Textos Científicos www.revista-nanociencia.ece.buap.mx ISSN 0188-6150

Inter*net* Electronic Journal
Nanociencia et Moletrónica

Diciembre 2003, Vol. 1; N°2, págs. 93-99

LA FÍSICA, EL CÁLCULO Y LA COMPUTACIÓN CUÁNTICA

M. Castro

Facultad de Ciencias de la Computación
Benemérita Universidad Autónoma de Puebla
14 Sur y Av. San Claudio edf. 135 Puebla, Pue. 72570
mcastro@cs.buap.mx
Otoño 2003

recibido: Noviembre 3, 2003 revisado: Diciembre 2, 2003 publicado: Diciembre 16, 2003

Citation of the article:
M. Castro, "La Física, el Cálculo y la Computación Cuántica", Internet Electrón. J. Nanocs. Moletrón. 2003, 1(2), 93-99:
http://www.revista-nanociencia.ece.buap.mx

LA FÍSICA, EL CÁLCULO Y LA COMPUTACIÓN CUÁNTICA

M. Castro

Facultad de Ciencias de la Computación
Benemérita Universidad Autónoma de Puebla
14 Sur y Av. San Claudio edf. 135 Puebla, Pue. 72570
mcastro@cs.buap.mx
Otoño 2003

recibido: Noviembre 3, 2003 revisado: Diciembre 2, 2003 publicado: Diciembre 16, 2003

Internet Electron. J. Nanocs. Moletrón. 2003, 1(2), pags. 93-99

Resumen

El desarrollo de la tecnología actual tiende a miniaturizar los circuitos empleados en la construcción de computadoras; sin embargo se ha establecido que ese proceso de miniaturización tiene laımites. Al llegar a niveles comparables con los tamaños de los átomos, las leyes y principios que rigen ya no son clásicos; estas leyes son las de la física cuántica. Desde la última década del siglo pasado ha comenzado a tomar auge la computación cuántica. Resulta que si tomamos en cuenta otro tipo de hardware, radicalmente diferente al hardware tradicional o clásico; entonces muchos problemas que hasta ahora se han considerado ”intratables”, tienen una solución si se consideran nuevos dispositivos computacionales subordinados en su funcionamiento a las leyes y principios de la física cuántica. En este trabajo tratamos de exponer los principios básicos de la computación cuántica.

Introducción

La teoría de la computación ha sido extensamente desarrollada durante las últimas décadas. Intuitivamente una computadora es un sistema físico que toma un conjunto de estados "entrada" y produce un conjunto de estados "salida". Estos estados son etiquetados en alguna forma canónica; la computadora es preparada en un estado con un etiquetamiento de entrada dado y, siguiendo alguna regla, luego se mide el estado de salida. En los sistemas clásicos determinísticos la medición de las etiquetas de salida es una función F de las etiquetas de entrada; además, los valores de estas etiquetas pueden ser en principio medidas por un observador externo. En este caso se dice que la computadora "calcula" la función F. ¿Que sucede si los dispositivos de las computadoras funcionan de acuerdo a las leyes de la física quántica? A pesar de que ya se había sugerido de que "algo nuevo" puede suceder cuando las computadoras se comportan de acuerdo a las leyes de la mecánica cuántica, no fue sino hasta que apareció el trabajo de Deutsch en 1985 [2] que los fundamentos de la computación cuántica fueron expuestas y formuladas teóricamente.

En su trabajo Deutsch considera el caso cuando las computadoras se comportan como sistemas quánticos; cuando los estados de estos sistemas se subordinan a la mecánica quántica y, por lo tanto, dejan de ser estados clásicos en el sentido meramente mecánico que le dieron Turing y Church.
El espín de una partícula puede ser el bloque fundamental de construcción de una computadora cuántica. Podríamos llamarlo como un qubit, para denotar que es análogo en algunas formas a un bit en una computadora clásica. Así como un registro de memoria en una computadora clásica es un arreglo de bits, un registro de memoria cuántica esta compuesta de varios espines de partículas de 1/2, o qubits. Como la proyección del spin de una partícula solo puede estar en dos estados, el llamado up ↑ y el estado down ↓ entonces, podemos designar al primero con el bit 0 y al segundo con el bit 1. Hay otras representaciones posibles para el qubit. En adelante, cuando hablemos de un qubit vamos a entender a este como las dos posibles proyecciones del spin en el sentido explicado arriba.
Las diferencias entre un bit clásico y un qbit se pueden plantear de la siguiente manera:
Un bit clásico almacenado en algún dispositivo o procesado por este es 0 o 1; sin embargo según la computación quántica un bit (llamado qubit) puede estar en una superposición de los estados 0 o 1 (se dice que con determinada probabilidad esta en "0" o en "1").
El estado de salida de una computadora cuántica, aunque esta completamente determinado por su estado de entrada, no es observable en el sentido clásico; esto es, un usuario no puede ver las etiquetas de salida sin perturbar al resultado mismo. El resultado de un proceso de cálculo en una computadora cuántica tiene un carácter probabilística y se obtiene mediante una medición sobre el sistema.
Con el fin de darle una forma más conceptual a estas ideas, vamos a dar algunas definiciones útiles en la comprensión del funcionamiento de las computadoras cuánticas.

Acerca del Formalismo de la Computación Cuántica

Una computadora cuántica es un modelo de computación basado en la mecánica quántica; por lo tanto, el formalismo que se necesita para formular las bases de la computación cuántica deberá, de igual forma, representar los estados y transformaciones cuánticas, como vectores y operadores en un espacio vectorial complejo. A continuación veremos algunas definiciones y reglas de los mecanismos cuánticos.
Como hemos establecido, el estado de un sistema quántico es representado por un vector en algún espacio vectorial H^n, donde n es la dimensión del espacio y a H se le denomina espacio de Hilbert.

Definición: *Un bit Cuántico o qubit es un vector normalizado* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ *en* H^2. *Donde* α *y* β *satisfacen la igualdad* :

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

En forma matricial los vectores |0> y |1> se escribirán:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} y\, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Los números $||\alpha||^2$ y $||\beta||^2$ son las probabilidades que el estado $|\psi>$ se encuentre en los estados |0> y |1> respectivamente. Donde |0> y |1> son estados que representan a una partícula con espines ↑ y ↓ respectivamente.

A diferencia de la computación clásica en la cual un bit tiene sin ambigüedad o el valor de "0" o el valor de "1", en computación cuántica los estados |0> y |1> son observados con cierta probabilidad: Un qubit lo podemos pensar como una superposición de esos dos estados.
Un bit clásico puede ser medido sin perturbarlo, sin embargo, un qubit es sensible a la medición. La medición destruye al estado original (en mecánica quántica se dice que la medición "colapsa" el estado).
Supongamos que nosotros hacemos la medición de un sistema que esta en el estado:
|ψ□=α|0□+β|1□ y como resultado obtenemos el bit 0 (la probabilidad de haber obtenido este resultado es ||α||²) lo cual quiere decir que después de la medición el estado del sistema queda en |0□. Ahora, si medimos otra vez debemos estar seguros que la medición dará 0 (con probabilidad uno).
La evolución de un sistema quántico debe ser unitaria, puesto que se debe conservar la norma del vector en el espacio lo que significa que no debe cambiar la distribución de las probabilidades.

Definición : Una transformación unitaria viene dada por un operador unitario que actúa en un espacio vectorial H^n. Esto significaquesedebensatisfacerlassiguientespropiedades

1.– $U : |\psi\rangle \rightarrow |\phi\rangle \; donde \; |\psi\rangle \; y \; |\phi\rangle \in H^n$

2.– $\langle\phi|\psi\rangle = \langle U\phi|U\psi\rangle \forall \phi,\psi \in H^n$

Para representar grupos de qubits, nosotros usaremos la noción de producto tensorial de espacios vectoriales; así, si tenemos un grupo de qubits en H^m y otro grupo en H^n entonces el espacio resultante será $H^{mn} = H^m \otimes H^n$, donde el símbolo " $\otimes$ " denota al producto tensorial.
El producto tensorial de dos matrices se define de la siguiente forma:

Si las matrices A y B las representamos como

$$A = \begin{pmatrix} a_{11} & a_{12} & . & . & a_{1n} \\ a_{21} & a_{22} & . & . & a_{2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{m1} & a_{m2} & . & . & a_{mn} \end{pmatrix} \; y \; B = \begin{pmatrix} b_{11} & b_{12} & . & . & b_{1l} \\ b_{21} & b_{22} & . & . & b_{2l} \\ . & . & . & . & . \\ . & . & . & . & . \\ b_{k1} & b_{k2} & . & . & b_{kl} \end{pmatrix}$$

entonces el producto tensorial de A y B será:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & . & . & a_{1n}B \\ a_{21}B & a_{22}B & . & . & a_{2n}B \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{m1}B & a_{m2}B & . & . & a_{mn}B \end{pmatrix}$$

o sea que como resultado tenemos una matriz de m□k filas y n□l columnas.
Podemos ahora dar una definición de registro quántico.

definición: Un registro quántico de n qubits es un vector normalizado en $H^{\otimes n} = H^{2^n}$ y puede ser expresado como una combinación lineal de los vectores base $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ con la restricción que $\sum_{i=0}^{2^n-1} \alpha_i^2 = 1$

Este vector es un producto tensorial de los qubits de la forma:
$|a_1 a_2 \cdots a_i \cdots\rangle = |a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_i\rangle \otimes \cdots$

Cuando tratamos con sistemas que son productos tensoriales de sus partes, debemos tomar en cuenta el efecto que puede producir, sobre el sistema, las transformaciones hechas a una de sus partes; para comprender esto introducimos la noción de estado ligado (entanglement)

definición: Decimos que un registro cuántico esta ligado (entangled) si no puede ser expresado como el producto tensorial de sus partes.

Por ejemplo si tenemos el estado:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

|>=(1/(√2))(|01□+|10□)
no puede ser expresado como el producto de dos estados puros $|\psi_1\rangle$ *y* $|\psi_2\rangle$ *o sea como* $|\psi_1\rangle \otimes |\psi_2\rangle$ |.

Cuando un sistema esta ligado sus partes están correlacionadas y todo lo que hagamos en una de sus partes influirá en la otra; así, si nosotros hacemos una medición sobre una parte del sistema anterior obtenemos con probabilidad 1/2 el estado |01□ o el estado |10□ o sea si lo que medimos fue el primer qubit, entonces obtenemos con probabilidad de 1/2 0 o 1, pero una vez hecha la medición la otra parte del sistema quedo con la certeza de tener 1 en el primer caso y 0 en el segundo.

Con los conceptos de registro cuántico y transformación unitaria podemos introducir la noción de cálculo en un procesador quántico: Si se tiene un registro quántico en el estado: $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ y un conjunto de transformaciones unitarias U_k un cálculo cuántico se realizara en los siguientes pasos:

1. Se prepara el registro cuántico en un estado conocido.
2. Se aplica una transformación unitaria al estado.
3. Se realiza una medición al estado final para leer el contenido.

Las transformaciones unitarias deben realizar las operaciones deseadas sobre el registro quántico y se les llama comúnmente compuertas quánticas. A estos operadores se les llama compuertas puesto que al actuar sobre los qubits realizan operaciones equivalentes a las operaciones lógicas de las compuertas en los sistemas digitales.

Las operaciones básicas que se conocen son las siguientes:

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|$$
$$X = |0\rangle\langle 1| + |1\rangle\langle 0|$$
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$
$$Y = |0\rangle\langle 1| - |1\rangle\langle 0|$$
$$H = \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|]$$

donde **I** es la operación de identidad, **X** la operación NOT, **Z** operación I con cambio de face, **Y** operación NOT con cambio de face y **H** es la llamada trasformada de Hadamard.
Las operaciones que aparecen en estas transformaciones las vamos a entender de la siguiente manera:

$$|a\rangle\langle b| = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}\begin{pmatrix} b_1 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 & a_1 b_2 \\ a_2 b_1 & a_2 b_2 \end{pmatrix}$$

Entonces los operadores anteriores serán

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};\ Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};\ H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Un par de qubits lo vamos a representar como un vector en el espacio generado por el producto tensorial de dos espacios de Hilbert H² o sea $H^2 \otimes H^2$ y los vamos a simbolizar de la siguiente manera:

$$|00\rangle = |0\rangle \otimes |0\rangle$$
$$|01\rangle = |0\rangle \otimes |1\rangle$$
$$|10\rangle = |1\rangle \otimes |0\rangle$$
$$|11\rangle = |1\rangle \otimes |1\rangle$$

De todos los posibles operadores que actúan sobre un par de qubit se encuentra uno de particular importancia; el llamado CONTROL-U

$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$, y se le llama así porque la acción sobre el segundo qubit esta controlada por si el primer qubit esta en el estado $|0\rangle$ *o* $|1\rangle$|0> si **U=X** entonces tenemos la llamada CONTROL-NOT o CNOT cuyo efecto sobre las diferentes combinaciones de pares |ij> es:

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |11\rangle$$
$$|11\rangle \rightarrow |10\rangle$$

Entonces, la acción de la transformada CNOT es como sigue: si el primer qubit es 0, el segundo qubit queda igual y si el primer qubit es 1 entonces el segundo qubit es la negación del segundo qubit de entrada.
En términos generales $|ab\rangle \rightarrow |a\rangle|a \oplus b\rangle$ donde el símbolo "⊕" denota la operación OR-exclusivo o XOR; por esta razón, a esta transformada se le llama también compuerta XOR.

Para representar otras operaciones se necesitan más qubit; este es el caso de la operación "and" la cual necesita de tres qubit y es como sigue:

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

Con más detalle, esta compuerta quedaría expresada de la siguiente forma:

$$|0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)$$

El tercer qubit experimenta un NOT si y solo si los dos primeros están en el estado 1. Esta compuerta recibió el nombre de Toffoli (1980) [3]. Si nosotros iniciamos el estado con el tercer qubit en 0 entonces, la compuerta Toffoli calcula un "and" de los dos primeros qubit o sea $|ab0\rangle \rightarrow |a\rangle \otimes |a \cdot b\rangle$ donde "a.b" simboliza la operación "and" lógica.

La tabla se vería de la siguiente manera:

$$|000\rangle \rightarrow |000\rangle \quad |001\rangle \rightarrow |001\rangle$$

$$|010\rangle \rightarrow |010\rangle \quad |011\rangle \rightarrow |011\rangle$$

$$|110\rangle \rightarrow |111\rangle \quad |111\rangle \rightarrow |110\rangle$$

Como podemos ver las primeras cuatro implementan la operación lógica "and".

Conclusiones

Como se puede ver de los desarrollos anteriores, es posible usando los principios de la física cuántica realizar las principales operaciones lógicas que son comúnmente utilizadas en el computo. No fue si no hasta la última década del siglo pasado que quedaron claras las potencialidades de las computadoras cuánticas y se exhibieran problemas específicos que se consideraban intratables en la computación clásica, pero que pueden resolverse eficientemente en una computadora cuántica. El mas claro ejemplo es el problema de factorización. Shor mostró en su trabajo [2] que usando un algoritmo quántico (o sea un algoritmo que corre en una computadora quántica) es posible descomponer un número entero largo en sus factores primos. Este problema fue considerado intratable en cualquier computadora clásica y Shor mostró que la clase de problemas accesibles a las computadoras cuánticas incluyen problemas que no pueden ser eficientemente resueltos por computadoras clásicas.

Bibliografía

[1] M. A. Nielsen y I. L. Chuang, Quantum Computation and Quantum Information Cambrige University, Press Cambrige, Inglaterra, 2002.
[2] Adrew Steane, Quantum Computing, quant-ph/708022 v2 Sep. 1997
[3] Peter W. Shor, Polinomial-Time Algorithms for Prime Factorization and Discrete Logarithm on a Quantum Computer, quant-ph/508027 v2 Jan 96.
[4] Deutsch David, Quantum Theory the Church-Turing Principle and the Universal Quantum Computer, Proceeding of the Royal Society of London A 400, pp. 97-117 (1985)
[5] Toffoli Tomas, Reversible Computing Seventh Colloquium on Automata, language and Programming, Eds. Springer, Berlin (1980)