Computación Cuántica

Rolando Saniz Balderrama

Departamento de Ciencias Exactas
Universidad Católica Boliviana, Regional Cochabamba
e-mail: saniz@ucbcba.edu.bo

1 Introducción

Todas las computadoras de hoy en día, desde la máquina que usa una persona en un café Internet para revisar su casilla electrónica, hasta las máquinas de última generación utilizadas por los investigadores en el CERN (Centro Europeo de Investigación Nuclear), cerca de Ginebra, en Suiza, son máquinas de Turing. Desde ese punto de vista, no son más sofisticadas que la Máquina Analítica de Charles Babbage de los años 1830. Todas obedecen al mismo principio, el de la Máquina Universal de Turing. En la actualidad, las computadoras más avanzadas siguen siendo máquinas que operan de manera sequencial sobre las operaciones elementales en que los programas dividen las tareas que se quieren ejecutar. Las llamadas supercomputadoras "paralelas", al fin y al cabo, no son más que varias máquinas trabajando en conjunto de cierta manera, y cada una de manera sequencial. El problema es que ese principio de funcionamiento limita seriamente las tareas computacionales que se pueden ejecutar. No se pueden atacar, por ejemplo, problemas grandes fuera de la clase P. Recordemos que un problema de la clase P es aquel para el cual el mejor algoritmo tiene un tiempo de ejecución polinomial en función del tamaño del input. La factorización de un número entero, por ejemplo, no está en P. No se dice que una factorización es imposible de realizar, ya que una computadora cualquiera puede, en principio, emprender la tarea, sino que para factorizar un entero grande se requiere tal capacidad de cálculo que, desde el punto de vista práctico, se puede considerar la tarea irrealizable.

A esto se añade otro problema, que se va haciendo más importante con el paso del tiempo. Desde el punto de vista físico, las computadoras actuales están basadas en un tipo de transistor, el CMOSFET, del inglés Complementary Metal Oxide Semiconductor Field Effect Transistor. Mucho del progreso en la capacidad de las computadoras se debe a la miniaturización de los componentes en un chip, gracias a los avances de la tecnología litográfica. Actualmente, por ejemplo, se pueden realizar compuertas lógicas y conexiones cuyo tamaño está por debajo del micrón (milésima de milímetro). En 1965, Gordon E. Moore, entonces de la compañía Fairchild Semiconductor, hizo notar que el número de transistores en los microprocesadores se estaba multiplicando

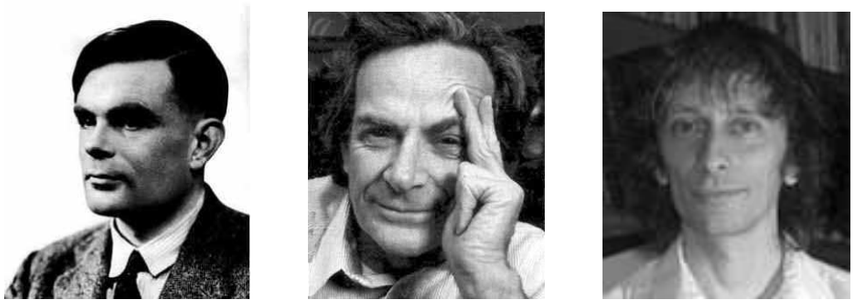

Figura 1: Alan Turing, Richard Feynman y David Deutsch: de la computadora universal a la computadora cuántica universal.

aproximadamente por 4 cada 3,4 años. Sorprendentemente, la observación de Moore sigue siendo válida hoy, habiéndose popularizado como la "ley de Moore". Pero esta tendencia no podrá continuar indefinidamente. Aparte de la limitación fundamental de que no se podrán hacer reducciones por debajo de la escala molecular o atómica, los problemas técnicos planteados por la miniaturización se tornan cada vez más difíciles de resolver. De acuerdo a Joel Birnbaum, Director Científico de Hewlett Packard, esto se refleja en la "segunda ley de Moore", que indica que el costo de producción se ha estado multiplicando por 4 cada 2 años, es decir, mucho más rápido que el incremento de capacidad de las computadoras. Esto puede causar el fin de la ley de Moore, porque no se podrán justificar grandes inversiones en investigación, desarrollo y manufactura de una tecnología sólo marginalmente mejor [1].

Es por estas razones que muchos investigadores buscan construir computadoras basadas en un nuevo paradigma tecnológico y un nuevo principio computacional. Una de las corrientes más importantes es la de la computación cuántica. La idea de la computación cuántica fue introducida por primera vez en 1982, por Richard Feynman (premio Nobel de Física en 1965), cuando consideró la simulación de sistemas en mecánica cuántica por otros sistemas cuánticos [2]. Sin embargo, la computación cuántica quedaba en un plano hipotético y no fue hasta 1985 que se logró un avance fundamental en esta dirección, con la publicación de David Deutsch, del Departamento de Física de la Universidad de Oxford, del artículo en el que describía una computadora cuántica universal [3], probablemente haciendo pasar a la historia la máquina universal descrita por Alan Turing, en Cambridge, en los años 30 [4].

Si bien las computadoras cuánticas no son aún una realidad, se han dado pasos importantes tanto en el desarrollo de bits cuánticos y compuertas lógicas cuánticas como en el desarrollo de algoritmos cuánticos. En la siguiente sección se tratará del principio en el que se basa la computación cuántica y de cómo funcionaría.

2 Bits cuánticos y paralelismo cuántico

Las computadoras actuales, o clásicas, tienen como unidad básica el bit. Este puede estar en uno de dos estados, convencionalmente 0 ó 1. En una computadora cuántica,

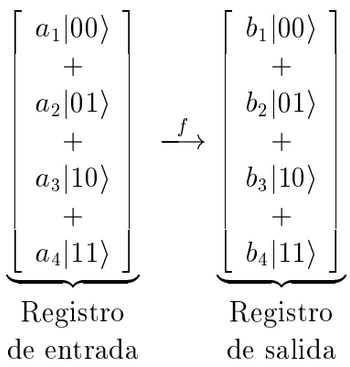

Figura 2: Un qubit en el registro de entrada estará dado por una combinación lineal de cuatro estados, cada uno con cierta amplitud de probabilidad a_i. Una operación f sobre el qubit lleva a un registro de salida en el que las cuatro amplitudes de probabilidad habrán cambiado, en un sólo paso.

en cambio, un bit cuántico, o "qubit", como se le ha venido a llamar en abreviación de "quantum bit", puede estar no sólo en uno de los estados 0 ó 1, sino que también puede estar en una superposición de ambos. En mecánica cuántica, en general, un sistema tiene acceso a un número discreto de estados—que puede ser infinito, y puede ser "preparado" experimentalmente en uno de esos estados o en una superposición de dos o más de entre ellos. Este es el elemento fundamental en la idea de computadora cuántica de Deutsch y el origen de su enorme potencial. Supongamos que se tiene un registro físico de ocho bits. En una computadora clásica se puede almacenar sólo uno de los 256 (2^8) números dados por las configuraciones $00000000, 10000000, 01000000\ldots$, etc. En cambio una computadora cuántica puede almacenar los 256 números a la vez. Más aún, puede operar sobre los 256 números a la vez. Obviamente el operar sobre los 256 números en un solo paso reduce el tiempo de cálculo de manera radical respecto a una máquina clásica, que tiene que operar sobre cada número, del 0 al 255, uno después del otro. Las computadoras cuánticas poseen, pues, un paralelismo intrínseco, diferente al de las máquinas paralelas actuales que, como se observó más arriba, siguen siendo máquinas sequenciales. En la Fig. 1 ilustramos cómo se opera en paralelo sobre los cuatro números de un qubit hecho de dos bits físicos.

El gran potencial de la computación cuántica fue finalmente puesto en evidencia, y de manera contundente, cuando Peter Schor, de los AT&T Bell Laboratories, publicó en 1994 un algoritmo de factorización en tiempo polinomial para computadoras cuánticas [5]. El número más grande que las supercomputadoras clásicas han logrado factorizar tiene 140 dígitos. Se ha estimado que factorizar un número de 1000 dígitos tomaría alrededor de 10^{20} años, i.e., 10 mil millones de veces la edad del Universo (que tiene, en principio, alrededor de 15 mil millones de años). El algoritmo de Shor, en cambio, permitiría factorizar un número de 1000 dígitos en aproximadamente media hora [6]. Dicho esto, es importante hacer notar que una computadora cuántica no es más rápida que una supercomputadora en cualquier cálculo. La multiplicación de dos números,

por ejemplo, no es más rápida en una computadora cuántica. La gran ventaja de la computación cuántica se ponde de manifiesto en problemas "paralelizables", es decir, aquellos problemas en los que se pueden ejecutar diferentes cálculos simultáneamente en la búsqueda de su solución. La mayor parte de los problemas de interés, sin embargo, son paralelizables en mayor o menor grado. Es por esta razón que se han desarrollado las supercomputadoras paralelas actuales y que se las considera los instrumentos computacionales más avanzados de los que se dispone hoy.

Otro de los algoritmos fantásticos desarrollados para computadoras cuánticas es el algoritmo de búsqueda de Lov Grover, de Lucent Technologies, capaz de encontrar uno de los ítems de una base de datos desordenada de N entradas en $\sqrt{N}$ pasos—en promedio, en lugar de los $N/2$ que se requieren en promedio en una computadora actual [7]. Es evidente que la diferencia es realmente enorme cuando se trata de bases de datos grandes.

3 Algoritmo de Schor

En esta sección se ilustra el algoritmo de Schor con un ejemplo simple, poniendo en evidencia las ventajas del paralelismo cuántico. Factorizar un número N es encontrar su factores primos, es decir, los números primos que, multiplicados, dan N. La manera más simple de saber si un primo p (menor a la raíz cuadrada de N) es factor de N es dividir N por p, y si el resto de la división es 0, p es un factor. El problema es que este algoritmo no es eficiente para números grandes. Suponiendo que una computadora puede hacer pruebas con 10^{10} números primos p por segundo (más rápido que una supercomputadora actual), factorizar un número de 60 dígitos tomaría más tiempo que la edad del Universo.

El algoritmo de Shor explota el paralelismo intrínseco de la computación cuántica. Se basa en un resultado conocido de teoría de números que convierte la factorización en la evaluación del período de una sucesión larga (el período r de la sucesión 1 5 13 0 2 1 5 13 0 2 1 5 13 0 2…, por ejemplo, es 5). Supongamos que se desea factorizar el número $N = 14$. Para empezar se toma al azar un número a más pequeño que N, por ejemplo 5. Se define entonces la función $f(n) = 5^n \bmod 14$. El resultado de teoría de números mencionado dice que f es periódica y que su período está relacionado con los factores de 14. Se puede verificar fácilmente que la sucesión determinada por f al ser evaluada en $n = 0, 1, 2, 3, \ldots$ es $1, 5, 11, 13, 9, 3, 1, 5, 11, \ldots$ Se observa que el período de esta sucesión es $r = 6$. Luego, para encontrar los factores de N sólo se requiere encontrar el máximo común divisor de N y $a^{r/2} + 1$ (o de N y $a^{r/2} - 1$). Así, el máximo común divisor de 14 y de $5^{6/2} + 1 = 126$ es 7. En el presente caso, la división de 14 por 7 da directamente el otro factor, 2. (El factor 2 es el máximo común divisor de 14 y $5^{6/2} - 1 = 124$.) En una computadora clásica este método no es nada ventajoso. Efectivamente, encontrar el período de f requiere que ésta se evalúe muchas veces y se puede demostrar que el número de evaluaciones necesarias es del mismo orden de magnitud que en el caso del método del resto descrito al inicio de esta sección. Una computadora cuántica, en cambio, actuando sobre un registro en que están represen-

tados los estados $0, 1, 2, 3, \ldots$ puede evaluar en un solo paso $f(0), f(1), f(2), f(3), \ldots$, valores que están representados todos en el registro de salida. Encontrar el período a partir de este registro es una tarea relativamente directa, que se efectúa con la versión cuántica de lo que se llama la transformada de Fourier. El algortimo necesario, también desarrolado por Shor, se ejecuta igualmente en tiempo polinomial.

4 Computadoras cuánticas

Como se ha mencionado en la introducción, las computadoras cuánticas, capaces de ejecutar algoritmos cuánticos, están aún en estado embrionario. Los investigadores aún deberán resolver varios problemas de orden científico y tecnológico antes de poder desarrollar una computadora cuántica. Pues, ya en 1995 se elaboraron compuertas lógicas cuánticas a dos qubits en base a sistemas atómicos. En el National Institute of Standards and Technology (NIST), en los Estados Unidos, se utilizaron los estados de vibración de iones de Berilio confinados a un espacio microscópico [9]. En la Ecole Normale Supérieure, en Francia, el grupo del Profesor Haroche empleó un campo electromagnético a dos niveles para cambiar los niveles de energía de un átomo de Rydberg en una cavidad [8]. Luego, en 1997, un equipo conformado por investigadores del Massachusetts Institute of Technology (MIT) y de Los Alamos National Laboratory (estado de New Mexico, Estados Unidos), logró realizar con éxito la operación de primero básico $1 + 1 = 2$ con un sistema de tres qubits en base a moléculas, y explotando el conocido principio de Resonancia Magnética Nuclear (RMN), utilizado cotidianamente en análisis químicos y en medicina [10]. Los qubits están definidos por el spin de algunos de los átomos en una molécula y la preparación del estado inicial, las operaciones lógicas y la lectura del resultado se hacen en base a pulsos de laser. Aunque no lo parezca, este trabajo fue un gran triunfo. Efectivamente, una de los mayores dificultades que enfrentaban los investigadores era el mantener a los qubits en una superposición estable de los diferentes estados de los bits individuales. El problema es que una superposición como la de la Figura 1, $a_1 |00\rangle + a_2 |01\rangle + a_3 |10\rangle + a_4 |11\rangle$, es frágil, en el sentido que cualquier perturbación, por ejemplo una vibración o un fotón, hace caer al sistema a uno solo de los cuatro estados, destruyendo el ingrediente básico del paralelismo cuántico. En realidad algunos investigadores pensaban que este problema era insalvable y que impediría el desarrollo de computadoras cuánticas. Aislar una molécula (o átomo), utilizada como bit físico, de manera que no tenga ninguna interacción no deseada con su entorno es practicamente imposible. Para eludir este problema, el equipo MIT-Los Alamos utilizó, no una, sino un vasto número de moléculas para representar un qubit, tantas como las que se encuentran, por ejemplo, en una muestra de líquido en un tubo de ensayo ($\sim 10^{23}$). De esta manera lograron mantener un número suficiente de moléculas en el necesario "estado coherente", como se dice científicamente, para realizar el cómputo cuántico, porque las interacciones no deseadas con el entorno y la lectura del resultado sólo afectan a una pequeña fracción del todo. En realidad, como dicen Gershenfeld y Chuang [10], los investigadores que han estado utilizando espectroscopía RMN, en el estudio de moléculas complicadas, desde hace décadas, han estado haciendo computación cuántica sin saberlo.

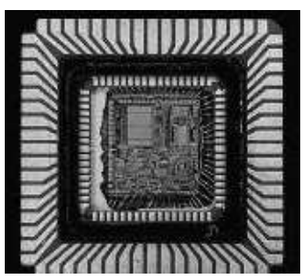

Figura 3: El microchip, símbolo de la tecnología de las computadoras de hoy y un baño de moléculas de cafeína, ejemplo de la inesperada dirección que puede tomar la tecnología del futuro.

5 Mirando hacia adelante

Es de esperar que, en los años que vienen, las computadoras clásicas muestren progresos impresionantes en cuanto a capacidad. Puede ser que incluso se lleguen a implementar los "cristales fotónicos" y que la velocidad de la computadoras se multiplique por un factor considerable [11]. Sin embargo, estos progresos seguirán incrementando la capacidad de nuestras computadoras de manera lineal, a diferencia de la computación cuántica, que lo haría de manera exponencial.

Otro aspecto grato de la computación cuántica es que, al parecer, como en el caso del RMN, no requerirá necesariamente de grandes esfuerzos en nanotecnología y equipos de fabricación sofisticados. Por ejemplo, Gershenfeld y Chuang utilizaron una simple molécula de cloroformo, $CHCl_3$, para elaborar una compuerta lógica O-exclusiva en base a dos spines nucleares—el del carbono (con un neutrón adicional) y el del hidrógeno. Para tener una computadora cuántica de mayor capacidad, se requerirán moléculas con más qubits, desde luego. Un candidato parece ser la molécula de cafeína [6]. El problema actual con moléculas demasiado grandes es que la señal RMN decrece con el número de núcleos magnéticos en la molécula [10]. Pero, como hace notar el mismo Lov Grover, es muy difícil predecir la rapidez con que se hará progreso en el futuro. A título de ejemplo cita un extracto del número de Marzo de 1949 de *Popular Mechanics* en el que, en un comentario sobre la computadora ENIAC (Electronic Numerical Integrator and Calculator), se dice "Donde una calculadora en la ENIAC está equipada con 18.000 tubos de vacío y pesa 30 toneladas, la computadoras en el futuro puede que tengan solamente 1.000 tubos de vacío y pesen solo 1,5 toneladas" [12]. Es así que puede que los componentes básicos de las computadoras del futuro se parezcan más a una taza de café que a un microchip actual.

Tal vez se puede tener una idea de la rapidez con que está avanzando la computación cuántica viendo los trabajos de investigación que se han estado realizando en este campo en los últimos años. Si, por ejemplo, el lector hace una búsqueda en el servidor de preprints de Los Alamos de las palabras claves "quantum AND (computer OR computing)", encontrará que en estos últimos años se han publicado centenas de trabajos en este campo [13]. Los tópicos cubiertos hacen una lista muy larga, contemplando

tanto aspectos teóricos como experimentales. Para dar una idea de la gran variedad de tópicos estudiados se pueden mencionar, por ejemplo, diferentes principios sobre los que se pueden desarrollar qubits, nuevos algoritmos cuánticos, teoría de la información cuántica, corrección de errores—software y hardware, decoherencia, codificación, velocidad de operación, memoria cuántica, formalismo matemático, etc. También se están considerando las posibles aplicaciones concretas, entre las cuales la modelación de sistemas físicos está en los primeros lugares, lo que, después de todo, era la idea original de Richard Feynman. Todo indica que el progreso en los próximos 10 años será increíble y, dentro de 25 años, es posible que los investigadores tengan colegas con una rapidez de cálculo y memoria fantásticas, una capacidad de aprendizaje y deducción difícilmente igualables y, además, curiosamente fáciles de confundir con una persona, algo reminiscente del personaje de HAL de "2001 Odisea del Espacio" de Arthur C. Clarke (ver el artículo de D. Pavisic en la página 203 de este mismo número de Acta Nova).

Referencias

[1] J. Birnbaum, Am. Phys. Soc. News Vol. 8, No. 6, 8 (1999).

[2] R. Feynman, Int. J. Theor. Phys. 21, 467 (1982).

[3] D. Deutsch, Proc. R. Soc. London A 400, 97 (1985).

[4] A. M. Turing, Proc. London Math. Soc. 2, 230 (1936).

[5] P. W. Shor, en Proc. 35th Annual Symposium on Foundations of Computer Science, Shafi Goldwasser, ed. (IEEE Computer Society Press, 1994).

[6] M. Antia y P. G. Brown, The Sciences, 11 (May/June 1997).

[7] L. K. Grover, en Proc. 28th Ann. ACM Symp. Theory of Computing (ACM Press, 1996).

[8] P. Domokos, J. M. Raimond, M. Brune y S. Haroche, Phys. Rev. A 52, 3554 (1995).

[9] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano y D. J. Wineland, Phys. Rev. Lett. 75, 4714 (1995).

[10] N. A. Gershenfeld y I. L. Chuang, Science 275, 350 (1997).

[11] Para leer sobre un avance reciente en este campo ver, por ejemplo, Sergey I. Bozhevolnyi, J. Erland, K. Leosson, P. M. W. Skovgaard y J. M. Hvam, Phys. Rev. Lett. 86, 3008 (2001).

[12] L. K. Grover, The Sciences, 24 (July/August 1999).

[13] Ver "Quantum physics" en <http://xxx.lanl.gov>