

LA COMPUTACIÓN CUÁNTICA: DESARROLLOS ACTUALES Y PERSPECTIVAS FUTURAS

Florentino Borondo Rodríguez

Catedrático. Departamento de Química. Universidad Autónoma de Madrid

RESUMEN

En este artículo se realiza un análisis descriptivo de la computación cuántica, importante disciplina que está destinada a revolucionar la manera en que procesamos la información y abordamos los problemas más complejos del mundo moderno. A tal efecto, se describen en primer lugar los antecedentes históricos en esta materia, abordándose a continuación los algoritmos cuánticos. Se hace asimismo una comparación con la computación *clásica*, destacándose las ventajas potenciales de la computación cuántica, así como sus desafíos técnicos actuales. Se describe además el *estado del arte* en cuanto a las computadoras cuánticas actuales, analizándose igualmente el futuro próximo de la computación cuántica, la cual ha pasado de ser una teoría exótica a una realidad tecnológica con aplicaciones emergentes en muy diversos sectores.

1. INTRODUCCIÓN

Más de un siglo después de su aparición, las ideas de la mecánica cuántica siguen generando resultados sorprendentes. De hecho, las primeras aplicaciones basadas en el transistor, que funciona gracias al efecto túnel, y los láseres dio lugar a la llamada primera revolución cuántica. En la actualidad, estamos en las puertas de la segunda revolución generada por los fenómenos cuánticos, y en ella la computación y los sensores van a sufrir un gran desarrollo.

La computación cuántica está destinada a revolucionar la manera en que procesamos la información y abordamos los problemas más complejos del mundo moderno. Esta tecnología emergente, basada en los principios de la mecánica cuántica, promete resolver problemas que las computadoras clásicas no pueden abordar en un tiempo razonable. Aunque todavía se encuentra en etapas experimentales, los avances recientes sugieren que la computación cuántica podría remodelar industrias enteras en los próximos años.

2. UN POCO DE HISTORIA...

El viaje hacia la computación cuántica comenzó con el desarrollo de la mecánica cuántica a principios del siglo XX. Científicos como Max Planck, Albert Einstein, Niels Bohr y Erwin Schrödinger fueron pioneros en el estudio de cómo las partículas subatómicas, como los electrones y fotones, no se comportan de acuerdo con las leyes de la física clásica. En lugar de seguir trayectorias predecibles como las partículas macroscópicas, los electrones, por ejemplo, pueden existir en múltiples estados al mismo tiempo o "saltar" de un lugar a otro de manera instantánea sin pasar por los puntos intermedios. Este comportamiento dio origen a la mecánica cuántica, una de las teorías más fascinantes y exitosas en la historia de la ciencia.

El físico teórico Richard Feynman, otro coloso en el desarrollo de las ideas cuánticas, fue uno de los primeros en proponer en la década de 1980 que, para simular eficazmente los sistemas cuánticos, necesitábamos una computadora que funcionara con principios cuánticos. Este fue el punto de partida para el desarrollo de la computación cuántica. En 1985, David Deutsch propuso la idea de una máquina cuántica universal, capaz de realizar cualquier cálculo que una computadora clásica pudiera hacer, pero mucho más rápido en ciertos casos. El concepto de computación cuántica, aunque revolucionario, permaneció en el ámbito teórico hasta la década de 1990, cuando el matemático Peter Shor desarrolló un algoritmo cuántico que podía factorizar números grandes de manera exponencialmente más rápida que cualquier algoritmo clásico conocido. Este avance sentó las bases para una de las aplicaciones más importantes de la computación cuántica: la ruptura de los sistemas criptográficos modernos.

A continuación, pasaremos a revisar algunos de los conceptos más importantes de la mecánica cuántica en relación con la computación cuántica, y que hacen que se diferencien fundamentalmente de la computación clásica.

En primer lugar, está la Superposición. En la computación clásica, los bits son la unidad básica de información y solo pueden estar en uno de dos estados: 0 o 1. Sin embargo, en la computación cuántica, la unidad básica es el qubit, que puede existir en una superposición de ambos estados (0 y 1) al mismo tiempo. Este fenómeno es difícil de conceptualizar, pero es esencial para entender el poder de las computadoras cuánticas. Así, el estado de un qubit no es una simple mezcla de 0 y 1, sino una combinación de probabilidades que permiten que una computadora cuántica realice cálculos con ambos estados simultáneamente. La capacidad de operar con múltiples estados a la vez, le da a las computadoras cuánticas una ventaja exponencial sobre las clásicas en ciertos tipos de problemas.

El segundo concepto cuántico relevante en la computación cuántica es el entrelazamiento. El entrelazamiento cuántico es esencial para la computación cuántica. Cuando dos qubits están entrelazados, el estado de uno de ellos está directamente correlacionado con el estado del otro, sin importar la distancia que los separe. Este fenómeno fue calificado por Einstein como "acción fantasmagórica a distancia" porque desafía la noción clásica de que la información no puede viajar más rápido que la luz. En el mundo cuántico, los qubits entrelazados actúan como una unidad, lo que permite procesar información de manera más eficiente. Por ejemplo, si se tiene un par de qubits entrelazados y se mide el estado de uno de ellos, automáticamente se puede inferir el estado del otro, incluso si están a años luz de distancia. Esta propiedad es aprovechada por los algoritmos cuánticos para procesar grandes cantidades de información en paralelo.

El tercer ingrediente importante en la computación cuántica es la llamada interferencia cuántica. La interferencia cuántica es el principio que permite a los qubits influenciar las probabilidades de sus resultados. Las computadoras cuánticas pueden manipular qubits de tal manera que ciertos resultados probables se refuercen y otros se cancelen, mejorando la probabilidad de llegar a la respuesta correcta. Este fenómeno es clave para la eficiencia de los algoritmos cuánticos que dependen de la optimización de resultados. Un ejemplo interesante es el algoritmo de Grover, que permite buscar en una base de datos desordenada cuadráticamente más rápido a como lo hacen los algoritmos clásicos.

3. ALGORITMOS CUÁNTICOS

Como se desprende de los párrafos anteriores, otro ingrediente importante en la computación cuántica son los correspondientes algoritmos. Por tanto, pasaremos a continuación a la revisión de algunos que han resultado clave en el desarrollo de la computación cuántica. De hecho, para aprovechar la mecánica cuántica en la resolución de problemas, se han desarrollado varios algoritmos cuánticos que demuestran cómo las computadoras cuánticas pueden superar a las clásicas en ciertas tareas.

3.1. Algoritmo de Shor

El algoritmo de Shor, propuesto por Peter Shor en 1994, es uno de los algoritmos más famosos en computación cuántica. Está diseñado para factorizar grandes números en sus factores primos de manera exponencialmente más rápida que los métodos clásicos. Dado que muchos de los sistemas de cifrado actuales, como el de los laboratorios RSA (https://es.wikipedia.org/wiki/Competici%C3%B3n_de_factorizaci%C3%B3n_RSA), dependen de la dificultad de la factorización de grandes números, el algoritmo de Shor representa una amenaza potencial para la seguridad de las comunicaciones digitales. Sin embargo, las computadoras cuánticas actuales no son lo suficientemente grandes ni estables para ejecutar este algoritmo de manera eficiente en números reales utilizados en la criptografía moderna. A medida que los avances en la construcción de qubits mejoren, el algoritmo de Shor podría tener un impacto profundo en la criptografía.

3.2. Algoritmo de Grover

El algoritmo de Grover, desarrollado por Lov Grover en 1996, permite buscar en una base de datos desordenada en tiempo cuadrático en lugar de lineal. En lugar de probar todas las posibles soluciones una por una, el algoritmo de Grover utiliza la superposición e interferencia cuántica para encontrar la solución correcta más rápido. Aunque no ofrece una ventaja exponencial como el algoritmo de Shor, el algoritmo de Grover sigue siendo significativamente más rápido que los métodos clásicos para ciertas tareas.

4. COMPARACIÓN CON LA COMPUTACIÓN CLÁSICA: UN SALTO EXPONENCIAL

La computación clásica sigue siendo el pilar de la tecnología actual, y probablemente lo seguirá siendo durante varias décadas. Las computadoras clásicas están diseñadas para realizar cálculos utilizando bits binarios, que están restringidos a los estados de 0 ó 1. Estas máquinas siguen una secuencia de instrucciones predefinidas, paso a paso, para resolver problemas. Aunque han avanzado enormemente en términos de potencia de procesamiento y capacidad de almacenamiento, aún hay problemas que son simplemente demasiado grandes para ellas.

Por ejemplo, la simulación computacional de moléculas complejas (Química Computacional) es extremadamente difícil para una computadora clásica debido a la cantidad de variables y estados posibles que deben considerarse. En química cuántica, la cantidad de recursos computacionales necesarios para simular una molécula crece exponencialmente con el tamaño de la molécula. Sin embargo, las computadoras cuánticas pueden modelar tales sistemas de manera más eficiente, gracias a su capacidad para manejar múltiples estados simultáneamente.

Además, las computadoras clásicas pueden paralelizar tareas para aumentar la velocidad de los cálculos, pero su estructura sigue siendo fundamentalmente limitada por el número de bits. En contraste, una computadora cuántica de n qubits puede representar simultáneamente 2^n estados diferentes. Esto significa que agregar más qubits a una computadora cuántica puede aumentar exponencialmente su capacidad de procesamiento, algo que es imposible en las computadoras clásicas.

5. VENTAJAS POTENCIALES DE LA COMPUTACIÓN CUÁNTICA

En cuanto a las ventajas potenciales de la computación cuántica podemos citar las siguientes:

- a) Optimización y Resolución de Problemas Complejos: La computación cuántica tiene el potencial de resolver problemas de optimización que son imposibles o inabordables para las computadoras clásicas. Esto tiene aplicaciones en campos como la logística, las finanzas, la ciencia de materiales y la inteligencia artificial.
- b) Simulación de Sistemas Cuánticos: Las computadoras cuánticas son inherentemente adecuadas para simular otros sistemas cuánticos, lo que es crucial en áreas como la química

cuántica y la ciencia de materiales, donde los científicos buscan diseñar nuevos materiales o medicamentos modelando reacciones químicas complejas.

- c) Criptografía Cuántica: Además de los avances en criptografía, los algoritmos cuánticos tienen el potencial de proporcionar comunicaciones seguras. La criptografía cuántica, basada en el intercambio de claves cuánticas (BB84), garantiza la seguridad de las comunicaciones mediante la detección de cualquier intento de espionaje, ya que la mera observación de un sistema cuántico puede alterar su estado.
- d) Aceleración del Aprendizaje Automático (Machine Learning en inglés): En el ámbito de la inteligencia artificial (IA), los algoritmos cuánticos prometen acelerar el proceso de aprendizaje automático mediante el uso de técnicas de optimización avanzadas. Este avance podría permitir entrenar modelos de IA con conjuntos de datos extremadamente grandes en una fracción del tiempo requerido por las técnicas clásicas.

Entre las técnicas de aprendizaje automático clásico y cuántico merece la pena destacar el recientemente desarrollado método de Reservoir Computing, en el que el grupo del autor ha hecho numerosas contribuciones. La base del método consiste en una red aleatoria de nodos de aprendizaje y su extensión cuántica consistente en un conjunto optimizado de puertas lógicas cuánticas.

6. DESAFÍOS TÉCNICOS ACTUALES

Obviamente el camino de la computación cuántica no está siendo un camino fácil, y aunque esta tiene un potencial increíble, todavía enfrenta numerosos desafíos técnicos que deben superarse antes de que pueda desplegarse de manera generalizada.

En primer lugar, existe un enemigo fundamental para este tipo de computación, que es la decoherencia cuántica y el ruido. De hecho, uno de los principales obstáculos en la computación cuántica es la llamada decoherencia cuántica, que ocurre cuando los qubits pierden su estado cuántico debido a interacciones con su entorno. En los sistemas cuánticos, es difícil mantener el aislamiento necesario para que los qubits conserven su coherencia, especialmente en entornos físicos reales donde hay ruido, fluctuaciones de temperatura y campos electromagnéticos que interfieren con los qubits. El ruido y la decoherencia provocan errores en los cálculos, lo que limita la capacidad de las computadoras cuánticas para realizar tareas de manera precisa y eficiente durante períodos de tiempo prolongados.

Para mitigar este problema, los investigadores están trabajando en técnicas de corrección de errores cuánticos. En la computación clásica, la corrección de errores es relativamente sencilla: los bits se copian varias veces y se comparan para detectar y corregir errores. Sin embargo, en la computación cuántica, la mera medición del estado de un qubit altera su estado, lo que hace imposible copiar directamente la información de un qubit. Para sortear este obstáculo, se están desarrollando qubits lógicos utilizando múltiples qubits físicos para representar un solo qubit lógico que puede corregir automáticamente los errores sin necesidad de medir el sistema directamente.

En segundo lugar, otro desafío técnico actual de la computación cuántica es su escalabilidad. Actualmente, los procesadores cuánticos solo cuentan con unas pocas decenas o cientos de qubits, lo que los limita a resolver problemas relativamente simples. Para que las computadoras cuánticas sean útiles a gran escala, es necesario desarrollar procesadores con millones de qubits. Este objetivo enfrenta varios obstáculos técnicos, desde la dificultad de mantener la coherencia de tantos qubits simultáneamente, hasta la fabricación de los propios qubits a una escala masiva. Las empresas e instituciones que lideran la investigación cuántica están experimentando con diferentes enfoques, como qubits superconductores, trampas de iones y qubits fotónicos, cada uno con sus propios beneficios y limitaciones en términos de escalabilidad y estabilidad.

Por último, podemos citar el desarrollo de software cuántico como el tercer reto importante en el camino de la computación cuántica. Aunque se ha avanzado mucho en el hardware cuántico, el software cuántico también plantea desafíos. Desarrollar algoritmos cuánticos eficientes y que puedan ejecutarse

de manera efectiva en las computadoras cuánticas actuales es complicado. Los algoritmos cuánticos, como los de Shor o Grover, han demostrado ser efectivos en teoría, pero implementar estos algoritmos en hardware cuántico real, donde los errores son comunes, requiere nuevas estrategias de programación. Además, existe una falta de herramientas de desarrollo y lenguajes de programación adecuados que permitan a los desarrolladores crear y probar software cuántico general de manera efectiva. A este respecto, una de las iniciativas más prometedoras en este campo es Qiskit, un marco de código abierto desarrollado por IBM que permite a los desarrolladores experimentar con algoritmos cuánticos utilizando tanto simulaciones como hardware cuántico real. Plataformas similares, como Cirq, desarrollado por Google, y Forest, de Rigetti, también están ayudando a democratizar el acceso a la computación cuántica al proporcionar herramientas que permiten la creación y prueba de algoritmos cuánticos.

7. ESTADO DEL ARTE: COMPUTADORAS CUÁNTICAS ACTUALES

Aunque la computación cuántica está en sus primeras etapas, existen ya varios sistemas cuánticos operativos desarrollados por gigantes tecnológicos y startups dedicadas al sector. A continuación, se destacan algunos de los sistemas cuánticos más avanzados (lo que obviamente cambia con extremada rapidez):

IBM Quantum

IBM ha sido uno de los pioneros en el desarrollo de la computación cuántica, lanzando su iniciativa IBM Q Experience en 2016, que permitió por primera vez que investigadores y desarrolladores accedieran a computadoras cuánticas a través de la nube. Su procesador cuántico IBM Eagle, con 127 qubits, es uno de los más avanzados disponibles actualmente y se ha utilizado para probar diversos algoritmos cuánticos. IBM también ha trazado una hoja de ruta que incluye el desarrollo de procesadores cuánticos con más de 1000 qubits para la próxima década, con el objetivo de alcanzar la supremacía cuántica en problemas prácticos.

Google Quantum AI

Google Quantum AI ha estado a la vanguardia de la computación cuántica desde que anunció en 2019 que había alcanzado la supremacía cuántica con su procesador Sycamore. Este sistema, con 53 qubits, resolvió un problema específico en solo 200 segundos que, según Google, le habría tomado a la computadora clásica más poderosa del mundo, Summit, unos 10,000 años. Aunque este logro ha sido objeto de controversia y debate dentro de la comunidad científica, representa un hito importante en el desarrollo de la computación cuántica. Google ha anunciado su intención de desarrollar un procesador cuántico con un millón de qubits en las próximas décadas.

Rigetti Computing

Rigetti es una startup enfocada exclusivamente en la computación cuántica. A diferencia de otras empresas que se centran en la investigación y el desarrollo, Rigetti ha creado una plataforma cuántica que permite a los desarrolladores escribir y probar algoritmos cuánticos a través de la nube. Su enfoque en la computación cuántica híbrida, que combina sistemas cuánticos y clásicos, ha generado interés en la industria por su capacidad de acelerar el desarrollo de soluciones comerciales prácticas.

D-Wave

D-Wave es única en su enfoque, ya que ha desarrollado computadoras cuánticas basadas en la optimización cuántica adiabática, una forma diferente de computación cuántica en comparación con los enfoques basados en qubits tradicionales. Aunque los sistemas de D-Wave no son capaces de ejecutar todos los algoritmos cuánticos, su tecnología ha demostrado ser efectiva en la resolución de problemas de optimización complejos, como los que se encuentran en la logística y el diseño de circuitos. El sistema

más reciente de D-Wave, el Advantage, cuenta con más de 5000 qubits y está disponible a través de su servicio en la nube.

8. FUTURO PRÓXIMO DE LA COMPUTACIÓN CUÁNTICA

El futuro de la computación cuántica es prometedor, aunque también está lleno de desafíos. A corto plazo, es probable que las computadoras cuánticas se utilicen principalmente en entornos de investigación y para aplicaciones altamente especializadas en las que su capacidad para resolver problemas complejos ofrezca una ventaja significativa. Sin embargo, a medida que se desarrollen mejores qubits, mejores algoritmos y se superen los obstáculos técnicos, las aplicaciones prácticas de la computación cuántica podrían comenzar a expandirse a múltiples industrias. Entre las áreas donde es probable que la computación cuántica tenga un impacto en los próximos años podemos citar las siguientes.

En la industria Farmacéutica y diseño de medicamentos, la capacidad de las computadoras cuánticas para simular procesos moleculares a nivel cuántico revolucionará el descubrimiento de nuevos medicamentos. La simulación precisa de interacciones entre moléculas permitirá a los científicos diseñar medicamentos más eficaces y específicos, reduciendo el tiempo y los costos de investigación. Empresas como Pfizer y Boehringer Ingelheim, entre otras, ya están explorando el uso de computadoras cuánticas para acelerar el descubrimiento de fármacos.

En el campo de la energía y materiales avanzados, el desarrollo de nuevos ejemplos, como los superconductores a temperatura ambiente o baterías más eficientes, se verá impulsado por la computación cuántica. Las simulaciones cuánticas permitirán a los científicos explorar nuevas configuraciones atómicas y moleculares que podrían llevar a avances en la eficiencia energética, la durabilidad de los materiales y el desarrollo de tecnologías sostenibles.

En cuanto a las llamadas finanzas cuánticas, el sector financiero es otro de los que se beneficiarán de la computación cuántica. Los problemas de optimización y modelado de riesgo son comunes en la industria financiera, y la capacidad de las computadoras cuánticas para resolver estos problemas de manera exponencialmente más rápida que las computadoras clásicas proporcionará una ventaja competitiva a las instituciones que adopten esta tecnología.

Finalmente, en criptografía cuántica, y como se mencionó anteriormente, la computación cuántica tiene el potencial de romper los sistemas de cifrado clásicos. Sin embargo, también ofrece soluciones a este problema a través de la criptografía cuántica, que garantiza comunicaciones seguras mediante el uso de claves cuánticas que son imposibles de interceptar sin alterar el estado de la transmisión. Se espera en la próxima década que los sistemas de comunicación cuántica comiencen a implementarse en aplicaciones militares, gubernamentales y comerciales.

9. CONCLUSIÓN

La computación cuántica ha pasado de ser una teoría exótica a una realidad tecnológica con aplicaciones emergentes en diversas industrias. Si bien aún estamos lejos de ver computadoras cuánticas en el escritorio de los usuarios comunes, su potencial para resolver problemas que son intratables para las computadoras clásicas es innegable. A medida que se superen los desafíos técnicos actuales, es probable que la computación cuántica se integre cada vez más en nuestras vidas, transformando áreas como la investigación científica, las finanzas, la energía y la seguridad de la información. El futuro de la computación cuántica es emocionante y, aunque todavía queda mucho por hacer, ya podemos vislumbrar cómo esta tecnología cambiará el mundo tal como lo conocemos.