TECNOLOGÍA

Bits, Ciencia y Sociedad

sep 14

Computación cuántica: ¿un sueño posible?

Posteado a las 14 de Septiembre de 2010 - 13:02 | 2 comentarios

Por Gonzalo Navarro, profesor del Departamento de Ciencias de la Computación, FCFM, Universidad de Chile.

Quien más, quien menos, todos hemos oído hablar de la computación cuántica. Pero ¿qué es? ¿Llegará algún día? ¿Cómo afectará nuestras vidas? Comencemos por el qué es. La computación clásica se basa en el concepto de que la información digital básica, el bit, tiene sólo dos valores posibles: cero o uno. Todo se construye sobre ello. Por ejemplo usando 10 bits puedo representar, gracias a las dos combinaciones que me ofrece cada bit, $2^{10} = 1024$ situaciones distintas. **El funcionamiento de los computadores se basa en la física clásica, más precisamente en el electromagnetismo. La computación cuántica se basa en la física cuántica y su elemento básico es el qubit**. El qubit no sólo puede valer cero o uno, sino una superposición de ambos. Evitando tecnicismos y yendo a lo conceptual, el qubit permite combinar "un poco de cero" y "un poco de uno". Un computador cuántico opera sobre estos qubits, produciendo como resultado otros qubits.

La computación cuántica promete resolver eficientemente problemas que en computación clásica son intratables. Tomemos un ejemplo prototipo de problema intratable (en la jerga de la computación, NP-completo). Suponga que usted tiene un camión y quiere llevar cargas en él. El camión tiene un peso máximo que puede transportar. Como el viaje le cuesta más o menos lo mismo, lleve lo que lleve, usted quiere naturalmente cargar el camión al máximo posible. Pero los elementos que tiene que cargar tienen todos distintos pesos. ¿Cómo elegir aquellos que llenen el camión de la mejor forma posible? Podemos tomar cada elemento y considerar las dos alternativas: lo pongo o no lo pongo en el camión. Así, evalúo todas las alternativas posibles de incluir o no cada elemento. El que este problema sea NP-completo significa, básicamente, que no se conoce un método significativamente mejor que éste para resolver el problema, y que nadie cree que exista. Al menos, en computación clásica.

¿Cuál es el problema de nuestra solución? Pues que si tenemos n elementos a considerar para incluir o no en el camión, tendremos que evaluar 2^n alternativas distintas. Si tenemos, por ejemplo, 100 elementos para elegir, el número de alternativas a evaluar tiene 30 dígitos decimales. Si pensamos que cada alternativa se describe con un vector de 100 bits (cada bit diciendo si un elemento se incluye o no), lo que queremos es encontrar el mejor de todos los posibles vectores de 100 bits.

El milagro de la computación cuántica es que es capaz de producir eficientemente un vector de 100 qubits donde están superpuestas todas las soluciones, y en principio, extraer la mejor de todas ellas. Se acerca así al ideal del "computador no determinístico", un concepto abstracto que se utiliza para caracterizar la dificultad de los problemas computacionales, el cual es capaz de adivinar la solución correcta y luego sólo necesita verificar que es la correcta. Si bien la vida es algo más complicada para un computador cuántico que para uno no determinístico, se ha demostrado que el primero podría adivinar rápidamente las claves secretas que se usan para la cuenta de correo, las transacciones bancarias internacionales, y las comunicaciones militares. Todos estos sistemas se basan en la dificultad de los computadores clásicos de resolver problemas NP-completos, y un computador cuántico podría hallar la aguja en el pajar, es decir dar con la clave secreta entre todas las posibilidades, en unos instantes.

Pero, **¿es factible construir el computador cuántico? Es difícil decirlo. Ciertamente se lo está intentando con ahínco.** Los desafíos tecnológicos son formidables. Hoy en día se ha logrado mantener trabajando 10 qubits juntos, y transmitir información a lo largo de unos kilómetros. Esto parece lapidario comparado con nuestros computadores clásicos, que mantienen terabits al mismo tiempo, y con nuestra Internet que conecta el mundo. Pero no creo que eso sea para desanimarse. El hombre ha hecho milagros en tecnología. Si miramos los comienzos de la computación clásica, la ENIAC, aquel primer computador de válvulas construido en los años 40 para descifrar las claves secretas nazis, ocupaba habitaciones enteras y tenía menos poder de cómputo que el chip de nuestro lavarropas. Pero existen también objeciones más serias, que tienen que ver con límites fundamentales de la física cuántica, y que hacen que la última palabra sobre la factibilidad del computador cuántico aún no esté dicha.

Y si se logra implementar el computador cuántico, ¿qué significaría para el mundo? Comenzaré tranquilizándolos acerca de la clave de su cuenta de correo. Ya se han desarrollado nuevos mecanismos criptográficos basados en computación cuántica que permiten cifrar mensajes secretos de una forma, ahora sí, absolutamente segura, es decir, que no depende de que su adversario tenga un computador muy potente para descifrarlos, sino que es físicamente imposible hacerlo. Asimismo, es curioso que los investigadores ya hayan desarrollado, en papel, montones de algoritmos cuánticos, que están listos para programarse el día que tengan al alcance de sus dedos un computador cuántico de verdad. El día que tal cosa ocurra, si es que ocurre, el mundo será mejor que hoy. **Los computadores cuánticos tendrán poder para resolver muchos problemas que hoy nos aquejan por falta de suficiente poder de cómputo,** desde cargar mejor los camiones hasta cosas más notorias como mejorar nuestras redes de transporte, optimizar nuestro uso de los recursos naturales, afinar nuestra predicción del clima, diseñar terapias genéticas, mejorar nuestra comprensión del mundo desde el espacio hasta el ADN, y un largo etcétera. Y, por supuesto, cambiará radicalmente nuestro concepto de qué es un computador, qué límites físicos tiene, y cómo se programa.

Tags: computación, cuántica, qubit

PERMALINK | BLOGS QUE CITAN ESTE POSTED

perfil del autor

El blog Bits, Ciencia y Sociedad de la sección de Tecnología de Terra es un espacio donde cuatro académicos del Departamento de Ciencias de la Computación de la Universidad de Chile hablarán de la Tecnología y su impacto político y social en nuestro país.

Aquí escribirán semanalmente José Miguel Piquer, Claudio Gutiérrez, Pablo Barceló, Gonzalo Navarro y Tomás Barros.

posteos

VER: MÁS RECIENTES | MÁS COMENTADOS

Computación cuántica: ¿un sueño posible?
14 de Septiembre de 2010 - 13:02

Aduana de Valparaíso: Computación hace medio siglo
6 de Septiembre de 2010 - 10:22

El agotamiento de las direcciones IP y la importancia de emigrar a IPv6
26 de Agosto de 2010 - 8:59

El más famoso problema de la computación: ¿resuelto?
18 de Agosto de 2010 - 12:02

Algoritmos por energía
11 de Agosto de 2010 - 11:56

BUSCAR

últimos comentarios