Ordenador Cuántico – Estado del Arte

Calificación: 100
Enhorabuena!

Fecha: 29/03/2019
Autores: Jessica Cortes, Juan Manuel Blanco, Sergio Paya, Cristian Mauricio, Raúl Blanco

1. Origen del ordenador cuántico

Tiene su origen en la necesidad de crear chips más funcionales, que procesen más información y que sean mucho más pequeños, ya que los actuales tiene límites, que al pasar cierto tamaño dejan de funcionar normalmente, pero con las partículas cuánticas la tecnología abre nuevas posibilidades.

La computación cuántica *[1]* tiene su origen en 1981, cuando el profesor Benioff Paul propuso que en vez de trabajar con voltajes eléctricos se puede trabajar con niveles cuánticos, lo que permitiría que se puedan realizar varias operaciones simultáneamente sin afectar la superposición coherente.

Y es que, en teoría, estas computadoras, que emplean qubits o bits cuánticos, capaces de estar en dos estados a la vez, utilizarán átomos en vez de circuitos. El problema es que a esa escala no funcionan las leyes que rigen el mundo macroscópico.

Así, las partículas pueden estar correlacionadas, aunque se encuentren físicamente separadas –lo que permite una especie de teletransporte de la información– y todo el sistema se altera con el simple hecho de medirlo.

La novedad con la computación cuántica es que, en vez de usar transistores que puedan generar estados 0 o 1, utiliza los llamados qubits (bits cuánticos), que no solo están en 0 o 1 sino en una superposición de ambos estados. Esta superposición de estados posibilita una capacidad de computación exponencialmente mayor, ordenadores más rápidos y eficientes.

2. Cómo funciona la computación cuántica

A diferencia de la computación digital que hoy en día se utiliza y que funciona con bits (cada bit puede tener un valor 0 o 1, la computación cuántica funciona con los denominados qubits. Cada qubit puede valer {0} = [1 0] y {1} = [0 1]. Mientras que el qubit no sea observado, puede valer tanto {0} como {1} porque se encuentra en una superposición de estados. No se puede predecir cuál de los dos será, pero al observarlo el valor 'colapsa' (se dice así) en un {0} o en un {1}.

Esto ocurre porque el proceso que realiza no es mecánico sino basado en la física cuántica, la característica superposición de estados con la cual trabaja esta tecnología permite ejecutar más de un cómputo a la vez, esto es gracias a los qubits que permiten ejecutar de forma paralela el sí y el no de cada suposición.

Dos bits pueden tener cuatro estados diferentes (0 0, 0 1, 1 0 o 1 1) pero solo se puede elegir uno de ellos a cada instante. Dos qubits pueden tener todos estos estados, a la vez, siempre y cuando se encuentren aislados de los otros qubits. Esto es así porque la propiedad de entrelazamiento cuántico se desvanece cuando los átomos forman parte de otras estructuras.

Tiene unas ventajas enormes. Mientras que con 50 bits podemos almacenar unas 7 letras en formato básico, con 50 qubits tenemos 50 TB de capacidad.

3. Últimos avances en ordenadores cuánticos

IBM ha desarrollado ***Q System One*** *[8],* siendo el primer ordenador cuántico comercial. Tiene ***20qubits*** y está diseñado para aplicaciones científicas. Se ha de tener presente que la potencia de un ordenador cuántico no está definida únicamente por el número de qubits con el que es capaz de trabajar, sino también por su calidad, entendida como la capacidad de estos qubits de no resultar perturbados por el ruido como, por ejemplo, pequeños cambios en la temperatura o campos eléctricos o magnéticos dispersos… todos ellos degradan la información cuántica, en un proceso conocido como "***decoherencia***" *[2]*.

En ese sentido ***Microsoft*** propone utilizar en la fabricación de los qubits una partícula conocida como ***fermión de Majorana*** permitirá conseguir qubits más estables y con una inmunidad muy superior al ruido externo. Por su parte Google ha dado a conocer el año pasado que tiene un procesador cuántico de ***72qubits***, al que ha llamado ***Bristlecone***, pero aún no ha conseguido reducir el margen de error lo suficiente.

En cuanto a la detección/corrección de errores, que es en estos momentos es el mayor reto al que se enfrenta el ordenador cuántico, recientemente se ha publicado en la revista ***Physical Review Letters*** *[3]* un avance en la línea de poder reducir las tasas de error a través de la redundancia. Robin Harper y Steven Flammia, demostraron que un esquema específico puede ayudar a reducir las tasas de error en un prototipo cuántico mediante la computadora que IBM ha puesto a disposición de los investigadores para experimentar de forma remota (***Quantum Experience de IBM***) *[7]*.

La corrección de errores en la computación cuántica se basa en la redundancia, al igual que en la computación convencional. Si no hubiera errores, el cálculo podría realizarse utilizando directamente los qubits físicos. Pero ante el ruido, que siempre está presente, se tienen que combinar múltiples qubits físicos para hacer un qubit lógico, que luego se vuelve menos propenso a errores.

4. El futuro del ordenador cuántico

Las academias de ciencias, ingeniería y medicina de EEUU publicaron en diciembre del pasado año "***Quantum Computing Progress and Prospect***" *[4]*. Dicho documento revela las conclusiones a las que llegaron los expertos en relación a la computación cuántica actual y en un futuro próximo. Las conclusiones más relevantes en relación a los futuros ordenadores cuánticos *[5]* son las siguientes:

1ª- La probabilidad de que se construya un ordenador cuántico que comprometa RSA 2048 o criptosistemas de clave pública en la próxima década es improbable.

2ª- La financiación en la investigación de ordenadores cuánticos vendrá condicionada por el éxito comercial acorto plazo.

3º- Tendrá un gran impacto, condicionando el desarrollo, la investigación de aplicaciones comerciales en ordenadores de escala intermedia ruidosa (Noisy Intermediate Stage Quantum o NISQ) *[6]*.

4º- Con la información actual no se puede predecir la existencia de un ordenador cuántico escalable. Pero si se puede monitorizar su progreso, monitorizando la tasa de escalado de qubits físicos y conservando una tasa de error constante.

5ª- La existencia de aplicaciones que puedan evaluar la comparación entre diferentes máquinas, mejoraría el desarrollo del software y hardware cuántico.

6º- La aparición de un futuro ordenador cuántico y la transición a nuevos sistemas de seguridad es un riesgo a largo plazo. Por ello se hace necesario el desarrollo e implementación de la criptografía post-cuántica.

5. Problemas de la computación cuántica

La primera dificultad que trae la computación cuántica es que a pesar de que podemos realizar muchas operaciones en paralelo y de forma rápida, no podemos obtener resultados de todas. Por lo tanto, el reto será es encontrar la manera de poder extraer la máxima información.

La segunda es que obliga a cambiar el mundo de la seguridad, ya que deben de desarrollarse nuevos algoritmos.

¿Cuál sería el impacto de un ataque con ordenador cuántico a la criptografía actual?

Criptografía de clave asimétrica: Actualmente es prácticamente imposible romper el cifrado de clave pública, aun usando la mejor computadora convencional de hoy en día, pero un ordenador cuántico si podría realizarlo en unas horas.

Lo que se recomienda es evitar cifrados de clave asimétrica como RSA, ElGamal o los basados en el protocolo Diffy-Hellman, ya que los ordenadores cuánticos podrían resolver de forma relativamente sencilla los problemas matemáticos en los que se basa su seguridad. Como un ejemplo, quebrar una clave RSA de 1.024 bits le tomaría 4 horas a un ordenador cuántico de unos 2.300 qubits lógicos.

Criptografía de clave simétrica: El estándar actual es AES-GCM (clave variable: 128, 192 ó 256 bits). Un ataque de fuerza bruta exige probar todos los posibles valores de la clave, el algoritmo de Grover es capaz de acelerar esta búsqueda, pero igualmente tomaría años.

6. Otras tecnologías cuánticas

Comunicación cuántica: Implica la generación y el uso de estados y recursos cuánticos para los protocolos de comunicación, cuyas aplicaciones principales se encuentran en la comunicación segura, el almacenamiento seguro a largo plazo, la computación en la nube y otras tareas relacionadas con la criptografía, así como una "web cuántica" segura.

Simulación cuántica: Los sistemas cuánticos interactuando podrían simularse eficientemente empleando otros sistemas cuánticos controlables con precisión, incluso en muchos casos en los que se espera que dicha tarea de simulación sea ineficiente para las computadoras clásicas estándar, utilizando la simulación cuántica.

Sensores cuánticos: El concepto central de un sensor es que una sonda interactúa con un sistema apropiado, cuyas propiedades son de interés y que cambian el estado de la sonda. Las mediciones de la sonda revelan los parámetros que caracterizan el sistema. En sensores mejorados cuánticamente, la sonda generalmente se prepara en un estado particular no clásico.

Control cuántico: El objetivo general del control cuántico es manipular activamente los procesos dinámicos de los sistemas cuánticos, generalmente mediante campos o fuerzas electromagnéticas externas.

Claves cuánticas: Actualmente son de un sólo uso, lo que quiere decir que se deben renovar constantemente. Un equipo de la Universidad de Bristol, está trabajando en un dispositivo parecido a una tarjeta de crédito que permitiría recoger un lote en un punto de la red, como si fuera un cajero automático y utilizarlo para conectarse a varios servicios.

Industria: Además, hay otros dispositivos en desarrollo, dos de ellos son: los detectores de gravedad ultra-sensibles para detectar tuberías subterráneas, cámaras para captar gases invisibles.

Bibliografía

[1] Computación Cuántica – Wikipedia - https://en.wikipedia.org/wiki/Quantum_computing

[2] Decoherencia Cuántica – Wikipedia -https://es.wikipedia.org/wiki/Decoherencia_cu%C3%A1ntica

[3] Robin Harper y Steven T. Flammia - Puertas lógicas tolerantes a fallas en la experiencia de IBM Quantum - Fis. Rev. Lett. 122 , 080504 - https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.122.080504

[4] National Academies of Sciences, Engineering, and Medicine; Division on Engineering and Physical Sciences; Computer Science and Telecommunications Board; Intelligence Community Studies Board; Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing; Emily Grumbling and Mark Horowitz, Editors - https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects

[5] Gonzalo Álvarez Marañón - "No, 2019 no será el año en el que los ordenadores cuánticos acaben con la criptografía que todos usamos" – https://blog.elevenpaths.com/2019/01/ordenadores-cuanticos-hallazgo-ciberseguridad.html

[6] Blog de THOMAS J. ACKERMANN – Artículo explicativo de la tecnología "Noisy Intermediate Stage Quantum" – https://www.bgp4.com/2018/10/17/noisy-intermediate-scale-quantum-nisq-technology/

[7] Quantum Experience de IBM – Plataforma para experimentación de puertas lógicas cuánticas sobre qubits de IBM – https://quantumexperience.ng.bluemix.net/qx/editor

[8] Q System One – Primer ordenador cuántico de IBM - https://www.research.ibm.com/ibm-q/system-one/