Estado del arte de la computación cuántica

Quantum computing's state of the art

Juan Pablo Rúa Vargas, Esp. , John William Branch B., PhD.
Escuela de Sistemas e Informática.
Universidad Nacional de Colombia sede Medellín.
{juanprua@gmail.com; jwbranch@unalmed.edu.co}

Recibido para revisión 30 de Julio de 2009, aceptado 25 de Agosto de 2009, versión final 15 de Septiembre de 2009

Resumen— Paradójicamente se vive una analogía entre las décadas de 1950s cuando se iniciaron los computadores que operaban con transistores y grandes máquinas que cubrían grandes espacios y la década de 2000s en la cual emergen nuevas hipótesis para optimizar el rendimiento del computador cuántico desde la algoritmia hasta los qubits y desde su composición hasta su comportamiento. Hoy en día se han mejorado diferentes aspectos relacionados al mundo cuántico donde se presentan retos como la criptografía, decoherencia, superposición de estados entre otros que son fundamentales para el alcance de este poderoso ordenador. Se han construido máquinas que factorizan pequeñas cifras, sin embargo persisten dificultades en cuanto a la lectura de la información ya que el mundo atómico es un inmenso océano el cual no se ha explorado lo suficiente, cuyas bases se mantienen en lo profundo de la metafísica.
La idea general es que las personas interesadas en esta temática se ilustren un poco acerca de la tecnología que abarcará toda la información del futuro, generar inquietudes que motiven al descubrimiento e investigaciones que generen discernimientos a partir de la descripción que se realiza desde el origen de la computación cuántica, sus elementos y su comportamiento.

Palabras Clave—Qubits, Superposición de Estados, Decoherencia.

Abstract— We live a paradoxically analogy between decades 1950s when computers started to work with transistors and huge machines that had covering big places and decade 2000s in which new assumptions appear to optimize the quantum computer performing from algorithm to qubits and from setting to behavior. Now days several aspects has been improved and most of them are involve in a quantum world where new challenges appear like cryptography, decoherence, states overlapping and others one that are basics to reach the capable computer.
It has been built machines which could factorize small numbers, how ever several difficult persist in data's lecture area being the quantum world a big ocean which it has not been explored plenty and theirs bases recline in metaphysics.
The idea is to describe this new technology that will cover the future data for people interesting in this area, generate questions that rise discovering and researching that could give new information which is done from the beginning of the quantum computing, their elements and their behavioral.

Keywords— Qubits, States Overlapping, Decoherence.

I. INTRODUCCIÓN

En el avance de la tecnología ha conllevado en las últimas décadas a innovar y ejecutar cada idea que al comienzo pareció ser irrealizable, ya que no se contaba con los elementos, materiales y avances de la ciencia necesarios. Pero con el transcurso de los estudios fue apareciendo los primeros ordenadores cumpliendo tareas excepcionales. Los transistores fueron el punto de partida que hasta ahora no han desaparecido de las necesidades para potencializar y optimizar el rendimiento de la computación, que ha requerido de máquinas más potentes para suplir las necesidades del mundo.

Estas máquinas día a día transcienden a un estado diferente, un mundo regido por materiales miniaturizados, proyectándose a rincones inhóspitos por la física clásica y llegando al mundo mínimo. Cada vez estos ordenadores tienen mayor número de transistores en un espacio igual de reducido, que aunque para muchos parezca no tener fin; traza un límite fundamental en la física y es el mundo de lo cuantificado a lo que se llama mundo cuántico regido por la física cuántica.

Cuanto más es el orden de cuantificación de los transistores llegarán a un punto en el cual no podrán comportarse de manera ideal ya que entrarán en la escala nanométrica. Esto debido a que los computadores actuales con su cuantificación de transistores tocarán un punto crucial el cual no pueden escapar de la física cuántica, ya que no esta regido por las leyes de la física clásica. Es un mundo aparentemente ambiguo y sin leyes comprensibles para el hombre pero que describen el mundo de lo que es posible optimizar y superar. El computador esta llegando a límites los cuales su tecnología no compagina con la realidad que lo espera. Sin embargo muchas son las sociedades, institutos y compañías que investigan día a día par conseguir el propósito de optimizar mucho mas el computador.

II. ORIGEN

La idea del computador cuántico se remonta en las décadas de 1970 y 1980 cuando Richard Feynman [13] del California Institute of tecnology, Paul Benioff[1], [2] de Argonne Nacional Laboratory, David Deutsche [4] de la universidad de Oxford y Charles Bennett [3], del T.J. watson Researh Center de IBM proponen el concepto de computación cuántica. Richard Feyman [14] muestra como un sistema cuántico puede ser utilzado para mejorar el rendimiento computacional y este actuar como un simulador para procesos cuánticos probabilísticos de gran peso donde las simulaciones no son eficientes para el almacenamiento probabilístico convencional.

Esta idea parecía irrealizable hasta que en 1994 Peter Shor [Shor 1994] de AT&T Research propuso el primer algoritmo cuántico específicamente diseñado para factorizar grandes números. Este algoritmo es caracterizado por:

- Utilizar métodos de computación cuántica que envuelven principios de la mecánica cuántica, como el comportamiento de las ondas, interferencia y coherencia.

- Utilizar algoritmos clásicos para verificar que la solución candidata generada por los algoritmos cuánticos sea correcta.

El éxito de éste algoritmo impulsó la búsqueda de un computador cuántico y en 1998 Chuang [10] demostró la primera computadora cuántica de un qubit, y ya en 1999 Grover [5] propone un algoritmo para hacer búsquedas en base de datos utilizando 3 qubits.

Existen dos algoritmos que permiten a los computadores cuánticos manipular sistemas criptográficos que se encuentran en una amplia área de investigación. El algoritmo de Shor y de Grover. El algoritmo de Shor permite factorizar grandes números en tiempo polinómico mientras que el algoritmo Grover permite buscar en una base de datos desorganizada con una velocidad cuadrática [11].

2.1. Describiendo el mundo cuántico

Glassner [6] define una existencia revolucionaría desde el campo de la computación, y se describe el origen en los pequeños elementos: partículas subatómicas que son la base de toda la materia que nos rodea. El comportamiento de estas partículas es materia de estudio de la física cuántica donde el tiempo y el espacio no son continuos pero están hechos de pequeñas unidades discretas. Hoy en día se utiliza computadores clásicos, las próximas máquinas serán llamadas computadores cuánticos que ayudarán a:

Velocidad de procesamiento: Si se tiene una lista no ordenada de N objetos opacos por píxel y se necesita encontrar el cerrado. El computador clásico tendría que buscar a través de todos los N objetos, donde al menos requerirá de N pasos. En un computador cuántico, se puede encontrar el cerrado en el orden de $\sqrt{N}$ pasos.

Radiosidad Instantánea: Es una manera de computar las imágenes sintéticas. Dentro del mundo cuántico se puede computar en un solo paso, tomando una fracción de un segundo, debido a la propiedad anteriormente mencionada.

Doble velocidad de transmisión: se desea enviar una imagen y para ello se necesita transmitir N bits: el producto de ancho por lo alto del número de bits por píxel. Con un computado cuántico, se comparen únicamente N/2 partículas cuánticas.

Los computadores clásicos trabajan manipulando dígitos binarios, o bits, mientras que los computadores cuánticos trabajan manipulando qubits. Los bits clásicos tomas los valores 1 o 0 mientras que los qubits pueden ser el 1 o 0, o ambos al mismo tiempo. Esta superposición de estados es posible debido a la inherente ambigüedad en la mecánica cuántica, en la cual se pueden observar las propiedades donde un objeto puede tener más de un solo valor a la vez [9].

Los computadores cuánticos codifican sus qubits en estados cuánticos, como el spin de un átomo, o la polarización de un fotón de luz. Una vez que un computador tiene más de un qubit, es posible explorar otros aspectos de la mecánica cuántica llamado enredamiento. De acuerdo a la mecánica cuántica, consiste en un enredo de dos estados cuánticos que tiene que describir por referencia uno con el otro, aunque los átomos, iones o partículas fundamentales que tienen los estados separadas físicamente [9].

Glassner explica el comportamiento de las partículas cuánticas:

«Se tiene una cuerda por un extremo de la mano y en el otro se encuentra atada a la pared en el momento que se comienza a agitar la cuerda se puede apreciar una perturbación vertical que viaja a través de la cuerda si se agito de arriba hacia abajo y se genera una perturbación horizontal cuando se agita de izquierda

a derecha». Esto mismo ocurre cuando un fotón atraviesa el aire puede generarse una vibración vertical u horizontal o un ángulo con respecto al suelo. Ahora cuando se hace pasar el fotón por unas barras paralelas a nivel microscópico la polarización de la luz cambia horizontalmente si las barras se encuentran verticalmente y así de forma inversa. El cambio de orientación de los fotones se debe a que cuando llega la luz a las barras en el ángulo dado de alguna manera rotan para esquivar el obstáculo y pasan entre las barras y se genera una nueva dirección. De esta manera surge la medida cuántica ya que ocurre cuando un objeto es medido por su configuración de salida y su estado se mantiene [6].

Esto mismo ocurre cuando se tiene un material flexible que microscópicamente se parece a una puerta con rendijas, compuesta por varias barras paralelas en forma vertical con delgadas brechas entre ellas. Para un fotón pasar este material, debe sortear el plano que es paralelo a las barras como lo muestra la Figura 1 Polarización de Fotones (Únicamente fotones alineados al filtro pasan a través de la rendija a). un filtro orientado verticalmente, b) un filtro orientado oblicuamente, c) un filtro orientado horizontalmente).

Se asume que los fotones vienen desde un láser cuya probabilidad de ser polarizados en cualquier dirección. Grassner [6] realiza un experimento en 5 pasos, el primer paso se coloca un láser en una pantalla y se utilza el medidor de luz para determinar la cantidad de luz reflejada (Figura 1 (a)). Para simplicidad se determina que el medidor calcula A unidades.

En el segundo paso (Figura 2 (b) Experimento Filtros de Polarización) se coloca una pieza de polarización entre el láser y la pantalla orientada a esta verticalmente (ejemplo 12 en punto), y la medida es A/2, se concluye que el filtro ha bloqueado alrededor de la mitad de la luz.

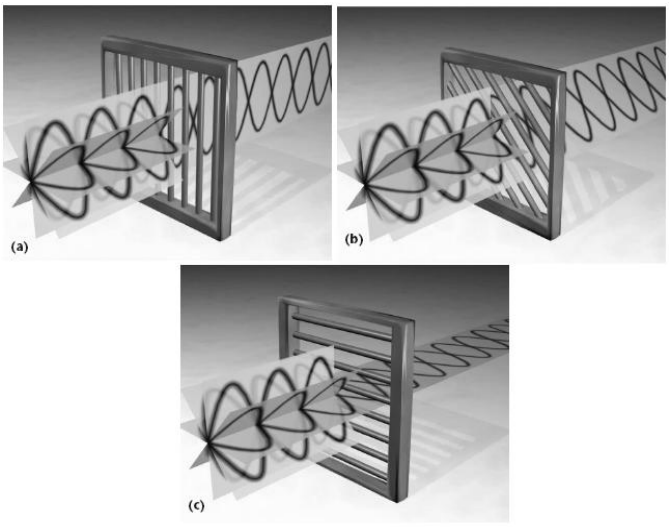

Figura 1. Polarización de Fotón.

En la Figura 2 (c) a través de la Figura 2 (e) se observa filtro de polarización entre el láser y la pantalla se lee A/2. Cuando se tienen dos filtros de polarización una detrás de la otra, a 90 grados de la otra, se tiene una lectura de 0. Si se coloca la tercera polarización entre estas dos anteriores, orientadas a 45 grados entre ellas, el resultado sería de A/8.

De la Figura 2 Experimento Filtros de Polarización se describe:

a) Paso uno: la configuración inicial no tiene filtros por lo tanto su lectura es A.

b) Paso dos: se coloca un polarizador vertical en el paso uno. El medidor de luz lee A/2.

c) Paso tres: se coloca un polarizador horizontal y nuevamente la lectura es A/2.

d) Paso cuatro: se coloca un polarizador horizontal y vertical en el paso uno. La lectura es 0.

e) Paso cinco: se coloca un moralizador oblicuo entre los polarizadores del paso cuatro la lectura es A/8.

Grassner [Grassner 2001] sugiere que lo fotones que entran son ajustados de alguna manera para pasar a través del polarizador. Quizás los fotones rebotan de un lado a otro, pasando los obstáculos. Se imagina que el polarizador de alguna manera cambia la dirección fotón y de alguna manera la vuelve a su estado de origen. En la 1:00 pone en práctica una proyección vertical es $\sqrt{3}$ mas grande que la horizontal, por lo tanto el fotón es tres veces mas probable que sea polarizado vertical que horizontalmente. A 45 grados, la probabilidad es 50/50.

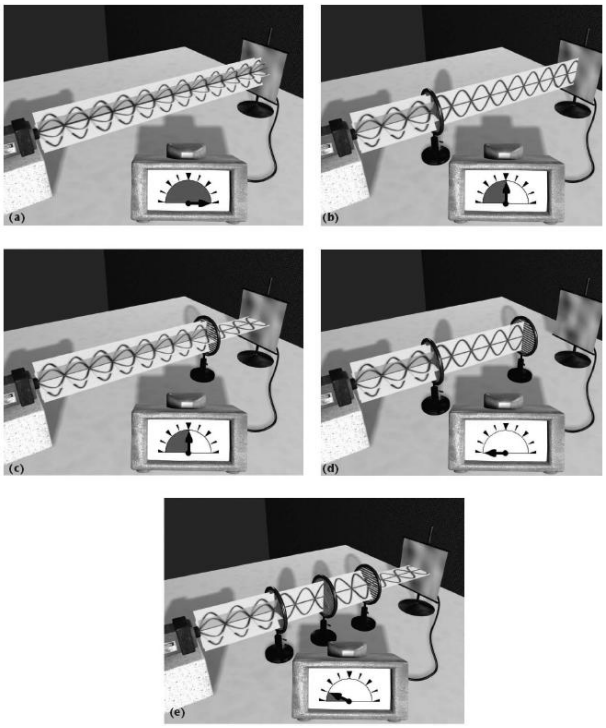

Figura 2. Experimento Filtros de Polarización.

La Figura 2(e) hay una probabilidad de 50/50 que los fotones sean polarizados vertical u horizontalmente. Estos fotones que atraviesan el primer filtro alcanzan el segundo y otra vez son transformados en un nuevo estado diagonal. La mitad de ellos son proyectados para que atraviesen el filtro, es decir solo un cuarto de los fotones originales alcanzan el tercer filtro. Acá nuevamente son nuevamente proyectados es un estado vertical u horizontal con igual probabilidad, la mitad de ellos son polarizados horizontalmente y atraviesan el último filtro, o sea un octavo de los fotones originales llegan a la pantalla. El punto que Glassner resalta es que cuando se mide un objeto cuántico con respecto a un conjunto de decisiones preseleccionadas, el objeto es proyectado en una de esas decisiones y el objeto cambia. Esto es la postulación de medida de la mecánica cuántica.

2.2. Problemas cuánticos

El artículo de Algoritmos cúanticos y problemas duros se toma la representación de un vector en espacio de dos dimensiones Hilbert complejas donde |0> y |1> forman la base en el espacio y el estado cuántico lo describen así [11]: $|\psi>=\alpha|0>+\beta|1>$. Donde los números α y β son números complejos. Cuando se mide un qubit se puede obtener el resultado 0 con la probabilidad $|\alpha|^2$ o el resultado 1 con la probabilidad $|\beta|^2$, donde $+=1$, en la cual las probabilidades deben sumar uno. Lo mismo ocurre con dos qubits donde los posibles valores son 00, 01, 10 y 11 correspondiente a un sistema computacional descrito así: |00>, |01>, |10> y |11>, donde se da:

$$|\psi>=\alpha_{00}|00>+\alpha_{01}|01>+\alpha_{10}|10>+\alpha_{11}|11>.$$

Explorando el enredamiento, el estado de un qubit puede ser ligado a otro, por lo tanto la configuración de un qubit para registrar el valor de 1 o 0 en otro se puede realizar, sin importar la distancia que los separe. Para ser utilizables, el computador cuántico debe dar una respuesta la cual se da por medio de la medida cuántica la cual torna el estado del qubit en 1 o 0. Un computador cuántico puede probar cada combinación de posibles valores para cada qubit simultáneamente y cada qubit agregado genera un poder computacional doble, es decir si un computador cuántico tiene 1000 qubits, puede realizar 2^{1000} combinaciones de entrada a la vez [9].

Monroe enfoca el desarrolla el computador cuántico utilizando trampas de iones, en donde genera campos eléctricos y magnéticos en la cual un ion puede estar en un punto del espacio evitando de esta manera la decoherencia, sin embargo se presentan más problemas cuando se agregan más iones[9].

III. ESTADO DEL ARTE

Con el tiempo las necesidades del mundo han cambiado drásticamente a tal punto de requerir evolución en la tecnología conllevando a aumentar la escala de integración; produciendo un mayor número de transistores en un espacio, fabricando procesadores más pequeños, y cuanto más pequeño es, mayor velocidad de proceso alcanza el procesador.

Sin embargo, no se puede hacer los elementos de los procesadores infinitamente pequeños. Ya que entran en límites no escalables a la física clásica, se llega a la escala de nanómetros, donde los electrones se escapan de los canales por donde deben circular. Allí los elementos diminutos, son partículas cuánticas y se comportan como ondas, donde la mitad de ellos pueden atravesar las paredes transportando la señal por canales donde no debería circular.

Por ello, el procesador cuando entra en el mundo cuántico deja de regir sus elementos, su física y su composición. En consecuencia, la computación digital tradicional, no tardaría en llegar a su límite, puesto que ya se han llegado a escalas de cientos de nanómetros. Surge entonces la necesidad de descubrir nuevas tecnologías y es ahí donde entra la computación cuántica.

Los computadores actuales codifican información utilizando números binarios (0, 1) y pueden hacer solo cálculos de un conjunto de números de una sola vez cada uno, las computadoras u ordenadores cuánticos codifican información como serie de estados mecánicos cuánticos tales como direcciones de los electrones o las orientaciones de la polarización de un fotón representando un número que expresaba que el estado del bit cuántico está en alguna parte entre 1 y 0, o una superposición de muchos diversos números de forma que se realizan diversos cálculos simultáneamente.

3.1. Descripción del computador cuántico

El computador cuántico se basa en procesamiento paralelo que por medio de superposición de estados, aprovecha la ventaja de los átomos, electrones entre otros elementos que poseen la virtud de estar en varios estados al mismo tiempo. Esta utiliza un principio básico de la mecánica cuántica por el cual todas las partículas subatómicas tienen una propiedad asociada llamada spin. El spin se asocia con el movimiento de rotación de la partícula alrededor de un eje. Esta rotación puede ser realizada en un sentido, o el opuesto. Por lo tanto se puede tomar cierto sentido 1 y el opuesto 0, es decir conllevando a llamarlos qubit.

Un ordenador cuántico funcionaría asociando el conocido carácter discreto del procesamiento de información digital (esto es, los bits) con el extraño carácter de la mecánica cuántica (niveles finitos de energía, estados atómicos

discretos). Así, una hilera de átomos de hidrógeno podría alojar qubits igual de bien que alojan bits una serie de condensadores. Un átomo en estado fundamental electrónico (el menor estado discreto de energía) podría ser la codificación de un 0, y en estado excitado un 1. Pero para que tal sistema cuántico pueda funcionar como un ordenador, no se debe limitar a almacenar qubits, sino que quien lo maneje ha de ser capaz de introducir información en el sistema, ha de procesar tal información mediante manipulaciones lógicas simples, y ha de poder devolver la información procesada: en conclusión han de poder leer, escribir y efectuar operaciones aritméticas.

La superposición cuántica, permite que un registro que contiene M qubits pueda representar 2^M valores simultáneos. Al realizar un cálculo utilizando este registro se producen todos los resultados posibles para los 2^M valores de entrada obteniendo así un paralelismo exponencial. Sin embargo para leer los resultados de un cálculo los qubits deben ser medidos. Esta medida hace que el qubit tome un valor particular y se destruya el estado paralelo (decoherencia). El desafío es entonces inventar cálculos cuánticos donde una propiedad pueda derivarse del estado paralelo en un tiempo no exponencial antes de realizar una medida.

3.1.1 El Mundo miniatura de la computación cuántica

De acuerdo a lo expuesto previamente, los computadores están compuestos de elementos del orden escalar de nanómetro el cual este hace referencia a la milmillonésima parte de un metro. Un átomo es la quinta parte de esa medida, es decir, cinco átomos puestos en línea suman un nanómetro. Bien, pues todos los materiales, dispositivos, instrumental, que entren en esa escala, desde 5 a 50 ó 100 átomos es lo que llamamos Nanotecnología.

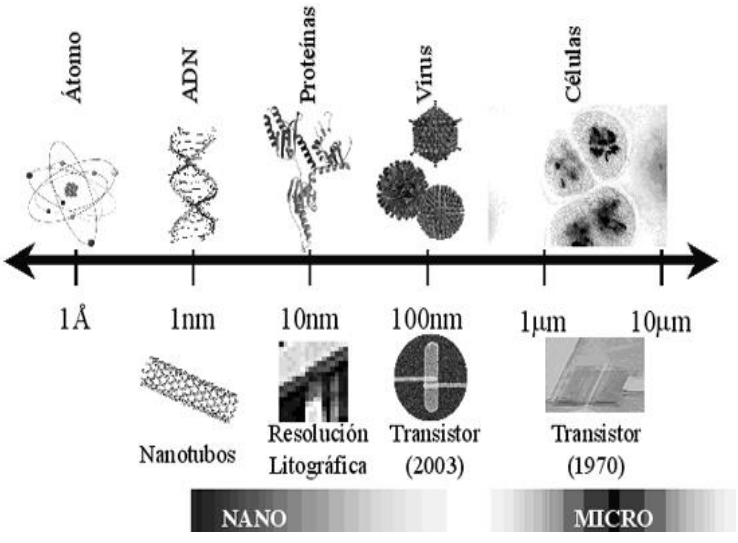

Figura 3. Escala del nanómetro.

En este figura se aprecia el tamaño de los elementos los cuales corresponde a cada unidad de medida en particular los elementos pequeños como iones cuánticos, puntos cuánticos, entre otros hacen parte de la escala del nanómetro. Estos son fácilmente manipulables y óptimos para el procesamiento de datos a nivel cuántico. Indicando una relación inherente entre la computación cuántica y la nanotecnología.

3.2. Ilustración del comportamiento cuántico

Para comprender claramente la ventaja de un computador cuántico se toma el siguiente ejemplo [6]: Se tiene un automóvil el cual diferentes compradores lo desean y difieren en cuanto al a sus características. Para identificar las características del automóvil se dan las siguientes posibilidades:

a -> 0 es blanco o 1 es negro

b -> 0 es tres (3) puertas o 1 es cuatro (4) puertas

c -> 0 es sedan o 1 es deportivo

Representando de esta manera el cero y uno como bits, en los computadores clásicos en el momento de relacionar las preferencias de cada comprador en potencia, se necesitan de 8 automóviles para entregar el indicado al comprador opcionado.

Las posibilidades son:

Tabla 1. Posibilidades de la compra del automóvil

A	B	C	Descripción
0	0	0	Blanco, 3 puertas, sedan
0	0	1	Blanco, 3 puertas, deportivo
0	1	0	Blanco, 4 puertas, sedan
0	1	1	Blanco, 4 puertas, deportivo
1	0	0	Negro, 3 puertas, sedan
1	0	1	Negro, 3 puertas, deportivo
1	1	0	Negro, 4 puertas, sedan
1	1	1	Negro, 4 puertas, deportivo

Por consiguiente se necesitan de estas combinaciones para su entrega elegida. Sin embargo con el computador cuántico no se necesitan de estas 8 posibilidades. Si se colocase una manta sobre este automóvil se desconocería el estado en que se encuentra este. Pero cuando conocemos el comprador elegido y se quita la manta del carro, se notará que las características dadas del automóvil destapado son las que se relacionan con el comprador. Concluyendo que el computador cuántico solo necesitaría de un automóvil para entregarlo con las características dadas. Esto sucede ya que cuando se cubre el automóvil con la manta entra en una superposición de estados,

es decir, se encuentra en las 8 posibilidades simultáneamente que se mencionaron anteriormente. Ya que aprovecha las condiciones de la superposición de estados de mantenerse en varios al mismo tiempo pero que en el momento de ser medidos son ajustados según lo determinado.

De hecho se da a conocer que si se tiene 8 combinaciones de 3 bits sería: 000, 001, 010, 100, 101, 110, 111 y solo una de ellas en los computadores clásicos se puede escoger de estas 8 combinaciones, en tanto que con solo 3 qubits (a, b, c) podemos tener esas mismas combinaciones en un mismo instante.

De esta manera se habla de exponencialidad en cuanto a que la superposición cuántica, permite que un registro que contiene n qubits pueda representar 2^n valores simultáneos.

3.3. Bit cuántico

Un qubit es la unidad mínima de información cuántica. Sus dos estados básicos se llaman, convencionalmente, |0> y |1> (se pronuncian: ket cero y ket uno). Un estado qubital puro es una superposición cuántica de esos dos estados. Esto es significa que el qubit se representa como una combinación linear de |0> y |1>.

Esta superposición es una coherencia en las que en el caso dos ondas se comportan como una sola onda.

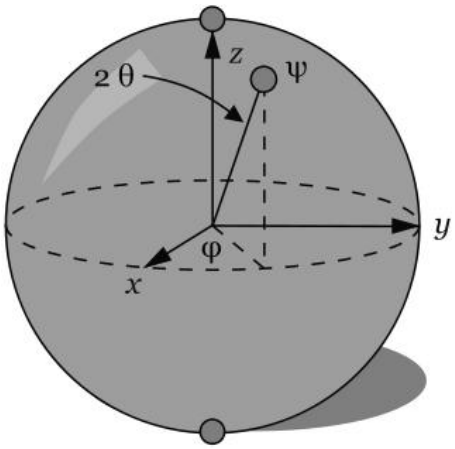

Figura 4. Representación gráfica del qubit.

Es decir la representación del qubit como vector sería:

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

Y su combinación lineal [8], es:

$$|\psi>=\alpha|0>+\beta|1>.$$

Donde alfa α y beta β son coeficientes complejos y satisfacen $|\alpha|^2>+|\beta|^2=1$.

Leyendo un qubit en la superposición de la ecuación, contiene a cero (0) como probabilidad de $|\alpha|^2$ y $|\beta|^2$ a uno (1) con la probabilidad.

En la práctica, la información podría ser soportada en una superposición de estados de un registro de muchos qubits.

En resumen, se habla de computadores u ordenadores cuyo comportamiento es determinado de forma importante por leyes de la mecánica cuántica. El sistema descrito está formado por bits cuánticos (quantum bits) o qubits, y pueden ser por ejemplo: núcleos, puntos cuánticos semiconductores y similares.

De hecho se ha probado que un ordenador con un tipo de registros cuánticos como los presentados anteriormente puede realizar en un mismo paso computacional la misma operación matemática que la que se realizaría con 2L inputs de números. En cambio para realizar la misma tarea, un ordenador clásico debería repetir el cálculo 2L veces, o debería utilizar 2L procesadores diferentes trabajando en paralelo. Esto representa una notable ganancia en el uso de recursos computacionales, tales como tiempo y memoria.

3.4. Compuesrtas cuánticas

Una de las ventajas considerables en el mundo cuántico es el de las compuertas cuánticas que manejan el principio de reversibilidad y universalidad, lo cual esto indica que cuando se trabaja con una compuerta CNOT u otra compuerta cuántica al conocer el resultado de los estados se puede determinar cuales fueron los estados ingresados, ajustándose al principio de reversibilidad y universalidad en cuanto a la aplicabilidad para mas qubits.

3.4.1 Compuerta de 1 Qubit

La compuerta de Hadamard. Esta compuerta existe en su versión de 1 qubit y de n qubits. En particular para 1 qubit la compuerta es:

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

De tal forma que

$$H^2=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\times\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}=I$$

Por el momento basta observar que aplicar la compuerta de Hadamard a un qubit nos da una superposición entre los valores $|0>$ y $|1>$.

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

La compuerta de Hadamard es sumamente útil para efectuar paralelismo cuántico, ya que al quedar en un estado superpuesto cualquier algoritmo que se calcule sobre el resultado de la compuerta de Hadamard se efectuara para todos las posibles configuraciones de entradas.

3.4.2 Compuerta de 2-Qubits

Compuerta CNOT (Negación Controlada)

La compuerta más común de 2 qubits es la compuerta CNOT. Esta compuerta intercambia el valor del segundo qubit si el primer qubit es igual a 1.

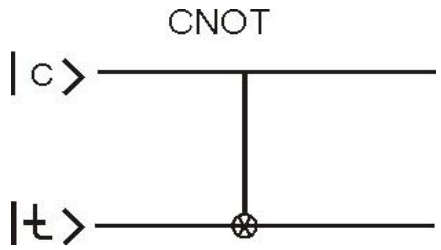

Figura 5. Compuerta CNOT.

Donde;

$$|c>=\alpha|0>+\beta|1>$$

$$|t>=\alpha'|0>+\beta'|1>$$

Este comportamiento da la tabla de verdad.

Tabla 2. Comportamiento Compuerta CNOT

Estados			
Entradas	$\|c>$	$\|t>$	Salidas
$\|00>$	0	0	$\|00>$
$\|01>$	0	1	$\|01>$
$\|10>$	1	0	$\|11>$
$\|11>$	1	1	$\|10>$

Si representamos estos valores $|00>|01>|10>|11>$ como sus respectivos vectores en C^4 tenemos que la matriz de transición de CNOT se construye a partir de productos directos de qubits dados en base computacional binaria.

Se tiene:

$$|0>=\begin{bmatrix}1\\0\end{bmatrix}\quad |1>=\begin{bmatrix}0\\1\end{bmatrix}$$, por lo tanto:

$$|00>=|0>\otimes|0>=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

$$|01>=|0>\otimes|1>=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$|11>=|1>\otimes|1>=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$|10>=|1>\otimes|0>=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

Lo cual indica que la transformación correspondiente es:

$$\begin{bmatrix}|00>\\|01>\\|11>\\|10>\end{bmatrix}=\begin{bmatrix}1000\\0100\\0001\\0010\end{bmatrix}*\begin{bmatrix}|00>\\|01>\\|10>\\|11>\end{bmatrix}$$

a) b) c)

a) Columna Estados de Salida

b) Matriz de CNOT

c) Columna Estados de Entrada

Donde la matriz b) es la representación matricial de la compuerta de CNOT.

El producto de ket c y ket t es:

$$|c>|t>=|ct>=(c|0>+c|1>)\otimes(t|0>+t|1>)$$
$$=|00>+|01>+|10>+|11>$$

3.4.2 Compuerta de 3-Qubits (Compuerta Toffoli)

La compuerta de Toffoli es una compuerta controlada con tres Qubits de entrada llamados: ket c, ket t y ket a, tal que la entrada c cambia de valor si las primeras 2 entradas son 1. Se puede interpretar como un CNOT con 2 qubits de control, es decir como compuerta.

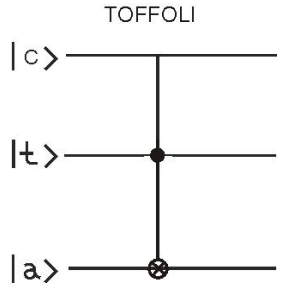

Figura 4. Compuerta TOFFOLI.

Donde;

$|c>=|0>+|1>$, $|t>=|0>+|1>$, $|a>=|0>+|1>$

Este comportamiento da la tabla de verdad.

Tabla 3. Comportamiento de Entrada y Salida de la Compuerta TOFFOLI.

	Estados			
Entradas	$\|c>$	$\|t>$	$\|a>$	Salidas
$\|000>$	0	0	0	$\|000>$
$\|001>$	0	0	1	$\|001>$
$\|010>$	0	1	0	$\|010>$
$\|011>$	0	1	1	$\|011>$
$\|100>$	1	0	0	$\|100>$
$\|101>$	1	0	1	$\|101>$
$\|110>$	1	1	0	$\|111>$
$\|111>$	1	1	1	$\|110>$

Si representamos estos valores $|000>|001>|010>|011>|100>|101>|111>|110>$ como sus respectivos vectores en C^8 tenemos que la matriz de transición de TOFFOLI se construye a partir de productos directos de qubits dados en base computacional binaria.

Se tiene:

$|0>=\begin{bmatrix}1\\0\end{bmatrix}$, $|1>=\begin{bmatrix}0\\1\end{bmatrix}$. Por lo tanto:

$$|000>=|0>\otimes|0>\otimes|0>=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}$$

$$|010>=|0>\otimes|1>\otimes|0>=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix}$$

$$|011>=|0>\otimes|1>\otimes|1>=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix}$$

$$|001>=|0>\otimes|0>\otimes|1>=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{bmatrix}$$

$$|110>=|1>\otimes|0>\otimes|0>=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix}$$

$$|101>=|1>\otimes|0>\otimes|1>=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\\0\\1\\0\\0\end{bmatrix}$$

$$|100>=|1>\otimes|0>\otimes|0>=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix}$$

$$|111>=|0>\otimes|1>\otimes|1>=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{bmatrix}$$

Lo cual indica que la transformación correspondiente es:

$$\begin{bmatrix}|000>\\|001>\\|010>\\|011>\\|100>\\|101>\\|111>\\|110>\end{bmatrix}=\begin{bmatrix}10000000\\01000000\\00100000\\00010000\\00001000\\00000100\\00000001\\00000010\end{bmatrix}*\begin{bmatrix}|000>\\|001>\\|010>\\|011>\\|100>\\|101>\\|110>\\|111>\end{bmatrix}$$

a) b) c)

a) Columna Estados de Salida

b) Matriz de Toffoli

c) Columna Estados de Entrada

donde la matriz b) es la representación matricial de la compuerta de Toffoli.

El producto de ket c, ket t y ket a es:

$$|c>|t>|a>=|cta>=(c|0>+c|1>)\otimes(t|0>+t|1>)\otimes(a|0>+a|1>)=$$
$$|000>+|001>+|010>+|011>+$$
$$|100>+|101>+|110>+|111>$$

En la siguiente figura se muestra como debería ser diseñada la compuerta cuántica CNOT a partir de las compuertas clásicas mediante un circuito que utiliza una compuerta AND y una XOR, para cumplir con las características de reversibilidad y universalidad y satisfaciendo la misma tabla de verdad.

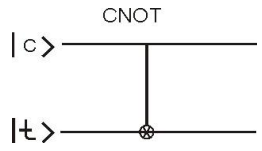

Figura 7. Compuerta CNOT

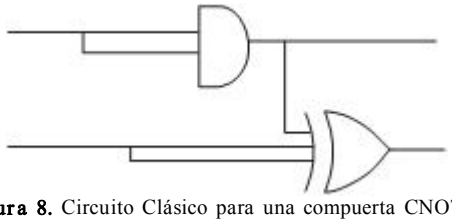

Figura 8. Circuito Clásico para una compuerta CNOT

En esta parte se muestra como debería ser diseñada la compuerta cuántica Toffoli a partir de la compuertas clásicas mediante un circuito que utiliza tres compuertas AND y una XOR, para cumplir con las características de reversibilidad y universalidad y satisfaciendo la misma tabla de verdad.

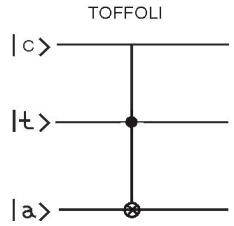

Figura 9. Compuerta TOFFOLI

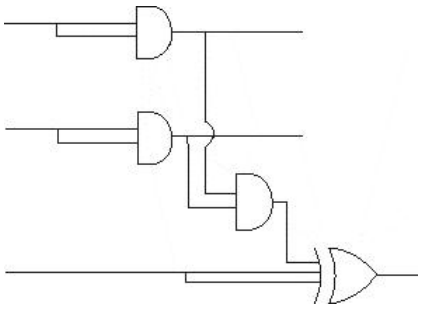

Figura 10. Circuito Clásico para una compuerta TOFFOLI

Las figuras nos indican que las compuertas cuánticas tienen ventajas significativas a partir de la potencia, espacio, características (reversibilidad y universalidad), funcionamiento; ya que para compararlas se necesitan de la combinación de varias compuertas clásicas para poder simular el comportamiento cuántico.

3.4.3. Reversibilidad

Una compuerta que actúa sobre un único qubit efectúa una operación reversible, dado que al tratarse siempre de matrices unitarias, se puede encontrar la inversa. Así, a partir de la salida es posible obtener la entrada. Además si se pretende que la dimensión del espacio de los estados de salida coincida con la de los de entrada, se debe mantener siempre todas las líneas.

3.5. Factorización cuántica

La criptografía es utilizada para codificar las transacciones de los bancos, gobiernos y militares. El método de encriptación es ampliamente empleado es un DES (Encriptación Estándar de Datos) basado en RSA. La RSA es llamada así por los inventores Ronald Rivest, Adi Shamir y Leonard Adleman y su sistema de clave pública de encriptación. El éxito de RSA depende de la intratable solución del problema de encontrar factores primos de grandes números enteros. Cuando este sistema fue inventado sus creadores retaron a cualquiera que fuese capaz de factorizar un número de 129 dígitos, conocido como RSA-129. Este reto fue relegado en 1994 por medio de 1600 computadores unidos en la web fueron capaces de determinar los factores en tan solo 8 meses. A pesar de esto, los criptógrafos emprendieron una nueva tarea de crear más dígitos a sus códigos. El problema de factorizar los números empieza a crecer exponencialmente a medida que crecen más. Sin embargo, Shor [15] propone un algoritmo cuántico que es capaz de factorizar una RSA-129 en unos pocos segundos, si se puede construir un computador cuántico tan rápido como un computador clásico.

3.5.1. Método cuántico de shor para factorizar

La interpretación de diferentes universos es utilizada por Shor en su método de computación cuántica para extraer números primos de largos enteros, donde el registro de memoria es posicionado en una superposición de posibles enteros contenidos, seguidos de diferentes cálculos para ser realizados en cada universo. La computación se detiene cuando los diferentes universos interfieren uno con el otro debido a las secuencias repetidas de enteros que son encontradas en cada universo y a través de ellos. Aunque no hay una garantía para decir que los resultados son correctos, una subsecuencia de verificación puede ser realizada a este punto para identificar donde los números retornados son de hecho los factores primos de los grandes enteros dados.

Para factorizar un número *n*, especificar un número arbitrario de universos paralelos *p* y aleatoriamente seleccionar un entero x entre 0 y *n*. En cada universo, se eleva a *x* al número de universos paralelos. Se divide por *n* y se almacena en cada universo. Para el siguiente número en secuencia por cada universo, *x* es elevada al número último almacenado, dividido por *n* y almacenado nuevamente. Esto se hace en cada universo repitiendo la secuencia. Por ejemplo, *n* es 33, x = 7 (o < x < n) y p = 17 [9].

Considerando u_2 y u_5:

$$u_2 = \begin{matrix} 7^2 \bmod 33 = 16, 7^{16} \bmod 33 = 4, 7^4 \bmod 33 = 25, \\ 7^{25} \bmod 33 = 10, 7^{10} \bmod 33 = 1, \textit{ect.} \end{matrix}$$

$$u_5 = \begin{matrix} 7^5 \bmod 33 = 10, 7^{10} \bmod 33 = 1, 7^1 \bmod 33 = 7, \\ 7^7 \bmod 33 = 28, 7^{28} \bmod 33 = 31, \textit{etc.} \end{matrix}$$

Tabla 4. Descripción de una factorización cuántica utilizando el algoritmo de Shor.

Función realizada en un circuito cuántico basado en compuertas lógicas cuánticas

Universo paralelo / segundo registro cuántico

Primer registro cuántico

u_0	1	7	26	31	7	26	31	7
u_1	7	26	31	7	26	31	7	26
u_2	16	4	26	10	1	7	26	31
u_3	13	13	13	13	13	13	13	13
u_4	26	10	1	7	26	31	7	26
u_5	10	1	7	26	31	7	26	31
u_6	4	26	10	1	7	26	31	7
u_7	20	31	7	26	31	7	26	31
u_8	31	7	26	31	7	27	31	7
u_9	10	10	10	10	10	10	10	10
u_{10}	1	7	26	31	7	26	31	7
u_{11}	7	26	31	7	26	31	7	26
u_{12}	16	4	26	10	1	7	26	31
u_{13}	13	13	13	13	13	13	13	13
u_{14}	26	10	1	7	26	31	7	26
u_{15}	10	1	7	26	31	7	26	31

La frecuencia de repetir a través de los universos, la frecuencia vertical, *vf*es 10 y puede ser verificado examinando el u_0 y u_{10}, u_1 y u_{11}, u_2 y u_{12} y así sucesivamente. Esto es porque en cada universo la repetición de frecuencias comienza en el mismo punto y repite los mismos números. Mientras otros universos comparten los patrones de repetición, no comparten el mismo punto de partida. Este es la equivalencia de la computación cuántica para el comportamiento de ondas en cada universo. A continuación se realiza un cálculo $x^{vf/1}-1$, donde x es la arbitrariedad escogida entre 0 y n y vf es la frecuencia común entre los patrones de universos. Esto nos da $7^{10/2}-1(\mathrm{mod}\,33)$ el cual es 9. Ahora encontrando el gran común divisor de 9 y 33 nos da uno de los factores que es 3.

El método Shor no se garantiza para todos los trabajos, y si el número derivado no se convierte en un factor primo de *n*, el procedimiento se repite utilizando una *x* diferente. El método de Shor utiliza algoritmos rápidos para tomar un factor primo candidato de *n*, y determinando donde esta el factor primo.

3.5.2. El Algoritmo de Búsqueda de Grover

Otra aplicación de la potencia de la mecánica cuántica en la resolución de problemas computacionalmente pesados es la búsqueda de elementos en listas. El método es una variante del de búsqueda del periodo de una función. Con una lista desordenada, un sistema clásico de búsqueda no tiene otra forma de recorrerlas sino buscando el elemento por medio de repetidas comparaciones. Existen diferentes alternativas, que mejoran la ciencia de las búsquedas, pero cada una de ellas parte de situaciones particulares en las que rentabiliza el número de operaciones.

Un ejemplo relativo a la seguridad informática es una lista de contraseñas que habitualmente se almacenan encriptadas en algún archivo de sistema, de modo que cuando cualquier usuario teclea su contraseña esta se encripta de nuevo (con un coste computacional insignificante) y se compara con la versión encriptada de la lista. Desencriptar una contraseña codificada por ejemplo vía RSA, es actualmente un problema inabordable cuando la clave es suficientemente compleja. Las personas que pretenden acceder a un sistema protegido de esta manera sin permiso habitualmente optan por hacer un ataque por fuerza bruta, esto es, recorrer todas las combinaciones posibles de caracteres una por una hasta encontrar una que sea una contraseña. Esta búsqueda a menudo se enfoca de un modo diferente: teniendo en cuenta que muchas personas utilizan palabras con sentido en algún idioma, utilizan diccionarios, que no son otra cosa que bases de datos de palabras en algún idioma, que lleva mucho menos tiempo recorrer, de modo que por regla general el coste computacional de romper la seguridad de un sistema informático puede disminuir considerablemente. Si estas condiciones se rompen el algoritmo puede hacerse muy ineficiente. De esta forma, si ningún usuario utiliza una clave basada en lenguaje natural el intruso recorrerá el diccionario completo sin obtener resultados satisfactorios. Cuando no se sabe nada sobre una lista no hay motivo para escoger un enfoque en lugar de otro, salvo el de maximizar las posibilidades de éxito. Esto incluso conlleva hacer más pesada la computación, pues nos obliga a hacer todas las comparaciones posibles.

Desde la perspectiva de la mecánica cuántica podemos utilizar el algoritmo presentado por Grover en 1997. El problema que resuelve puede representarse del siguiente modo:

Se parte de una lista desordenada $\{X_i\}_{i=1}^{N}$, en la que se trata de localizar un elemento particular, $X_j = t$

Un algoritmo clásico, recorriendo una lista de N elementos requiere en promedio realizar N/2 comparaciones, el método de Grover necesitará sólo hacer $\sqrt{N}$ .Bennett demostró que esto es lo mejor que se puede hacer[3]. El método no supone trasladar el problema a una nueva clase en el sentido de peso de computación, pero sí supone una aceleración tanto más significativa cuanto mayor sea la lista.

3.5.3 Metodología para un Algoritmo Cuántico

La siguiente línea representa un acercamiento a la caracterización de la metodología para el diseño y desarrollo de los computadores cuánticos.

1. El problema debe ser expresado en una forma numérica, y si no, utilizar un método que deba ser empleado para convertirlo en dicha forma.
2. La configuración inicial debe ser determinada.
3. La condición final debe ser definida concisamente.
4. El problema debe ser manejable para poder dividirlo en subproblemas más pequeños.
5. El número de universos requeridos debe ser identificado.
6. Cada subproblema debe ser asignado a su universo.
7. La computación en los diferentes universos ocurre en paralelo.
8. Debe existir una forma de interacción entre los universos. La interferencia debe ser una solución en cualquier campo o debe generar una información para los universos con el fin de ser utilizado para localizar dicha solución.

IV. TENDENCIAS, PERSPECTIVAS Y DESAFÍOS

Aunque son muchos los retos que la ciencia debe afrontar, se han presentado diferentes alternativas las cuales son un acercamiento para sus posibles soluciones. Hoy en día muchas organizaciones privadas y gubernamentales están trabajando en el diseño y construcción de este ordenador cuántico, ya que se encuentran en una carrera contra el tiempo para construirlo debido a que la seguridad se verá afectada con este procesamiento paralelo el cual solo basta de unos cuantos milisegundos para descifrar una clave RSA-129 la cual a un computador actual le tomaría mas de ocho meses, describiendo un posible caos que podría desatar una inseguridad en las redes y sistemas de información las cuales necesitan de confidencialidad como para ser lo suficiente seguras.

De esta manera si se construye el ordenador en mentes criminales no solo afectaría la seguridad sino que tendrían el poder de responder y replantear soluciones a enigmas que no son lo suficientemente claros y descritos por la ciencia. Es clara la realidad que vive la ciencia por implementarlo y de las organizaciones por las cantidades exorbitantes de dinero que destinan para este elemento, aún no se sabe cuando se podrá disponer de este computador se calcula que en unos 25 a 35 años se tendrían en cada hogar del mundo, por el momento solo se debe esperar a que la ciencia avance lo necesario como para resolver cuestionamientos que aún no poseen soluciones efectivas.

Actualmente el problema de crear un computador cuántico es de mantener su estabilidad en el tiempo, donde cada físico al agregar un qubit más la tarea de ingeniería se hace más laboriosa. Al agregar más qubits se hace más vulnerable el factor de la decoherencia, en donde el estado del qubit se degrada. La decoherencia puede ser ocasionada por las interacciones con el mundo y se generan problemas para mantener la coherencia en el sistema por más de varios segundos. Sin embargo se han dado varios progresos, en 1995 en la US Instituto Nacional de Estándares y Tecnología se construyó la primera compuerta cuántica de dos qubits y en el 2005 un equipo liderado por el profesor Rainer Blatt en el Instituto de Física Experimental en Austria construyó un prototipo de computador cuántico utilizando unos pocos iones de calcio. Su grupo estaba en un nivel de enredamiento de ocho iones de calcio, lo máximo [9].

El National Institute of Standards and Technology dispone de un programa específico de computación cuántica que al igual que el de la prestigiosa Universidad de Yale pretenden ofrecer avances reales en este complicado campo que podría revolucionar la informática a medio plazo. Por primera vez se ha conseguido unir dos de esos procesadores cuánticos mediante un enlace de circuitos superconductores, creando una cavidad a través de la cual se transmitían los datos cuánticos. Para lograr las propiedades de superconducción todo el dispositivo fue enfriado a bajas temperaturas. La importancia de este descubrimiento reside en el hecho de que este tipo de bus cuántico será utilizado con mucha probabilidad en los computadores cuánticos del futuro - o al menos, será la base de los futuros buses de comunicación - y ahora centrarán sus investigaciones en la estabilidad de las comunicaciones con más de 6 qubits, que fue la referencia inicial que sí funcionó sin problemas.

La compañía D-Wave localizada en Burbany, Britrish Columbia. En Enero 19 del 2007 publicó su trabajo acerca de un prototipo viable comercial de computador cuántico. El prototipo, de acuerdo a D-wave, es un computador conformado por 16 qubits el cual fue demostrado en Febrero 17 de 2007 en el Museo de Historia Computacional en Mountain View, California.

Los mayores retos que tiene actualmente el computador cuántico es el asilamiento del qubit ya que cualquier contacto con su mundo macroscópico rompe la coherencia lo que haría posible hasta su mera observación, por lo tanto, es necesario mantener al qubit totalmente aislado para ello hay que retenerlo con una trampa iónica, es decir, mantenerlos suspendido entre campos magnéticos y ases de rayos lásers esto hace muy difícil imaginar que aspecto tendrá el computador cuántico.

4.1. Qubit físicos

La demostración más exitosa de la computación cuántica hecha hasta hoy, usó resonancia magnética nuclear (NMR) y siete núcleos de atómicos en un campo magnético para ejecutar la factorización de un algoritmo de cuatro números de bit como qubits. La mecánica cuántica permite dos posibles orientaciones del núcleo (spin ½) en un campo magnético. La NMR controla las interacciones de los qubits, sometiendo un par de núcleos a una radiación en una frecuencia específica a ellos. En este experimento, 21 controles diferentes de frecuencia fueron escogidos con una precisión de partes por millón, algo que muchas tecnologías no pueden igualar. La irradiación hace rotar el spin a una tasa finita, y su irradiación es apagada cuando alcanza la superposición deseada de estas dos posibles orientaciones. Sin embargo el método parece ser limitado por 10 qubits [8].

La tecnología de estado sólido ofrece una opción para manipular miles de qubits así como objetos complejos. La industria electrónica ha desarrollado métodos de interconexión de grandes números de dispositivos complejos en un substrato de silicio para fabricar diez millones de transistores en un chip. Muchos estudios de qubits de estado sólido se han enfocado en semiconductores, con el silicio el material elegido para los qubits semiconductores. En la práctica, los empresas construyen dispositivos de estado sólido sometiendo al silicio o sustratos similares a una serie de tratamientos físicos y químicos, a menudo a elevadas temperaturas. La creación de dispositivos en estado sólido describe el proceso en detalle. Controlando los parámetros que gobiernan el proceso, el resultado final genera incertidumbre en las características de los dispositivos sólidos disponibles a los usuarios [8].

4.2. Computación cuántica en el silicio

Una investigación de la propuesta de un computador cuántico en silicio [Keyes 2005-2] revela los problemas de imperfección que el procesamiento de dispositivos causa. La propuesta actual utiliza silicio tecnología de circuitos integrados para colocar una serie de spin 1/2 átomos de fósforo a una pequeña distancia debajo de la superficie de un sustrato de silicio. Los núcleos del fósforo son como qubits. Un campo magnético define los dos estados distinguibles para los spines de los electrones que el átomo nuclear P positivo cargó en trampas, y el campo interactúa con los electrones.

4.3. Dispositivos con superconductividad

Los experimentos con estos dispositivos proveen conocimiento esencial para el entendimiento de la física básica para las características cuánticas de los dispositivos macroscópicos. Un experimento con la caja de Colulomb, es tomado como una estructura con una capacitador tan pequeño que la energía que se necesita para adicionar un solo electrón a ella es la dominante energía en la operación de un circuito [8].

4.4. Comunicación en la computación

Los cálculos implican interacciones entre las diversos partes de un sistema. Los circuitos lógicos reciben información de otras partes del sistema. Las computadoras electrónicas necesitan de esquemas de interconexión para proveer comunicación cercana y lejana de fuentes y destinos. Algunas conexiones largas son necesarias, y la prestación del servicio es un aspecto difícil de la tecnología de circuito integrado [8].

La tecnología del estado sólido produce dispositivos en una plana superficie. Qubits vecinos sobre una superficie podrían interactuar el uno con el otro a través de la superposición de funciones de onda, o por medio de un enlace capacitivo, que se utiliza con superconductotes de qubits. Sin embargo, es difícil ver cómo proporcionar a lo largo de un punto a otro punto las conexiones que la computación cuántica requiere [8].

4.5. Decoherencia cuántica

La computación cuántica se enfrenta a otro problema. La decoherencia, una interacción no deseada de la información cuántica con entidades ajenas, es un peligro de la informática cuántica en el sentido de que se destruye la información que el sistema está procesando. Los investigadores han propuesto un método de corrección de errores que compara qubits redundantes cada paso para luchar contra la decoherencia. Sin embargo, la aplicación de corrección de errores en la computación cuántica aumenta sustancialmente el número de dispositivos necesarios y el número de pasos de procesamiento por uno en dos órdenes de magnitud. Por lo tanto, un mínimo de nivel de precisión en las operaciones será necesario para la corrección de errores a converger [8].

Sin embargo hay una limitación para observar los resultados de cada archivo computacional distribuido ya que se encuentran en diferentes universos. Si una observación es realizada el universo colapsa y los resultados del otro universo se pierden. Las técnicas computacionales las cuales exploran el paralelismo cuántico deben llegar con una observación de métodos que aseguren que el universo colapsado en la observación de alguna manera representa la solución del problema o tiene la suficiente información para permitir diferentes soluciones [10].

V. CONCLUSIONES

Las ventajas que tiene el computador cuántico desde su procesamiento en paralelo a nivel exponencial hasta el

almacenamiento de grandes cantidades de información son asombrosas, sin embargo se tienen todavía falencias para su construcción uno de los elementos mas importantes en este caso son los procesadores cuánticos los cuales deben ser mejorados no solo en la parte del hardware de los computadores sino también el software de cada uno de ellos es decir una reconstrucción total, conllevando a la innovación de criptografia, seguridad, redes, entre otros elementos que hacen parte del manejo de la información en los computadores.

Dentro del hardware se encuentran otros elementos como las compuertas cuánticas ya que juegan un papel fundamental en el desarrollo del ordenador cuántico, pero persiste la búsqueda de elementos de superconductividad lo suficiente apropiados como para ser implementados.

En la actualidad el mundo cuántico es un universo complejo y se tienen una gran cantidad de retos los cuales la ciencia no ha podido resolver, se mencionan paulatinamente los diferentes avances que ha realizado la ciencia para su implementación y aunque se conocen las dificultades que puede afrontar el mundo de la información a nivel de confidencialidad y de seguridad se deben efectuar los procedimientos adecuados para enfocar la construcción e implementación de este computador cuántico en bien de la humanidad.

VI. REFERENCIAS

[1] Benioff P, Comment on Dissipation in, Phys. Rev. Lett. 53, 1203 (1984).
[2] Benioff P, Quantum Mechanical Hamiltonian Models of Computers, Ann. N. Y. Acad. Sci. 480, 475 (1986).
[3] CH Bennett, G Brassard, C Crépeau, R Jozsa, Teleporting an unknown quantum state via dual classical and Einstein - podolsky Rosen Channels, Phys. Rev. Lett. 70, 1895-1899 (1993).
[4] Deutsch D., A. Barenco, A. Ekert and R. Jozsa, Conditional quantum dynamics and logic gates, Phys. Rev. Lett. 74, 4083-6 (1995).
[5] Grover L, Quantum computing, The sciences, July/August 1999.
[6] Glassner A., Quantum Computing Part 1, Andrew Glassner's Notebook, July/August 2001.
[7] Keyes B., After the transistor, the Qubit?, IBM Research Division 2005.
[8] Keyes B., Challenges for Quantum Computing with Solid-State Devices, IBM Research Division January 2005.
[9] Knights Miya, The Art of Quantum Computing, January 2007.
[10] Narayanan A., Quantum computing for beginners, University of Exter, 1999.
[11] Nielsen M. and Chuang I., Quantum Computation and Quantum Information, Cambridge University Press.
[12] Quantum Algorithms and Hard Problems, Vidya Raj C., Phaneedra H. D., Dr. Shivakumar M.S., 2006.
[13] RP Feynman, Int. J. Theor. Phys. 21, 467.
[14] RP Feynman, Quantum Mechanical Computers Int. J. Theor. Phys. 16, 507.
[15] Shor P, Algorithms for quantum computation: Discrete logarithms and factoring, Proc 35th Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, Ed.), IEEE Computer Society Press (1994), 124-134.