation***. Phys. Rev. A, 51, 1995.

[21] D.P. DiVincenzo. ***The physical implementation of quantum computation***. To appear in Fort. Phys., special issue on ***"Experimental Proposals for Quantum Computation"***. quant-ph/0002077, 2000.

[22] K. Dorai, Arvind, and A. Kumar. ***Implementing quantum logic operations, pseudo-pure states and the Deutsch-Jozsa algorithm using non-commuting selective pulses in NMR***., 2000.

APÉNDICE

[1] Artin, M., ***Algebra and Quantum Space***. Prentice Hall. (1991)

[2] Brylinski R. K., ***Mathematics of Quantum Computation***, CRC Press, (2002)

[3] Cohen, Miserg, D., ***An Introduction to Hilbert Space and Quantum Logic***. Springer-Verlag. 1989.

[4] Drake, A., ***Fundamentals of Applied Probability Theory***. McGraw Hill. (1967)

[5] Jeffreys, H. Proc. Roy. Soc. London A. 453-461. (1946) Cramer, H., ***Mathematical Methods of Statistics***. Princeton UP (1946).

[6] Landau L., Lifshitz E., ***Curso de Física Teórica*** - Física Estadística (Vol IV) - Ed. Reverté (1975)

[7] Landau L., Lifshitz E., ***Curso abreviado de Física Teórica***, Libro 2: Mecánica Cuántica, Ed. MIR, Moscú, (1974)

[8] Murray, M., Rice, J., ***Differential Geometry and Statistics***. Chapman and Hall. (1993)

[9] Oppenheim, A., Verghese, G., 6.011 ***Communications and Control Systems***. Lecture notes. Fall 1997. Massachusetts Institute of Technology.

[10] Rota, G.-C. ***Indiscrete Thoughts***. Birkhauser. (1997)

[11] Santaló L. A., ***Vectores y Tensores***, Manuales EUDEBA, (1961)

[12] Sattinger, D., Weaver, O., ***Lie Groups and Algebras with Applications to Physics, Geometry, and Mechanics***. Springer-Verlag. (1986)

[13] Strang, G., ***Introduction to Applied Mathematics***. Wellesley Cambridge (1986)