Computación Cuántica: Un Nuevo Paradigma

Enrique A. Cingolani[*]
Email: enrique.cingolani@uai.edu.ar

Nos encontramos en los albores de un cambio de paradigma en cuanto al hardware y al software de computación, de la mano del revolucionario concepto de la computación cuántica.

Resumen

Desde mediados del siglo pasado, a partir del desarrollo de los semiconductores, los sistemas de cómputo están progresando a pasos agigantados, gracias a la aplicación de los principios de la mecánica cuántica en el área del hardware. Hoy estos mismos principios traspasan las fronteras entre hardware y software, dando origen al qubit, una nueva unidad lógica que está llamada a reemplazar al bit en los nuevos sistemas de computación cuántica. En este artículo se describen las diferencias fundamentales entre el bit y el qubit, las características de sistemas basados en qubits, y los tipos de problemas que podrían resolver. Asimismo se explican brevemente distintas alternativas para construir qubits y se dan referencias acerca de algunos de los sistemas existentes en la actualidad. Se exponen reflexiones finales, recalcándose la importancia que presenta este campo de investigación para la ingeniería informática.

Bits versus Qubits

Los grandes progresos en el campo de la física dieron origen al enorme desarrollo de los sistemas computacionales. Desde la época de los sistemas basados en las válvulas termoiónicas en la década de 1940, a partir de las que fueron desarrolladas las primeras computadoras con un poder de cálculo significativo, el avance no cesó.

Pronto las válvulas fueron reemplazadas por los transistores, y el aumento del poder de cómputo se disparó acompañado por la miniaturización, la reducción del consumo energético y la integración de compuertas lógicas a gran escala, pasando de miles, a millones y a cientos de millones de ellas en un solo circuito integrado de pocos milímetros cuadrados.

Hoy en día se está vislumbrando un límite teórico para la miniaturización, y desde hace tiempo se acuden a técnicas de paralelización para acelerar las tareas de cómputo. Así se desarrollaron sistemas de hardware con unidades de cómputo de múltiples pipelines, núcleos y procesadores, para reducir tiempos al realizar operaciones "en paralelo" sobre distintos dispositivos macroscópicos. Sin embargo se sigue operando con lógica binaria, sobre bits, unidades lógicas que pueden tomar uno de entre dos valores posibles: 0 o 1.

En este contexto surge la computación cuántica, que promete una profunda revolución en el campo de los sistemas informáticos, al operar sobre novedosas unidades lógicas,

[*] Lic. Ciencias Físicas. Profesor Titular de Física II. Profesor Adjunto Permanente de Electromagnetismo Estado Sólido I y II. Facultad de Tecnología Informática - Universidad Abierta Interamericana.

denominadas *qubits* (quantum bits o bits cuánticos), que proveen una base intrínseca de paralelización: el paralelismo cuántico. Los algoritmos de computación basados en qubits, hacen uso de un concepto proveniente del mundo de la mecánica cuántica que es el de *superposición de estados*, que significa que un qubit puede hallarse en un estado cuántico que es simultáneamente (paralelamente) mezcla de dos estados. Los algoritmos computacionales desarrollados utilizando qubits permiten modificar la complejidad de las tareas, haciendo posible abordar problemas que clásicamente resultan intratables.

Qubit y Operación de Medición

El qubit o bit cuántico es la unidad de información utilizada en computación cuántica. Se trata de un ente de naturaleza cuántica que puede ser, por ejemplo, el espín de un electrón (asociado al sentido de giro –horario u antihorario– del electrón sobre su propio eje) o el momento magnético de un grupo de moléculas. Al ser observado el qubit puede presentar uno de dos estados posibles pero, a diferencia del bit clásico que tiene siempre sólo uno de dos valores (0 o 1), el qubit permanece, mientras no se lo observe, en un estado representado por una *función de onda*, que es una combinación lineal o superposición de ambos estados observables.

Al medir (observar) un qubit, se produce lo que se denomina el colapso de su función de onda: el qubit deja el estado de superposición en que se encontraba, y toma un valor concreto, ya sea 0 o 1, con una determinada probabilidad para cada uno de ellos.

Puede imaginarse un qubit haciendo una analogía con una moneda que se hace girar de canto sobre una mesa. En tanto la moneda no pare de rotar, la misma está en un estado que es superposición de los dos estados que pueden observarse, cara (estado 0) o cruz (estado 1). Medir u observar sería como aplastar la moneda con la mano contra la mesa. En ese instante colapsará su función de onda y se observará uno de dos estados: cara (estado 0) con probabilidad ½ o cruz (estado 1) con probabilidad ½.

Sistemas con Múltiples Qubits

Así como un sistema clásico de un bit no posee demasiado poder de cómputo, tampoco lo tiene un sistema de un qubit. La verdadera diferencia aparece cuando se utilizan sistemas de múltiples qubits.

Supongamos tener un sistema compuesto por 2 qubits. Este sistema podrá colapsar a 4 estados posibles al ser observado (00, 01, 10 y 11), dependiendo respectivamente del estado que adopte cada uno de los 2 qubits componentes. Por lo tanto el sistema compuesto por los 2 qubits estará antes de ser medido en un estado que es superposición de estos cuatro estados observables, es decir que el sistema de 2 qubits se encuentra en un estado que es paralelamente la mezcla de 4 (o sea 2^2) estados.

Análogamente si se tiene un sistema de 3 qubits sus estados observables serán 000, 001, 010, 011, 100, 101, 110 y 111, y se encontrará, mientras no se lo mida, en un estado que es paralelamente la mezcla de estos 8 (o sea 2^3) estados.

Puede inferirse por lo tanto que un sistema de computación cuántica de n qubits (podemos llamarlo un registro de n qubits) se encontrará en un estado que es superposición de ¡2^n estados!

En este hecho se basa el paralelismo en los algoritmos de computación cuántica. El sistema cuántico, que está en un estado de superposición, debe "prepararse" de modo que al ser observado (medido) entregue la solución a un problema determinado. Todas las posibles soluciones son analizadas simultáneamente. La cuestión ahora es desarrollar un algoritmo de medición que provoque que la función de onda del sistema colapse al estado que sea el resultado buscado.

Problemas de Optimización Discreta y Factorización

Uno de los tipos de problemas apropiados para ser tratados por sistemas de computación cuántica, debido a la naturaleza de los mismos, son los de optimización discreta. Son situaciones en las que hay que analizar una enorme cantidad de posibilidades entre las cuales se encuentra la solución. Un caso típico es el conocido problema del "viajante de comercio" que debe minimizar el camino para visitar varias ciudades.

Clásicamente estas cuestiones se resuelven recorriendo todas las posibilidades hasta encontrar la solución buscada. Si bien en algunos casos pueden aplicarse algoritmos ingeniosos que permiten reducir algo el tiempo de búsqueda de la solución, se trata de problemas que consumen muchísimo tiempo.

Utilizando hardware y software de computación cuántica, este tipo de problemas se resuelve preparando el sistema de múltiples qubits en un estado que sea la superposición de todas las posibles soluciones. Luego se hace evolucionar el sistema de modo que al medir colapse al estado que sea la solución buscada.

Por ejemplo, encontrar clásicamente la solución a un problema que presenta 2^{500} posibilidades discretas, implicaría probar una por una cada una de estas posibilidades. Aún con los sistemas de computación más rápidos de hoy en día, no alcanzaría el tiempo del universo para cumplir esta tarea.

Sin embargo con una computadora cuántica de 500 qubits, el sistema estaría en un estado de superposición que sería paralelamente la mezcla de los 2^{500} estados posibles, entre los cuales está la solución al problema. El sistema cuántico trabaja con un paralelismo intrínseco y el algoritmo de computación cuántica debe hacerlo evolucionar para que colapse al estado que sea la solución.

Otro tipo de problemas que ha sido tratado desde las primeras investigaciones realizadas en computación cuántica y continúa siendo objeto de estudio, es el de la factorización de números. Esto resulta particularmente interesante dado que los algoritmos de encriptación de datos más ampliamente utilizados, como RSA con claves pública y privada, se basan en la factorización de grandes números.

El tiempo que una computadora actual requiere para realizar esta factorización, puede medirse en cientos o aún miles de años, dependiendo del número a factorizar, por lo cual la seguridad ante el quiebre de las claves está convenientemente garantizada. Esto podría cambiar drásticamente con el uso de computadoras cuánticas de múltiples qubits, y algoritmos cuánticos existentes, como el de Shor, que en principio permitirían realizar esta labor en tiempos del orden de minutos.

Realización Física de Qubits

Básicamente un qubit debe ser un sistema cuántico en un estado que sea superposición de dos estados observables. Así, por ejemplo, si se tiene un qubit asociado al espín de un electrón, estará en un estado que es superposición de los dos estados observables de espín (espín UP representado por 0 –giro horario– y espín DOWN representado por 1 –giro antihorario–).

No cualquier sistema cuántico es apto para realizar computación cuántica, ya que existen ciertos requerimientos que debe cumplir. Entre ellos el qubit debe tener memoria confiable, es decir que un qubit debe mantener su estado cuántico de superposición a lo largo del tiempo, propiedad que se conoce como coherencia. Los tiempos de coherencia deben ser lo más largos posibles. Por otra parte debe ser viable cambiar los estados cuánticos de los qubits de manera individual, es decir manipularlos para preparar estados cuánticos especiales. Los qubits deben poder relacionarse a través de compuertas que permitan operaciones lógicas entre ellos. Por último debe existir acoplamiento (interrelación) entre qubits, pero a su vez deben estar completamente aislados del exterior, de modo que los campos o condiciones externas no alteren al sistema de computación cuántica.

Existen varias alternativas para realizar qubits físicamente, muchas de las cuales han sido utilizadas con mayor o menor éxito, pudiendo mencionarse las siguientes:

Trampa iónica: Se trata de iones en trampas al vacío, levitados eléctricamente, que se comportan como pequeños imanes. Los estados observables de cada qubit corresponden a dos orientaciones del momento magnético del ión. Los iones se manipulan utilizando láseres.

Espines nucleares en equipos de resonancia magnética nuclear (RMN): Son de los primeros sistemas que se utilizaron, dada la experiencia previa en el campo de la resonancia magnética nuclear. Aquí los núcleos atómicos de un grupo de moléculas en dilución se comportan como pequeños imanes. Los estados observables de cada qubit corresponden a las dos orientaciones de su momento magnético. Las moléculas se manipulan utilizando ondas de radio en equipos de RMN.

Qubits de flujo (flux qubits): En este caso, se establecen corrientes eléctricas en anillos superconductores micrométricos (interrumpidos por una o más junturas Josephson), que funcionan a muy baja temperatura. Los estados observables de cada qubit corresponden a las orientaciones horaria y antihoraria del sentido de circulación de la corriente en el anillo superconductor. Las corrientes se manipulan utilizando campos magnéticos y radiación de microondas.

Otros qubits propuestos incluyen defectos cristalinos en diamantes, puntos cuánticos, polarización de fotones y espín de electrones.

Hardware Cuántico

Existen enormes desafíos a vencer para construir una computadora cuántica, sin embargo se siguen realizando avances continuos desde 1998, año en el que Isaac Chuang construyó la primera computadora cuántica de 1 qubit en Berkeley.

En 2001 IBM construyó una computadora cuántica de 7 qubits, con la que factorizaron el número 15 (3 x 5). En 2005 Rainer Blatt en Innsbruck desarrolló una computadora cuántica de 8 qubits y recientemente (2012) Jiangfeng Du y su grupo de la Universidad de Ciencia y Tecnología de Hefei, China, lograron la factorización del número 143 (11 x 13).

Contrastando con estos modestos avances por el lado académico, la empresa canadiense DWave presentó en 2011 su computadora cuántica DWave One de 128 qubits, enteramente desarrollada, construida y ofrecida comercialmente por esta firma. Esto produjo grandes debates e intercambio de opiniones, ya que muchos académicos dudan que se trate de una verdadera computadora cuántica, aunque por supuesto DWave asegura lo contrario.

Dentro de toda esta controversia resulta llamativo que la empresa Lockheed Martin Corporation, fabricante del avión F35, haya adquirido en 2011 una DWave One y un contrato de soporte técnico por 10 millones de dólares. Asimismo en agosto de 2012 la prestigiosa revista Nature publicó un artículo del Dr. Alejandro Perdomo-Ortiz y el grupo liderado por el profesor Alan Aspuru Guzik de la Universidad de Harvard, en el cual presentaron los resultados del mayor problema de plegado de proteínas resuelto hasta ese momento, para cuya solución trabajaron con una DWave One.

De acuerdo con la información técnica proporcionada por DWave, el sistema utiliza un procesador compuesto por un circuito integrado superconductor con 128 flux qubits, que trabaja a temperaturas de alrededor de 20 milésimas de Kelvin, cercanas al cero absoluto (-273,15 °C), y es refrigerado con helio líquido. Se necesitan varias horas para llegar a esta temperatura de funcionamiento, la cual una vez alcanzada puede mantenerse por meses. Para lograr aislar los qubits de campos magnéticos externos se utiliza un blindaje magnético con capacidad de filtrado mejor que 1 nano Tesla, lo que es una cien milésima parte de la intensidad del campo magnético terrestre.

Este sofisticado equipo está específicamente diseñado para resolver problemas matemáticos de optimización discreta, aplicando algoritmos basados en computación cuántica adiabática, en los cuales la solución de un problema coincide con el estado de mínima energía del sistema.

Reflexiones Finales

Más allá de las controversias desatadas en el terreno del hardware cuántico entre el mundo académico y el empresarial, es indiscutible que el futuro de la computación cuántica es muy prometedor. Hoy en día se está trabajando tanto en el desarrollo de sistemas físicos de múltiples qubits como en el de software y algoritmos específicos para ser aplicados a estos nuevos dispositivos.

El interés que despierta es muy grande porque ya no se está hablando del desarrollo de un nuevo procesador, más pequeño, más rápido o con mayores prestaciones. El tema que aquí se vislumbra es la gestación de una nueva manera de hacer computación, con un hardware diferente desde la base, que incorpora el paralelismo intrínsecamente, en la definición misma de su unidad de información “el qubit”.

La expansión de este hardware vendrá, indiscutiblemente, a la par del desarrollo de algoritmos y software adecuados, que exploten las nuevas capacidades disponibles. Esta tecnología está madurando rápidamente y todo indica que conducirá a un verdadero cambio de paradigma.

Los ingenieros en sistemas informáticos no pueden permanecer al margen. Deben acercarse al fascinante mundo que aquí se les presenta, comprender los principios físicos involucrados y aportar su experiencia a este novedoso campo de la ciencia y la tecnología.

Referencias

Cohen Tannoudji, Claude, Diu, Bernard, Laloe, Franck, *Quantum Mechanics*. Wiley, 1977.

Dwave Systems Inc, *128 qubit processor*, Aug 2012, en http://www.youtube.com/watch?v=PqSgmCg1kew&feature=player_embedded

Feynman, Richard, *Física.TIII. Mecánica Cuántica*. Addison-Wesley Iberoamericana, México, 1987.

Monroe, Cristopher, Wineland, David, *Quantum computing with ions*, Scientific American Magazine, Aug 11, 2008.

Perdomo Ortiz, Alejandro et al, *Finding low-energy conformations of lattice protein models by quantum annealing*. Nature, Scientific Reports 2, Article number: 571, Aug 13, 2012.

Rieffel, Eleanor. *An Introduction to Quantum Computing for Non- Physicists*. ACM Computing Surveys, Vol. 32(3), pp. 300 - 335, Sept 2000.

Shor, Peter, *Polynomial time for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal Sci. Statist. Comput. 26, 1484, (1997).

Smalley Eric, *DWave defies world of critics with first quantum cloud*, Wired Magazine, Feb 22, 2012, en http://www.wired.com/wiredenterprise/2012/02/dwave-quantum-cloud/all/1