Arquitectura Cuántica

Hillary Caituiro-Monge

Electrical and Computer Engineering Department
University of Puerto Rico, Mayagüez Campus
Mayagüez, Puerto Rico 00681-5215
Hillary.Caituiro.Monge@acm.org

Resumen

La computación cuántica trata el almacenamiento y procesamiento de la información, a diferencia de la computación actual donde los bits pueden estar en un estado discreto y alternativo a la vez, en base a bits que mantienen dos estados simultáneamente en un instante determinado, reduciendo enormemente el tiempo de procesamiento. La teoría de la computación cuántica esta basada en las interacciones del mundo atómico y en futuras implementaciones de las computadoras cuánticas.

En este artículo se desarrollan los fundamentos y los elementos básicos que conforman la computación cuántica. También se presenta una arquitectura cuántica muy aceptada entre los investigadores que desde un principio han orientado sus investigaciones hacia lograr una arquitectura compatible con las actuales, de ahí que esta tiene muchas semejanza con las arquitecturas existentes, con elementos propios de la computación cuántica. En la última sección se relata brevemente los lineamientos que debe seguir el diseño de una computadora cuántica.

1. Introducción

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

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

Mucho tiempo después, se desarrollaron modelos mecánicos y eléctricos, es así que, Blaise Pascal, en 1649, fabricó la PASCALINA, una máquina que hacía operaciones de 8 dígitos. En 1820, Charles Babbage con la ayuda de la Condesa Ada Byron, construyó dos equipos totalmente mecánicos, usaban ejes, engranajes y poleas para realizar cálculos; Byron fue la primera persona que programó una computadora, tiempo después un lenguaje de programación fue nombrado como Ada en su honor. Herman Hollerith desarrolló unas máquinas que clasificaban, ordenaban y enumeraban tarjetas perforadas. Estas se usaron en el censo realizado en 1890 por el gobierno de los Estados Unidos de Norte América. Konraz Suze, ingeniero alemán, en 1942, construyó la primera computadora digital (electromecánica binaria) programable. Entre 1937 y 1942 Atanasoff y Berry, construyeron un prototipo compuesto de tubos al vacío, capacitores y un tambor de rotatorio para el manejo de los elementos de la memoria, fue usada para resolver ecuaciones matemáticas complejas. En 1941 Turing construyó la COLLOSUS, una computadora que usaba miles de válvulas, 2400 bombas de vidrio al vacío, y un escáner con capacidad de leer 5000 caracteres por cinta de papel. En 1944 IBM (Interna Business Machines) construye la MARK I en cooperación con la Universidad de Harvard, media 15 metros de largo, 2.40 metros de altura y pesaba cinco toneladas. La ENIAC contaba con 17468 tubos de vidrio al vacío similares a los tubos de radio, fue construida en 1946 en la Universidad de Pensylvania.

Finalmente se inició la era digital, con modelos electrónicos basados inicialmente en tubos de vacío y luego en transistores. La EDVAC fue la primera computadora electrónica digital, su memoria consistía en líneas de mercurio dentro de un tubo de vidrio al vacío,

donde se podía almacenar ceros y unos. El transistor, es el invento que más ha influenciado en la evolución de las computadoras, este fue concebido en 1948, por tres científicos en los laboratorios de Bell, este contiene un material semiconductor que funciona como un interruptor. En 1958 Kilby y Noycea, de la Texas Instrument, inventaron los circuitos integrados, haciendo que las computadoras fuesen cada vez más pequeñas. En Intel, en 1971, Hoff desarrollo un microprocesador de 4 bits que contenía 23000 transistores que procesaban 108 kHz o 0.06 MIPS, tenía 46 instrucciones y 4 kilobytes de espacio de almacenamiento. En 1974 Intel presentó una CPU compuesto por el microchip 8080, este contenía 4500 transistores y podía almacenar 64 kilobytes de memoria RAM, tenía un bus de datos de 8 bits. Wozniak y Jobs, en 1976, empiezan con Apple, revolucionando el mundo de las computadoras al introducir la interfaz gráfica y el ratón. El microprocesador Intel 8086, se lanzó en 1978, e inició una nueva era en la producción de computadoras personales. A comienzos de la década de los 80 IBM empezó a desarrollar las computadoras personales con PC-DOS como sistema operativo, empezando así una nueva era, donde las computadoras estaban al alcance de todos. Las computadoras portátiles, las computadoras vestibles, y los modelos no comerciales que son tan pequeños como una moneda de un centavo.

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

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

Este artículo esta organizado de tal manera que en la segunda sección se desarrollan los fundamentos y los elementos básicos que conforman la computación cuántica; se han utilizado sencillas expresiones matemáticas para mostrar la representación de los estados de un bit cuántico y el mecanismo del paralelismo cuántico. En la tercera sección se presenta una arquitectura cuántica muy aceptada entre los investigadores que desde un principio han orientado sus investigaciones hacia lograr una arquitectura compatible con las actuales, de ahí que esta tiene muchas semejanza con las arquitecturas existentes, con elementos propios de la computación cuántica. En la cuarta y última sección se relata brevemente los lineamientos que debe seguir el diseño de una computadora cuántica.

2. Computación cuántica

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

La teoría de la computación cuántica esta basada en las interacciones del mundo atómico y en futuras implementaciones de las computadoras cuánticas. Estas aún están en los laboratorios de investigación pero ya se tienen resultados alentadores, como el desarrollo de la computadora cuántica de cinco qubits desarrollado por Steffen et al [Steffen01].

2.1 Fundamentos de la computación cuántica

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

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

lograr el paralelismo cuántico y el paralelismo cuántico masivo.

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

2.2 Elementos básicos de la computación cuántica

2.2.1 El bit cuántico "qubit"

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

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

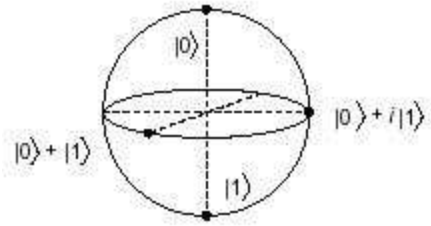

Figura 1. Representación de cuatro estados diferentes de un qubit. [Steffen01]

Cualquier sistema cuántico con dos estados discretos distintos puede servir como qubit, un espín de electrón que apunta arriba o abajo, o un espín de fotón con polarización horizontal o vertical. En la figura 1 se tiene una representación pictórica de cuatro diferentes estados basado en el espín de un núcleo atómico, por lo que puede ser usado como un qubit. Un qubit no puede ser clonado, no puede ser copiado, y no puede ser enviado de un lugar a otro.

2.2.2 Compuertas cuánticas

Las compuertas lógicas son operaciones unarias sobre qubits. La compuerta puede ser escrita como $P(\theta)=|0\rangle\langle 0| + \exp(i\theta) + |1\rangle\langle 1|$, donde $\theta = \omega t$. Aquí algunas compuertas cuánticas elementales: [Steane97]

I ≡ $|0\rangle\langle 0| + |1\rangle\langle 1|$ = identidad
X ≡ $|0\rangle\langle 1| + |1\rangle\langle 0|$ = NOT
Z ≡ $P(\pi)$
Y ≡ XZ
H ≡ $\frac{1}{\sqrt{2}}\left[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|\right]$

Donde I es la identidad, X es el análogo al clásico NOT, Z cambia el signo a la amplitud, y H es la transformación de Hadamard.
Esas compuertas forman uno de los más pequeños grupos de la computación cuántica. La tecnología de la física cuántica puede implementar esas compuertas eficientemente. Todos excepto el CNOT operan en un simple qubit; la compuerta CNOT opera en dos qubits.

Una compuerta de dos qubits en especial interesante, es la conocida como "U controlada", [Steane97]

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

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

2.2.3 "Entanglement"

La capacidad computacional de procesamiento paralelo de la computación cuántica, es enormemente incrementada por el procesamiento masivamente en paralelo, debido a una interacción que ocurre durante algunas millonésimas de segundo. Este fenómeno de la mecánica cuántica es llamado "entanglement".

Debido al "entanglement", dos partículas subatómicas, permanecen indefectiblemente relacionadas entre si, si han sido generadas en un mismo proceso. Por ejemplo la desintegración en un positrón y un electrón. Estas partículas forman subsistemas que no pueden describirse separadamente. Cuando una de las dos partículas sufre un cambio de estado, repercute en la otra. Esta característica se desencadena cuando se realiza una medición sobre una de las partículas. [Vedral01]

2.2.4 Tele transportación cuántica

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

La tele transportación cuántica es descrita por Stean [Steane97] como la posibilidad de *"transmitir qubits sin enviar qubits"*. En la computación tradicional para transmitir bits, estos son clonados o copiados y luego enviados a través de diferentes medios como el cobre, fibra óptica, ondas de radio y otros. En la computación cuántica no es posible clonar, tampoco copiar, y mucho menos enviar qubits de un lugar a otro como se hacen con los bits.

Si enviamos un qubit $|\varnothing\rangle$ donde $\varnothing$ es un estado desconocido, el receptor no podrá leer su estado con certidumbre, cualquier intento de medida podría modificar el estado del qubit, por lo tanto se perdería su estado, imposibilitando su recuperación. La tele transportación cuántica, resuelve este problema, esta se basa en el "entanglement" para poder transmitir un qubit sin necesidad de enviarlo. El emisor y el receptor poseen un par de qubits "enredados" (entangled). Entonces el qubit es transmitido desde el emisor, desaparece del emisor y el receptor tiene el qubit tele transportado. Este fenómeno es posible debido a un mecanismo conocido como el efecto EPR[2]. En la tele transportación cuántica primero dos qubits E y R son "enredados" y luego separados (entangled), el qubit R es ubicado en el receptor y el qubit E es ubicado en el emisor junto al qubit original Q a ser transmitido, al realizar la lectura del estado de los dos qubits Q y E, estos cambian su estado a uno aleatorio debido a la interacción. La información leída es enviada al receptor, donde esta información es utilizada para un tratamiento que es aplicado al qubit R, siendo ahora R una réplica exacta del qubit Q. [Nayak02] [Ambainis02]

2.2.5 El paralelismo cuántico

La superposición cuántica permite un paralelismo exponencial o paralelismo cuántico en el cálculo, mediante el uso de las compuertas lógicas de qubits. [Steffen01] Los qubits, a diferencia de los bits, pueden existir en un estado de superposición, representado por $a|0\rangle + b|1\rangle$, donde a y b son números complejos que satisfacen la relación $|a|^2 + |b|^2 = 1$.

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

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

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

Por linealidad de los mecánica cuántica, la compuerta lógica *f* transforma el estado del qubit a

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

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

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

La compuerta lógica *g* transforma el estado de entrada a

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

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

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

2.2.6 Criptografía cuántica

Criptografía, es la ciencia matemática de las comunicaciones secretas, tiene una larga y distinguida historia de uso militar y diplomático que se remonta a los antiguos Griegos. Fue un elemento importante y decisivo durante la segunda guerra mundial. Hoy en día su uso es muy común y necesario, para brindar seguridad en las transacciones comerciales, comunicaciones, y privacidad; que se llevan a cabo mediante Internet. [Hughes94]

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

El factorizar es un aspecto muy importante en la criptografía moderna, debido a que, la seguridad del mecanismo de criptografía RSA de clave pública, se

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

basa en la dificultad de factorizar número grandes. El mejor algoritmo para hallar los factores aún sigue siendo el de las divisiones sucesivas.

Dado M, R_1 y R_2, mediante el mecanismo de RSA se define una función p, tal que $C_1 = p(Q_1, P_1, M_1)$ y $C_2 = p(Q_2, P_2, M_2)$, donde P_1 y P_2 son claves públicas generadas en base a Q_1 y Q_2 que son claves privadas pertenecientes a A y B respectivamente. A y B comparten sus respectivas claves públicas P_1 y P_2, y ambos pueden obtener y descifrar sus mensajes mediante p^{-1}, de tal modo *que* $M_1 = p^{-1}(Q_1, P_1, M^1)$ y $M_2 = p^{-1}(Q_2, P_2, M_2)$.

El tiempo que requeriría el realizar la factorización se estima en aproximadamente $4x10^{16}$ años. Sin embargo en 1994 se logró desarrollar un algoritmo, usando recursos en redes, donde la factorización únicamente tomo 8 meses, el equivalente a 4,000 MIPS-años. [Hughes94]. Los algoritmos cuánticos de factorización, se estima que realizarían este cálculo en apenas unos segundos. El algoritmo cuántico de Peter Shor para factorizar números grandes, muestra el gran poder de las computadoras cuánticas.

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

La criptografía cuántica hace posible la distribución de la clave privada P. P es transmitida mediante un canal cuántico. Cualquier intento de medir P será notado, debido a que es imposible observar un qubit sin dejar rastro. La distribución cuántica de claves es posible con la tecnología existente. En 1997 Zbinden et al lograron distribuir cuánticamente una clave a través de 23 Km. de fibra bajo el lago Génova.

3. Arquitectura de una computadora cuántica

La arquitectura de una computadora cuántica es similar a la de las computadoras tradicionales, con ciertos elementos propios de la computación cuántica.

Oskin et al [Oskin02] propone una arquitectura de una computadora quántica que esta conformada por una ALU cuántica, memoria cuántica, y un planificador dinámico, tal como puede observarse en la figura 2.

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

3.1 ALU cuántica

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

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

- Hadamard (raiz cuadrada, transformada de Fourier de 1 qubit),
- I, Identidad (I, NOP cuántico),
- X, NOT cuántico,
- Z, cambia los signos de las amplitudes),
- Y = XZ,
- rotación por $\pi/4$ (S),
- rotación por $\pi/8$ (T), y
- NOT controlado (CNOT).

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

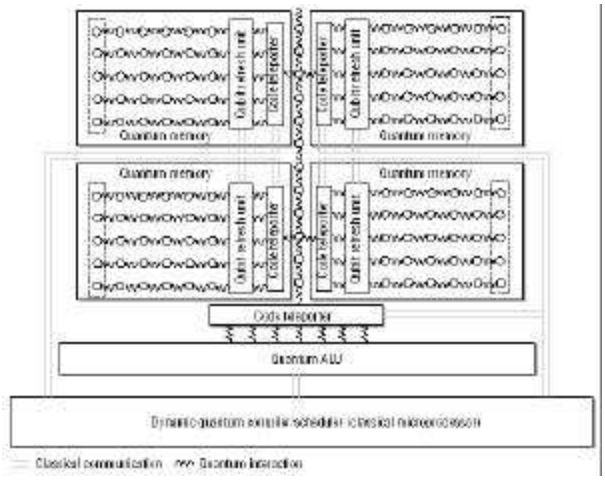

Figura 2. Arquitectura cuántica. [Oskin02]

3.2 Memoria cuántica

Al igual que en las arquitecturas actuales en la arquitectura cuántica, la memoria cuántica es un elemento arquitectural muy importante. La memoria cuántica debe ser confiable, con el propósito de dotarla

de tal característica Oskin et al [Oskin02] incluyen una unidad especializada de "actualización" en cada banco de memoria, cuya representación pictórica se puede apreciar en la figura 2. Una unidad especializada actualiza periódicamente los qubits lógicos individuales, ejecutando algoritmos de detección y corrección de errores.

3.3 Tele transportadora de código

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

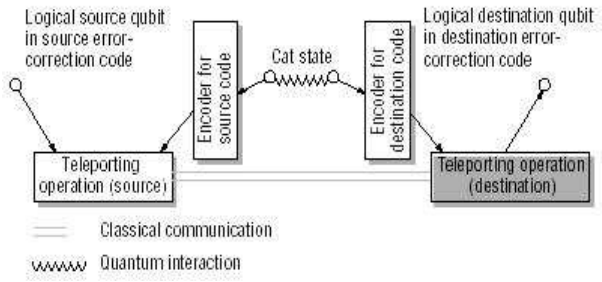

Figura 3. Tele transportadora de código. [Oskin02]

Este mecanismo se usa para la corrección de errores en el codificador de código origen y en el codificador de código destino, como puede observarse en la figura 3. El emisor y el receptor entonces ejecutan qubits lógicos equivalentes en la operación de tele transportación en cada terminal del par "enredado" (entangled).

3.4 Planificador dinámico

Oskin et al [Oskin02] proponen un procesador clásico de alto desempeño como parte principal del planificador dinámico. Este procesador ejecuta un algoritmo de planificación dinámico que toma operaciones cuánticas lógicas, intercaladas con construcciones clásicas de control de flujo, y dinámicamente las traduce en operaciones individuales de qubits físicos.

4. Computadora cuántica

Una definición acerca de las computadoras cuánticas ampliamente aceptada por los investigadores, es la expuesta por Beth [Beth00]. El la concibe como un sistema de circuitos cuánticos, actuando en un espacio de estados, que es un espacio complejo 2n-dimensional de Hilbert. El circuito es una secuencia de transformaciones unitarias $U_t \in SU(2^n)$ seguido por una medición. Esas transformaciones, son llamadas compuertas cuánticas, y son controladas por una computadora clásica. El espacio de estados de una computadora cuántica tiene la estructura de un espacio de un vector Hermitian. Así esto permite la superposición simultanea de estados básicos ortogonales (correspondientes a estados clásicos "0" y "1") con la posibilidad de interferencia constructiva y destructiva entre las diferentes rutas de computación. Este principio permite el uso de los estados confusos (entangled states).

4.1 Requerimientos de implementación

Para la implementación de una computadora cuántica, se deben cumplir al menos cinco requisitos. Primero, se necesita un sistema de qubits. Segundo, los qubits deben ser individualmente direccionables y deben interactuar con otros para conformar compuertas lógicas de propósito general. Tercero, debe ser posible la inicialización de las compuertas. Cuarto, se debe tener la posibilidad de extraer los resultados computacionales. Y Quinto, es la necesidad de un tiempo de coherencia duradero. [Steffen01]

5. Conclusiones

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

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

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

Prevenir la incoherencia y preservar los frágiles estados cuánticos. Esto es facil en pequeños sistemas pero mas comlejo en grandes sistemas cuánticos.

En el futuro, se espera que las computadoras cuánticas, estén completamente desarrolladas aproximadamente el 2020. Sin embargo, la computación cuántica, ya esta siendo aplicada, es así que "Magiq" es la primera empresa que lanzará al mercado, el 2003, tecnología de encriptación cuántica. [Johnson02a]. Otro sistema de encriptación cuántica es el desarrollado por Prem Kumar y Horace Yuen, profesores de la universidad "Northwestern", [Johnson02b] capaz de codificar flujos de datos y enviarlos velocidades de las troncales de Internet.

Referencias

[Ambainis02] Ambainis, A., Smith, A., Yang, K., "Extracting Quantum Entanglement", in Proceedings of the 17th IEEE Annual Conference on Computational Complexity", 2002.

[Beth00] Beth, T., "Quantum Computing: An Introduction", IEEE, 2000.

[Hughes94] Hughes, R., J., "Quantum Cryptography", 1994.

[Johnson02a] Jonson, R., "Magiq employs quantum technology for secure encryption", in EETIMES, http://www.eetonline.com/at/news/OEG20021105S0019, November 6, 2002.

[Johnson02b] Jonson, R., "Quantum encryption secures high-speed data stream", http://www.eetonline.com/at/news/OEG20021107S0031, November 8, 2002.

[Nayak02] Nayak, A., Salazman, J., "On Communication over an Entanglement-Assisted Quantum Channel", in Proceedings of the 34th Annual ACM Symposium on Theory of Computing, 2002.

[Oskin02] Oskin, M., Chong, F., L., Chuang, I., "A Practical Architecture for Reliable Quantum Computers", IEEE, 2002.

[Steane97] Steane, A., "Quantum Computing", Department of Atomic and Laser Physics, University of Oxford. Clarendon Laboratory, Parks Road, Oxford, OX1 3PU, England, July, 1997.

[Steffen01] Steffen, M., Vandersypen, L., Chuang, I., "Toward Quantum Computation: A Five-Qubit Quantum Processor", IEEE, 2001.

[Vedral01] Vedral, V., Plenio, M.B., "Entanglement Measures and Purification Procedures", IEEE, May 25, 2001.