COMPUTACIÓN CUÁNTICA

Por Ing. Leonel Morales Díaz, leonel@ingenieriasimple.com

RESUMEN

La Computación Cuántica aprovecha las características de las partículas previstas por la mecánica cuántica, especialmente la superposición y el enmarañamiento, para ejecutar procesos y realizar cálculos con ciertas ventajas respecto a los sistemas tradicionales. Se trata de una tecnología en desarrollo cuyo florecimiento está por venir. En este artículo se revisan los principios que la soportan, los retos que enfrenta y las posibilidades para los investigadores que deseen involucrarse.

DESCRIPTORES

Computación cuántica. Qubit. Superposición. Enmarañamiento. Algoritmos cuánticos. Teoría de la Información.

ABSTRACT

Quantum Computing takes advantage of some features of particles described by quantum mechanics, specifically superposition and entanglement, to allow the execution of processes and calculations with computational advantage over the traditional systems. Quantum Computing is an emerging technology that will see an increase of development in the years to come. In this article the author briefly reviews the supporting theory, the challenges the technology confronts and the opportunities for researches willing to get involved.

KEYWORDS

Quantum Computing. Qubit. Superposition. Entanglement. Quantum algorithms. Information theory.

COMPUTACIÓN CUÁNTICA

COMPUTACIÓN Y BITS

La más pequeña unidad de información es el bit. Un bit sólo puede tener uno de dos valores, que para efectos prácticos representamos como 1 o 0, pero como bien apuntaron Claude Shannon, padre de la teoría de la información, y Warren Weaver en el libro Teoría Matemática de la Comunicación: "la información no debe confundirse con el significado". La información sobre el resultado de la lotería para un número en particular puede representarse con un bit: 1 ganó, 0 no ganó, pero el significado de tal mensaje sería muy grande, y por otra parte una fotografía digital puede requerir una gran cantidad de bits pero tener un pobre significado. No debe por tanto asociarse cantidad de información con cantidad de significado.

Dónde se almacena un bit de información es una cuestión mucho más práctica y que desde que las computadoras digitales empezaron a existir se convirtió en un factor clave de eficiencia energética, capacidad y velocidad de cómputo. Si para almacenar un bit se requiere una gran cantidad de energía la computadora resultará anti-económica, como sucedía cuando se usaban bulbos al vacío y relevadores para almacenamiento; si almacena pocos bits su funcionalidad se reduce y si es lenta para acceder a cada bit entonces presentará resultados en lapsos inaceptables.

Aún más importante es cómo se procesa cada bit, qué papel juega, si representa una entrada, una salida, un resultado intermedio, un indicador de proceso que sirve para realizar cálculos posteriores, etc. Aquí es cuando el bit se convierte en parte de una computación, de una operación o de un cálculo.

Los bits están participando constantemente en nuevas computaciones que a su vez responden a procesos bien estructurados denominados algoritmos.

Y aunque nos parezca que las computadoras actuales son omnipotentes la cruda realidad es que tienen muchas limitaciones. El conjunto de problemas que pueden resolver es más bien pobre, aunque claro, los problemas que les atañen usualmente los resuelven mucho más rápido que lo que nosotros los seres humanos podríamos hacerlo.

Parte de su limitación fundamental radica en que tienen una cantidad finita de estados, son máquinas discretas y en un momento dado solo pueden estar en uno de esos estados perfectamente identificado y se puede predecir con exactitud que llegará a él, esto es, son máquinas determinísticas.

En 1982 Richard Feynman observó que ciertos procesos cuánticos no pueden ser simulados eficientemente por una computadora tradicional y sugirió que estos efectos podrían ser

utilizados para realizar computaciones en una manera totalmente nueva. En 1985 Feynman presentó el concepto en una conferencia titulada "Quantum Mechanical Computers" y así nació este nuevo campo.

Utilizando los principios de la mecánica cuántica se ha identificado un tipo de máquina que puede estar en más de un estado al mismo tiempo: la computadora cuántica. Esta cualidad le ayuda, en teoría, porque todavía no se ha construido un prototipo funcional y estable, aunque ya se han presentado bastantes candidatos, a realizar computaciones en tiempos inconcebibles para las computadoras clásicas.

POTENCIAL DE LA COMPUTACIÓN CUÁNTICA

Supongamos que encontrar los números primos de exactamente 48 dígitos toma 10 años usando los procesadores comúnmente disponibles. Una computadora cuántica usaría sólo una fracción de ese tiempo, digamos unas pocas horas, gracias a que en lugar de pasar afanosamente por cada uno de los posibles estados que la resolución del problema requiere, el algoritmo cuántico toma un atajo pasando por muchísimos estados al mismo tiempo y volviendo al proceso tradicional únicamente para reportar resultados o para tomar la siguiente entrada. Este atajo se denomina paralelismo cuántico.

En el corazón de la computadora cuántica reina el flamante y elusivo sucesor del bit: el qubit[1] o quantum binary digit, que puede presentar uno de los dos estados del bit (1 y 0) pero también es capaz de colocarse en ambos estados al mismo tiempo gracias a la superposición – la ley básica de la mecánica cuántica – proeza imposible para cualquier sistema digital en uso.

Al superponer estados, los qubits pueden procesar la información en simultáneo, en lugar de hacerlo en serie o en paralelo, como las computadoras actuales. Por ejemplo, para procesar 8 bits en paralelo se usarían 8 bits físicos que en un ciclo de computación representan un solo valor de entre 256 posibles, con lo cual el sistema tiene 256 estados. Procesar todos los estados requeriría igual cantidad de ciclos como mínimo. En cambio, en la computadora cuántica 8 qubits podrían asumir todas las combinaciones de estados de 8 bits y procesar todo en un solo ciclo de computación.

Con todo, las computadoras cuánticas no serán de uso general. No es probable que veamos aplicaciones completas basadas exclusivamente en este tipo de computación. Esto se debe a que en la gran mayoría de problemas en los que nos ayudan estas máquinas hoy en día, necesitamos conocer los resultados de cada operación individual. Por ejemplo, al procesar

[1] Algunos autores en español lo denominan "Cubit", pero ese término parece menos adecuado por forzar la composición de una palabra en español "cuántico" con un término de uso común pero de origen anglosajón "bit". El término más común en la literatura es el utilizado aquí "Qubit".

una lista de 1 millón de clientes para asignarles una cuota mensual, se necesita registrar el resultado para cada uno de ese millón de registros. En teoría es posible realizar todas las operaciones en un solo paso usando computación cuántica, pero solamente uno de todos los resultados podrá ser conocido en cada momento, lo que en la práctica significa que no se obtiene ningún beneficio de rendimiento para este caso. Nuevamente esto es un resultado previsto por la mecánica cuántica pues los estados cuánticos superpuestos se "colapsan" a un solo valor al momento en que se efectúa una medición.

Lo que sí veremos será combinaciones de computación clásica y computación cuántica, lo que de hecho será el caso general. Con técnicas cuánticas se cubrirán secciones especiales de cada algoritmo para las que su uso rinda los mejores beneficios.

LOS FACTORES PRIMOS Y LA SEGURIDAD INFORMÁTICA

Existe un problema que es notablemente adecuado para la aplicación de la computación cuántica. Se trata de la descomposición de números enteros enormes en sus factores primos, o lo que es lo mismo, dado un número entero positivo cualquiera, encontrar todos los números primos que al multiplicarse dan por resultado ese número.

Si el número a factorizar es grande resolver este problema requiere tal capacidad de cómputo, que para ciertos números muy grandes, puede considerarse irresoluble con las técnicas de computación clásica[2].

Las técnicas criptográficas de llave pública y llave privada, como RSA o intercambio de clave de Diffie y Hellman, entre otras, pueden recibir ataques, es decir, intentos no autorizados de desencriptamiento, pero los atacantes se enfrentarán con el problema de factorización de números grandes y el problema del logaritmo discreto respectivamente. Estos problemas se vuelven computacionalmente irresolubles si los números primos involucrados son muy grandes.

Pero con computación cuántica un villano informático podría – y fácilmente – resolver ambos problemas y descifrar la información contenida en los mensajes. Esta posibilidad compromete seriamente la seguridad de muchísimos sistemas informáticos actuales, incluyendo bancos, universidades, empresas de Internet, etc.

Tal escenario de ataque informático con computación cuántica fue descubierto por Peter Shor, en 1994, trabajando para AT&T. Shor describió completamente el algoritmo cuántico para encontrar los dos números primos que factorizan a un número, sabiendo que es el

[2] A la computación no cuántica, basada en estados fijos, sin superposición ni enmarañamiento, se le llama computación clásica, por analogía con la distinción entre mecánica clásica y la mecánica cuántica.

resultado de multiplicar dos primos, y por ello se le nombró en su honor Algoritmo de Shor.

Aunque el desarrollo de computadoras cuánticas todavía tomará algunos años – nadie sabe cuántos – es importante empezar a pensar en nuevos métodos para garantizar la seguridad de las comunicaciones informáticas. La solución involucra el desarrollo de nuevos algoritmos de encriptamiento, con computación cuántica.

EL PAPEL DEL ENMARAÑAMIENTO CUÁNTICO

Albert Einstein decía del enmarañamiento cuántico – *quantum entanglement* en inglés – que se trata de una escalofriante acción a distancia (*spooky action at a distance*). Este fenómeno establece un vínculo entre dos objetos de forma que el estado cuántico de uno no puede describirse completamente sin hacer mención del estado del otro, aun cuando entre los dos medie una distancia considerable.

Por ejemplo, si dos partículas están cuánticamente enmarañadas y al medir el espín de una de las dos y se encuentra que apunta hacia arriba, inmediatamente se conoce que el espín de la otra apunta hacia abajo. La distancia entre ellas es totalmente irrelevante.

En una computadora cuántica se aprovecha el enmarañamiento para determinar o manipular el estado de todos los qubits sin que sea necesario observar a cada uno individualmente.

Ambas propiedades, el enmarañamiento y la superposición son igualmente importantes para implementar este tipo de computación.

EL PROBLEMA DE LA ESCALABILIDAD

Diseñar y construir un qubit que funcione puede resultar una tarea difícil y complicada. Se ha hecho ya con iones atrapados entre campos magnéticos, que se leen con un láser especialmente calibrado para que la luz tenga cierta frecuencia y longitud de onda. Con esta técnica se puede apuntar el láser a un ión particular y leer su estado, que como se dijo antes, en ese momento deja la superposición y se colapsa a un único valor.

El verdadero problema es agregar más qubits y hacer que funcionen juntos por enmarañamiento. Al agregar más qubits, más iones por ejemplo, se enfrentan problemas difíciles de resolver. Es necesario aislarlos de cualquier influencia externa para evitar que se produzca una decoherencia, es decir, una lectura del estado del qubit que le obliga a abandonar la superposición y colapsar a un único estado, lo que significaría el fin de ese

ciclo de computaciones cuánticas. La coherencia significa, en este contexto, mantener los estados de superposición de las partículas involucradas y para lograrlo hay que evitar cualquier interacción con el entorno, como la que podría darse por choques de átomos vagando por el lugar o algunas formas de radiación.

Al mismo tiempo debe implementarse un método de carga de entradas y lectura de resultados. Ambas cosas implican una interacción del entorno con la computadora. Es difícil mantener un balance entre aislamiento e interacción.

ALGORITMOS CUÁNTICOS

El Algoritmo de Shor que permite encontrar factores primos usando computadoras cuánticas, fue el primero que demostró un uso práctico y de gran interés para este tipo de computación.

Una buena parte del trabajo de investigación actual en el campo consiste en desarrollar nuevos algoritmos. Lo que se busca es tomar un problema que se considera irresoluble, impracticable o simplemente no apto para computadoras clásicas y crear una versión que pueda aprovechar las propiedades de superposición y enmarañamiento de las computadoras cuánticas.

Estos algoritmos tienen usualmente dos partes: una de computación clásica y otra de computación cuántica. En la primera las técnicas aplicables son las mismas que conocen buena parte de los estudiantes de ciencias de la computación o ingeniería en informática y sistemas. En la segunda se trabaja con los vectores de probabilidades y los estados que describen el sistema para obtener un resultado y puede ser bastante complicada de analizar y diseñar.

Entre los ejemplos más notables se encuentra el Algoritmo de Grover, por el que se pueden localizar valores concretos en bases de datos no ordenadas. Con la mayoría de manejadores de bases de datos actuales, la solución pasaría por construir un índice sobre el campo de búsqueda y luego utilizar ese índice para localizar más fácilmente el valor deseado. Este podría ser el caso, por ejemplo, si se intenta buscar el nombre de una persona dado su número de teléfono en una guía telefónica que está ordenada alfabéticamente. Se construiría un índice sobre los números de teléfono y con él se buscaría el nombre de la persona.

Considérese el siguiente problema: dado un número de factura y el número de NIT de su emisor, localizar a los contribuyentes que reportaron ese número de factura en sus declaraciones de IVA en la base de datos de la SAT. Para resolverlo con computación

clásica habría que construir un índice sobre los números de factura reportados por los contribuyentes en una base de datos que bien podría ser de las más grandes del país.

Pero la construcción del índice implica recorrer afanosamente cada uno de los registros para indexarlos y solo entonces aprovecharlo para la búsqueda que interesa.

Como hay una buena probabilidad de que el número no sea el último de la lista puede resultar mejor recorrer la base de datos registro por registro, comparándolo contra el valor buscado, es decir, una búsqueda secuencial pura.

El Algoritmo de Grover muestra cómo puede realizarse esa búsqueda secuencial con computación cuántica y reducir el tiempo que toma a nada más la raíz cuadrada del que tomaría con una computadora tradicional.

CONCLUSIÓN

La computación cuántica es una excelente oportunidad de investigación y desarrollo para matemáticos, físicos, informáticos y expertos en ciencias de la computación. Por estar en su infancia, esta nueva rama del conocimiento verá el despliegue de su potencial en los años por venir, pero no hay que hacerse muchas ilusiones de verla llegar a nuestro escritorio muy pronto.

AGRADECIMIENTOS

Enrique Pazos Avalos, guatemalteco estudiante de doctorado en física en la universidad de Maryland, gentilmente accedió a revisar el manuscrito de este artículo y sugirió correcciones. Mil gracias.

REFERENCIAS

- **Scientific American**. Artículos disponibles sin necesidad de suscripción
- **Monroe, Christopher R. y Wineland, David J**. "Quantum Computing with Ions", disponible en línea en http://www.sciam.com/article.cfm?id=quantum-computing-with-ions
- **Robinson, Hans**. "What makes a quantum computer so different (and so much faster) than a conventional computer", entrevista, disponible en http://www.sciam.com/article.cfm?id=what-makes-a-quantum-comp

- **Minkel, JR**. "First 'Commercial' Quantum Computer Solves Sudoku Puzzles", disponible en línea en http://www.sciam.com/article.cfm?id=first-commercial-quantum-computer

- **Gershenfeld, Neil & Chuang, Isaac L**. "Quantum Computing with Molecules", disponible en línea en http://www.media.mit.edu/physics/publications/papers/98.06.sciam/0698gershenfeld.html

ACM artículos en la biblioteca digital que pueden requerir suscripción y pago:

- **Bacon, Dave & Leung, Debbie.** "Toward a World with Quantum Computers", Communications of the ACM, Septiembre de 2007.

- **Rieffel, Eleanor & Polak, Wolfgang**. "An Introduction to Quantum Computing for Non-Physicists", ACM Computing Surveys, Septiembre de 2000.

- **Jorrand, Philippe & Lalire, Marie.** "Toward a quantum process algebra", Proceedings of the 1st conference on Computing frontiers, Abril de 2004.

- **Prawer, Steven.** "Quantum mechanical approaches to information processing", Proceedings of the 20th annual international conference on Supercomputing, Junio de 2006.

Otros artículos en Internet:

- **Bone, Simon & Castro, Matias.** "A Brief History of Quantum Computing", disponible en http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/

- **Morales Díaz, Leonel.** "El Poderoso Qubit", disponible en http://guateciencia.wordpress.com/2009/03/10/el-poderoso-qubit/

- **Wikipedia.** Artículos de Quantum Computer, Quantum Superposition, Quantum Entanglement, Qubit, Shor's Algorithm, Grover's Algorithm

MORALES DÍAZ, LEONEL VINICIO

Ingeniero de Sistemas e Ingeniero Electrónico, graduado de la Universidad Francisco Marroquín, con maestría en Sistemas de Información y Bases de Datos de la Universidad Galileo. Docente universitario, ha sido Director de la Carrera de Informática y Sistemas de la Universidad Rafael Landívar. Actualmente se desempeña como consultor en desarrollo de sistemas e interacción humano-computador. Web site: www.ingenieriasimple.com/leonel