COMPUTADORES CUÁNTICOS
"PARADOJA DE LA SUPERPOSICIÓN"

Richard Primera
Universidad Rafael Belloso Chacín. Venezuela

RESUMEN

En los últimos años, ha despegado y se ha constituido una nueva disciplina de estudio, la computación cuántica, a diferencia de la computación actual, donde cada bit puede estar en un estado (0 ó 1), el qbit que es la unidad fundamental de almacenamiento de la computación cuántica, puede tener múltiples estados simultáneamente, pretende desencadenar una nueva perspectiva que culmine con la concepción de los computadores ó ordenadores cuánticos. El objetivo de este trabajo es describir los pasos a seguir para que este hecho sea una realidad en el mundo macrocósmico.

Palabras claves: cuanto, qbit, mundo macrocósmico.

ABSTRACT

In the last years, it has taken off a new discipline of study, the quantum computation has been constituted, unlike the present computation, where each bit can be in a state (0 or 1), qbit that is the fundamental unit of storage of the quantum computation, can have manifold simultaneously states, tries to trigger a new perspective that culminates with the conception of the computers or quantum computers. The objective of this paper is to describe the steps to follow so that this fact is a reality in the macrocosmic world.

Keywords: whatever, qbit, macrocosmic world

INTRODUCCIÓN

Las grandes revoluciones en la historia de la tecnología han implicado nuevas formas de utilizar la naturaleza explotando los recursos que puede ofrecer, a través de la historia el ser humano ha utilizado diversos materiales y múltiples mecanismos en el diseño, construcción y operación de máquinas que agilicen y automaticen la realización de cálculos y el procesamiento de información. Desde el ABACO hasta la aparición de los últimos equipos de computación existentes en el mercado. En esta búsqueda ha recorrido diferentes caminos y para explicar los fenómenos ocurridos en el macro mundo debemos recurrir al microcosmo, recordando que todo lo que conocemos esta compuesto por átomos. Una de las áreas de mayor

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

investigación actualmente es la computación cuántica, que correlaciona elementos de la informática teórica y la mecánica cuántica, para producir modelos de computación que utilicen todo el potencial, las propiedades y los efectos inherentes a las partículas atómicas. El impacto de esta naturaleza a sido colosal, gracias a ello hemos podido conocer que, “la microfísica actual sería inconcebible sin el auxilio de los principios cuánticos”.

La teoría moderna de la información surgió de los trabajos de Claude Shannon, matemático estadounidense que a finales de la década de los cuarenta del siglo pasado formuló las ecuaciones básicas de dicha teoría. Un poco antes, los físicos, Bardeen, Brattain y Shockley, habían inventado el transistor, producto de la aplicación de la mecánica cuántica a la física de materiales y casi al mismo tiempo Jhon von Neumann elaboraba su teoría de los autómatas, origen de la robótica moderna. Estos descubrimientos han sido decisivos para el desarrollo en la práctica de los conceptos de la teoría de la información, y es innegable que la teoría cuántica desempeña un importante papel en la comprensión profunda de los elementos físicos necesarios para este desarrollo.

El presente artículo esta estructurado de la siguiente manera: como primer aspecto se describe un poco la historia y orígenes de la computación cuántica, el segundo punto trata de los computadores cuánticos, por tercera parte se describen los fundamentos de la computación cuántica, en cuarto término se explica la arquitectura de un computador cuántico, como quinto aspecto comentan las aplicaciones, el sexto se trata del análisis de los resultados y el finalmente se denotan las referencias bibliográficas utilizadas. Es el deseo que luego de leer el presente artículo, el lector obtenga una visión más amplia y entendible del fascinante nuevo mundo de la computación.

UN POCO DE HISTORIA

Max (Karl Ernst Ludwig) Planck se vio abocado a discretizar los cambios de energía entre átomos y radiación para conseguir explicar los datos experimentales sobre el espectro del cuerpo negro. Fue, diría más tarde, “como un acto de desesperación”. El 14 de diciembre del año 1900 presentó ante la Sociedad Alemana de Física su famoso trabajo donde introducía en la física la constante universal *h* y el término cuanto. Pocos años después, en su *agnus mirabilis* de 1905, Albert Einstein explicaría el efecto fotoeléctrico postulando que la energía de la luz monocromática de frecuencia *n* esta concentrada en forma de gránulos indivisibles de valor *h*n. Estos quanta o paquetes de energía recibirían veinte años después el nombre de fotones.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

Estos primeros trabajos obligaban simplemente a aceptar que la energía aparecía a veces en paquetes discretos, pero no se podía incorporar este hecho a una concepción física de la naturaleza. El gran avance en la teoría se produjo en 1925, con el descubrimiento de la mecánica cuántica, realizado por Heinsenberg y luego por Schrodinger. La hipótesis cuántica es, pues, la que afirma que la cantidad mínima de materia está cuantificada; que existe una partícula material mínima, no siendo posible una porción menor. Toda partícula material, por muy pequeña que fuere, ocupa siempre más de un punto-instante del espacio-tiempo.

En este mismo orden de ideas se plantea que la "hipótesis granular implica que existan valores prohibidos para las medidas cuantitativas de las distribuciones de materia, pues al no existir realmente una fracción de partícula materia (ya que está cuantizada) la medida total de la distribución ha de ser múltiplo del cuanto mínimo" [9]. Existen, pues, valores prohibidos para la medida de las distribuciones materiales, y, en consecuencia, para la medida de sus magnitudes teóricas (energía, impulso, etc.). Habrá de existir el cuanto mínimo de energía, de impulso, etc., y sus valores para un sistema habrán de ser múltiplos de ese cuánto mínimo. Para el desarrollo de la mecánica cuántica esta se baso en los siguientes principios, la cuantización, el principio de incertidumbre, la superposición cuántica, el tuneleo, el entrelazamiento y la decoherencia.

Roto el viejo tabú y liberado el duende de la discretización, la visión de la realidad ya nunca sería como antaño. "Los cuantos asomaron por doquier (fotones, fonones, fluxones, excitones, rotones, magnones, plasmones, spinones, holones, orbitones), y todas las partículas del universo pasaron a ser excitaciones elementales de unos pocos campos", uno por especie, lo que explicaba su total indistinguibilidad dentro de cada una de estas. Nueve genios sentaron en el primer cuarto del siglo XX las bases de la nueva física: Planck (1900), Einstein (1905) y Niels (Henrik David) Bohr (1913), seguidos de Louis (Víctor Pierre Raymond, 7o Duque) de Broglie (1923), Werner Karl Heisenberg (1924), Wolfgang Pauli (1925), Erwin Schrodinger (1926), Max Born (1926), y Paul (Adrien Maurice) Dirac (1928).

La culminación de los esfuerzos creadores de Schrödinger, Heisenberg y Dirac fue la interpretación de Copenhaguen, una formulación matemáticamente coherente de la mecánica cuántica, pero que se rodeó de un cierto halo de misterio. Si por una parte Einstein se oponía decididamente a ella por considerarla incompleta, por otra su aplicación conducía a intrigantes paradojas como la del gato de Schrödinger o la paradoja de Einstein, Podolski y Rosen, que ponía de manifiesto una incompatibilidad de la mecánica cuántica con principios tan básicos de la física como la

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

causalidad o la realidad. Como alternativa a la mecánica cuántica, surgieron una serie de teorías que conocemos como teorías de variables ocultas, cuya pretensión era que si se pudiesen conocer los valores de estas variables "extra" todo quedaría bien determinado y no habría lugar para incertidumbres ni resultados probabilísticos. A pesar de esta falta generalizada de interés por los fundamentos de la mecánica cuántica, en la década de los años 60 un físico del CERN (Ginebra), John Bell, propició un cambio radical en esta apreciación. Bell se apercibió que la hipótesis de la existencia de variables ocultas llevaba a predicciones distintas de las obtenidas mediante la aplicación de la mecánica cuántica. Se podía, por tanto, pensar en la realización de experimentos que pudieran distinguir cuál de las dos teorías era la correcta. Se trata de las desigualdades de Bell que llevaban las cuestiones sobre los fundamentos de la mecánica cuántica del campo de la especulación filosófica a la realidad física del laboratorio.

No fue, sin embargo, hasta la década de los 80 que la tecnología fue capaz de llevar a cabo estos experimentos. Alain Aspect, en Orsay (Francia), comprobó por vez primera que los experimentos sobre las desigualdades de Bell decantaban la balanza a favor de la mecánica cuántica. A partir de este momento, los experimentos imaginarios que habían usado Einstein o Heisenberg para argumentar sus opiniones estaban al alcance de los experimentos reales. Como consecuencia, la década de los 90 ha vivió la explosión de este nuevo campo en el que se han realizado experimentos tan fascinantes que han despertado el interés popular: *"L'expériencie qui cointredit Einstein"*, así titulaba en portada, en su número de enero de 1998, la revista *Science et Vie* un artículo sobre el experimento de teleportación realizado por Nicolas Gisin y su equipo de la Universidad de Ginebra. [10].

COMPUTACIÓN CUÁNTICA

A lo largo de los últimos 50 años, las computadoras han ido duplicando su velocidad cada dos años, al tiempo que el tamaño de sus componentes se reducía a la mitad. Los circuitos actuales contienen transistores y líneas de conducción cuya anchura es solo una centésima parte de la de un cabello humano, las máquinas de nuestros días son millones de veces más potentes que sus rudimentarias antepasadas. [4]. Un computador cuántico realiza las operaciones en bits cuánticos, los bits, como ya se sabe codifican la información en 0s o 1s, que no son más que estados bajos y altos de voltaje, en los diversos transistores que componen su placa [1]. Ya sabemos que un bit entonces puede estar en uno de estos dos estados, que representan dos valores lógicos: si ó no, pero un bit puede ser representado también por dos diferentes polarizaciones de la luz, o por dos estados electrónicos de un átomo.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

Ahora la mecánica cuántica dice que si un bit puede estar en cualquiera de dos estados distinguibles, también puede estar en cualquier superposición coherente de ellos, y claro esta, estos son más estados, que no tienen análogos clásicos, en los cuales un átomo representa ambos valores 0 y 1 simultáneamente y este comportamiento es propio de los sistemas cuánticos [8]. En este mismo orden de ideas y considerando la definición anterior, se puede afirmar que un qbit representa dos estados ortogonales de una sub. partícula atómica, como se representa en la figura 1. El estado de un qbit se puede escribir como {|0>, |1>}, describiendo su múltiple estado simultaneo.[3]. Esto se explica de una manera más clara utilizando el experimento de Schrödinger, en el famoso gato de Schrödinger, esta es una paradoja propuesta en 1937 para ilustrar las diferencias entre interacción y medida en el campo de la mecánica cuántica. El mismo consiste en imaginar un gato metido dentro de una caja que también posee un dispositivo formado por una ampolla de vidrio que contiene un veneno muy volátil y por un martillo sujeto sobre la ampolla de forma que si cae sobre ella la rompe y se escapa el veneno, con lo que gato moriría. El martillo esta conectado a un detector de partículas alfa; si llega una partícula alfa al martillo cae rompiendo la ampolla con lo que el gato muere, si no llega, no ocurre nada y el gato no muere. 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, como resultado de la interacción, en el interior de la caja, el gato esta vivo o esta muerto. 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 el gato a la vez estaría vivo y muerto. [7].

FUNDAMENTOS DE LA COMPUTACIÓN CUÁNTICA

La computación cuántica se basa en las propiedades de la interacción cuántica entre las partículas subatómicas, como la superposición simultanea de dos estados en una sola partícula. Esta propiedad es altamente aprovechada para el desarrollo teórico de algunos algoritmos cuánticos, logrando una capacidad de procesamiento exponencial. La superposición cuántica permite mantener simultáneamente múltiples estados en un bit cuántico es decir 0 y 1 a la vez, a diferencia del bit elemental en la computación actual que únicamente es capaz de mantener un estado discreto de 0 ó 1 a la vez. [3].

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

|0>
|1>
|0> + |1> |0> + |1>

Figura 1. Representación de cuatro estados diferentes de un qbit

ARQUITECTURA DE UNA COMPUTADORA CUÁNTICA

La arquitectura de un computador cuántico, es similar a la de las computadoras tradicionales, con ciertos elementos propios de la computación cuántica. Se propone una arquitectura de una computadora cuántica que esta conformada por una ALU cuántica, memoria cuántica, y un planificador dinámico. La corrección de errores debe ser considerado un aspecto importante en el diseño de una arquitectura cuántica.

Hoy se sabe como leer y escribir información en sistemas cuánticos, para ello se realizan los procesos de escritura donde se manipula la energía que se debe aplicar para poder escribir un 0 ó un 1 respectivamente, en el proceso de lectura sería parecido, para la corrección de errores es indispensable acotar que este es fundamental ya que todos los sistemas de registro y procesamiento de información son sensibles al ruido, que puede invertir bits de modo aleatorio.

Los métodos clásicos de corrección de errores, entrañan la medición de bits para ver si son erróneos, lo que en un ordenador cuántico provocaría la decoherencia. [8], [3]. La ALU cuántica tiene como funciones fundamentales la ejecución de operaciones cuánticas y la corrección de errores. Esta prepara los datos, antes de ejecutar cualquier compuerta lógica, aplicando una secuencia de transformaciones cuánticas básicas, que incluyen:

- Hadamard (raíz cuadrada, transformada de Fourier de 1 qubit).
- I, Identidad (I, NOP cuantico).
- X, NOT cuántico.
- Z, cambia los signos de las amplitudes.
- Y = XZ
- Rotación por p/4 (S)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

- Rotación por p/8 (T), y

- NOT controlado (CNOT) [2]

En los ordenadores clásicos las puertas lógicas que procesan la información son elementos no lineales basados en la tecnología de los semiconductores, como los transistores, verdaderas "neuronas" del computador, en los cuánticos, las puertas lógicas se consiguen con interacciones no lineales entre las magnitudes cuánticas. Todas las puertas clásicas tienen su contrapartida cuántica, pero hay puertas cuánticas exóticas sin análogo clásico. Una puerta monaria no clásica vNOT, que como su nombre lo indica aplicada dos veces equivale a un NOT. [6].

Actualmente se han construido puertas experimentales control-not de dos qubits, y se han usado algunas técnicas simples de corrección de errores. Para construir un ordenador cuántico se necesita solventar varios problemas: elección de los sistemas físicos que representan los qubits, control de las puertas cuánticas, control de errores y posibilidad de escalar el ordenador para tratar problemas de distinto tamaño. Con estos requerimientos se están estudiando diferentes sistemas físicos que se pueden clasificar dependiendo de sus características o de su interacción, entre ellos se encuentran:

1.- Dipolos magnéticos en moléculas, controlados mediante técnicas de resonancia magnética nuclear. Con estos sistemas se han logrado los mayores progresos desde el punto de vista experimental. Se ha implementado el algoritmo de Deutsch, Cory ha podido implementar un método para corregir errores de fase debido a fluctuaciones de un campo magnético externo, usando como sistema de tres qubits la alanina (tres Carbonos -13) y el tricloroetileno (un H y dos Carbonos -13). El Dr. Wei en el 2001, ha implementado puertas control-not y control-raíz cuadrada-not, usando 7 qubits representados por los 4 carbonos y 3 hidrógenos del ácido crotónico.

2.- Sistemas de iones ultrafríos atrapados en trampas iónicas y controlados mediante haces láser. Mediante esta técnica se construyó la primera puerta CNOT cuántica en el Nacional Institute of Standards and Technology (Colorado). En los experimentos se usaron dos niveles hiperfinos del estado fundamental del ion Be+ como qubit imagen, mientras que los dos primeros modos de vibración (fonones) simulan el qubit de control. Ambos qubits de la puerta CNOT están en distintos grados de libertad del mismo sistema. Monroe obtiene un funcionamiento correcto de la puerta en un 90%. Cirac y Zoller propusieron en 1995 el uso trampas de iones lineales lo cual

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

eliminaría el problema de escala. Hasta el momento y a pesar del gran esfuerzo dedicado, no se ha implementado ninguna puerta CNOT mediante estos sistemas, aunque existen trampas para controlar conjuntos de iones como los de Ca+. 3.- Polarización de los fotones, o bien algún tipo de proceso que permita introducir fases globales. Existen dos métodos principales: el método de los "qubits voladores" del grupo de Kimble en Caltech, y el montaje de Haroche de la École Normale Supérieure de París.

3.- Sistemas en fase sólida, basados en las características de coherencia macroscópica de los pares de Cooper a través de una heterounión Josephson para implementar una lógica cuántica. Aunque se han construido puertas experimentales CNOT que involucran dos qubits, y se han usado algunas técnicas simples de corrección de errores, no se espera que existan ordenadores cuánticos de forma inminente que hagan tareas de cierta importancia. [2].

Aplicaciones

Son muchas las áreas en donde se puede observar la potencia y el rendimiento de un computador cuántico. El mismo puede llegar a tener una eficacia importante, porque puede estar en muchos estados al mismo tiempo y operar simultáneamente en todos ellos. Mediante una sola unidad procesadora central, un computador cuántico puede, en forma natural, ejecutar en paralelo una enorme cantidad de operaciones. Esto lleva a la deducción que a mayor capacidad de procesamiento de información, menores serán los tiempos de respuestas en los procesos que este solucionando.

La capacidad de memoria de un computador cuántico puede ser enorme. Por ejemplo Carlos Stroud propone almacenar información en un solo átomo semi-clásico. Un electrón en uno de estos átomos puede habitar en una superposición de más de 2500 niveles de energía. Por lo tanto, su función de onda es suficientemente compleja para almacenar una gran cantidad de información. Para la protección de los datos será una poderosa herramienta ya que permitirá encriptar de manera segura y confiable información a la cual nadie tendrá acceso.

La criptología hunde sus raíces en el pasado, ya en el siglo V a.c. los militares de esparta transmitían y descifraban mensajes secretos, a mediados del siglo pasado en la década de los cuarenta, cuando se convierte en parte de la teoría de la información a través de los trabajos seminales de Shannon, la criptografía se basa en los principios de complementariedad e incertidumbre, y en la indivisibilidad de los quanta. El

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

pionero ha sido Stephen Wiesner, quien en 1969 sugirió, entre otras cosas, como fabricar billetes infalsificables, ósea, billetes cuánticos.

A mediados de los 80 Bennett y Brassard idearon un criptosistema cuántico basado en el principio de Heisenberg, que pronto se implementaría experimentalmente mandando con fotones polarizados información secreta a 30 cm. de distancia. Este sistema (conocido como protocolo BB84) usa estados cuánticos no ortogonales para evitar su clonación por un posible escucha; por emplear 4 estados distintos, se llama también *esquema de cuatro estados*. El empleo de correlaciones cuánticas no locales con pares de fotones enredados por conversión paramétrica a la baja fue propuesto luego por Ekert; en este sistema E91 serían las desigualdades de Bell las encargadas de proteger la seguridad. De ahí su calificativo de *esquema EPR*. [5], [3].

ANÁLISIS DE LOS RESULTADOS

Las computadoras actuales no podrán seguir evolucionando más allá de aproximadamente el año 2020 según la ley de Moore, debido a las limitaciones físicas en la miniaturización, energía para cambio de estado, frecuencia de reloj y cantidad de electrones en sus componentes fundamentales, sin embargo, esto no significa que no tendremos computadoras más veloces; nuevas alternativas están surgiendo, una de las más prometedoras es la computación cuántica ampliamente definida mediante la mecánica cuántica.

La computación cuántica ha logrado evolucionar satisfactoriamente y tiene definidos sus fundamentos basados en la interacción subatómica y sus elementos como el bit cuántico, compuertas cuánticas, tele transportación de código. No obstante, no se ha logrado implementar una computadora cuántica que maneje todos los aspectos concernientes a la mecánica cuántica. Aun así, se tienen grandes avances como la definición de una arquitectura cuántica, ampliamente aceptada por los investigadores, la implementación de pequeños prototipos como la computadora de 5 bits cuánticos desarrollada por Steffen, y el desarrollo de tecnologías cuánticas comerciales.

Una limitación en la implementación de una computadora cuántica es la presencia de elementos en estado líquido y gaseoso en el proceso de interacción subatómica, que hacen muy difícil lograr modelos donde intervengan miles de bits cuánticos. Otra limitación esta dada por la naturaleza de las interacciones con los elementos subatómicos, no se puede realizar una lectura sin producir cambios en el. Estos cambios son impredecibles y se propagan a lo largo de todo el sistema, por lo que es

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

necesario integrar complejos mecanismos de corrección de errores que agregan sobrecarga en proporciones exponenciales. En el futuro se espera que los computadores cuánticos, estén completamente desarrollados para el 2020, y tomen el lugar de los computadores actuales.

REFERENCIAS BIBLIOGRÁFICAS

[1] "¿Qué es la Computación Cuántica?". En: http://cultura.terra.es/cac/ciencia/consulta/portada.cfm?consulta_id=145

[2] "2020, La Odisea Cuántica". En: www.webzinemaker.com/admin/exec/print.php3?ident=tendencias&rubr=4&id=10460

[3] Caituiro-Monge, Hillary. "Arquitectura cuántica". En: http://www.abcdatos.com/tutoriales/tutorial/l6344.html

[4] "Computadores Cuánticos". En: http://www.monografias.com/trabajos7/cocu.shtml

[5] Luque Jaime, Moraga Luís (2000). "El Computador Cuántico: ¿Historia de una Revolución Anunciada?". En: http://www.ucentral.cl/pdf/computador.pdf

[6] Galindo, Alberto (2000). "El extraño y prodigioso mundo de los Quanta". En: http://teorica.fis.ucm.es/~agt/conferencias/RAC99web.pdf

[7] Gomez, M.A. "El gato de Schodinger". En: http://centros5.pntic.mec.es/ies.victoria.kent/Rincon-C/curiosid/Rc-31.htm

[8] "El ordenador cuántico". En: http://www.um.es/docencia/campoyl/Cuantico.PDF

[9] En: http://personales.ya.com/casanchi/fis/cuant1.htm

[10] Baig, Maria. "Información cuántica". En: http://www.cianciadigital.net/abril2001/frame_opinion.html

[11] Oskin, M., Chang, F., Chuang, I., "A Practical Architecture for Reliable Quantum omputers". En: http://feynman.media.mit.edu/ike/homepage/papers/QC-oskin-chong-chuanga-practical-architecture-for-reliable-quantum-computers-computer-jan2002-vol35-p79.pdf

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005