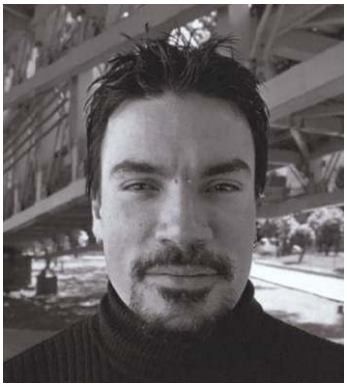
De vuelta a la moda cuántica

DOI: 10.29236/sistemas.n173a2



Las modas vienen y van y muchas veces se repiten. Estamos ahora en la segunda o tercera ola de la "cuántica" tomándose el "main stream" pero esta vez viene con descubrimientos concretos y la posibilidad de afectar nuestro día a día.

Jaime Enrique Gómez Hernández

Un día cualquiera después de una cita odontológica, la doctora, una gran amiga mía, me pidió que le explicara brevemente mecánica cuántica. Vaya mi sorpresa. Para nada dudé de la inteligencia de mi amiga, ni de su capacidad para entender, ni que yo no pudiera explicar los principios cuánticos de forma sencilla, pero con lo que no pude fue con la curiosidad de saber de dónde se había originado la pregunta tan particular.

Sucede que al igual que muchos términos científicos, la denominación de "cuántica" está siendo usada por una corriente de "nueva era" para tratar de validar, darle visos de seriedad o de fundamento formal de sus creencias. Entonces se encuentra uno con términos tan diversos como homeopatía cuántica, coaching cuántico, mente cuántica, sanación cuántica por entrelazamiento de mentes (análogo del entrelazamiento cuántico), en fin, toda una selva de términos. Y sorpresivamente no es una cuestión nueva. Esta manipulación perversa de términos es tan vieja como el habla y es parte de la evolución de las len-

guas humanas, tenga fundamento o no, nos guste o no.

Por ejemplo, hoy en día vivimos el boom de la inteligencia artificial, así esta exista en el mundo de la ciencia ficción hace varias décadas (o quizá más de un siglo): Vicky (I Robot), SkyNet (Terminator), HAL (Odisea 2001), nombres que vienen a mi cabeza. Este tema me parece divertidísimo, sobre todo siendo un lector apasionado por Asimov y ahora que veo todas las sociedades, entidades políticas, gobiernos, EU, ONU, USA, en pánico tratando de regular el uso de las IA y, pero nadie menciona a Asimov, quizá por ser considerado una sobre-simplificación de la ética para IAs, pero sus 3 leyes fundamentales de la robótica serían un muy buen comienzo para una discusión. A propósito, y como nota al margen, el pasado 29 de agosto de 2024 SkyNet tomó conciencia en el universo de Terminator. Lastimosamente, como la gran mayoría de nuestra tecnología es ideada por militares buscando una forma más rápida y eficiente de matarnos entre nosotros, no vamos a hacer nada hasta que lo logremos (Recuerden las bombas H que aun parece que no aprendemos).

Volvamos a los términos populares que nos rondan todo el tiempo, algunos con más resistencia que otros y nuestras disciplinas suelen ser muy propensas a esto por ser consideradas "modernas". Existen muchos en todos los campos del conocimiento humano como "Cloud", "híbrido", "bipolar", "pandemia", "fintech" y yendo más atrás "compacto", "relatividad", "atracción", "coaching", "coworking". etc. Y al volverse términos de moda, estos comienzan a ser utilizados de manera indiscriminada solo por el hecho de sonar elegantes y estar en la vanguardia del conocimiento. Nada más recordar los escalofríos que siento cada vez que escucho a algún servidor público al que le van a "aperturar" una investigación.

Hoy estamos empezando a vivir quizá la segunda o tercera ola del término "cuántico", por varios eventos particulares que están ocurriendo en nuestra época y a pesar de la desconfianza que nos generan los términos de moda, que son usados de manera indiscriminada, esta vez anuncia un cambio de nuestro día a día. El primer evento son los experimentos exitosos del acoplamiento cuántico, cada vez a mayor distancia.

Este fenómeno dicta que dos partículas que pertenecen a un mismo sistema, mantendrán esa relación no importa la distancia entre ellas. En otras palabras, si una cantidad constante que se conserva como el momentum angular o la energía (en mecánica clásica) o los estados en mecánica cuántica, cuando parte del sistema es afectada una de las partículas, la otra reacciona para balancear y conservar los valores /estados. Aun cuando este fenómeno no tiene equivalente en mecánica clásica podemos usar un

ejemplo que todos hemos visto (los experimentos mentales de Einstein): Tomemos el patinador girando que recoge sus brazos y aumenta su velocidad por la conservación de momentum angular del sistema. Ahora separen al patinador y dejen sus patines en el camerino, y observen cómo los patines giran más rápido cuando el patinador cierra sus brazos en el hielo. Así de bizarro es el entrelazamiento cuántico, que no solo es instantáneo, sino que no importa la distancia.

Lo más interesante ocurre cuando empiezo a ver las implicaciones: Yo separo estas partículas relacionadas kilómetros y generó una reacción a distancia implica que estoy, teóricamente, llevando información a velocidades mayores a la velocidad de la luz (1). Sí, tal como se oye y esto es fascinante porque rompe, teóricamente, una camisa de fuerza que nos incomoda a todos: la famosa C que Einstein nos dió en e=mC^2. El mismo Einstein consideraba este fenómeno "espeluznante". Inclusive muchos han llegado a especular que este fenómeno tan particular nos abre la puerta a la teletransportación de la materia, quizá aún demasiada ciencia ficción y en este momento estamos lejos de hacer realidad alguna de estas posibilidades, pero Verne y Wells nos llamarían la atención por incrédulos (3).

El siguiente fenómeno y muy relacionado con el anterior es la expectativa de las redes cuánticas: Como al entrelazar dos partículas y al hacerlas cambiar de estado, estoy transmitiendo información, es natural pensar en mensajes más complejos utilizando la misma tecnología. En 2020 un grupo de investigación china publica en Nature (2) que transmitió un mensaje cifrado a 1200 Km de distancia usando fenómenos cuánticos de entrelazamiento (en 2023 ya se replicó con 3400Km). Además de abrir el camino a las redes cuánticas también es no interceptable. Tratemos de imaginar como intercepta una comunicación de este tipo, no hay cable para cortar ni señal que escuchar. Desconocemos el "medio". Claro está, como todo el conocimiento científico es temporal y pueden ser revaluado, re-escrito, disputado y posiblemente reemplazado; quizá llegue el día que entendamos el entramado del universo del entrelazamiento cuántico y descubramos las partículas que lo transmiten, y solo hasta entonces podamos interceptarlas.

Las redes cuánticas me llevan a soñar con el Ansible de los Fórmicos (originalmente considerada telepatía) en la Saga de Ender de Orson Scott Card que inicia con el "Juego de Ender". En esta serie se habla de unas comunicaciones que llevan mensajes más allá de la velocidad de la luz, a pesar que los viajes espaciales aún siguen siendo relativistas (exactamente la situación que tendríamos algún día) y entonces plantea la proliferación de conocimiento, libros, leyendas y re-

ligiones, más allá de las personas. Como cualquier red social galáctica.

No quiero dejar de mencionar la "detección" cuántica, que no es más que la implementación del scanner de Star Trek donde podían detectar lo que desearan a casi cualquier distancia. La Marina de UK ha probado una tecnología que suena similar a la creación de Rodenberry, pero aún no tenemos mucha información detallada ya que es una publicación militar (7).

Y por último estos fenómenos nos traen a la computación cuántica con todas sus promesas y realidades, algunas sorprendentes y otras decepcionantes. Esta tecnología es considerada el siguiente gran hito en la escala de procesamiento de datos: la escala de crecimiento de la capacidad deja de ser aritmética para ser exponencial. Por lo tanto, el flujo de dinero $$ es inmensa en muchos países concentrando en USA y China, pero sin dejar atrás a Australia, Alemania, Francia, India, Reino Unido, Rusia, Canadá, Japón y Corea del Sur que invierten en su desarrollo

Las realidades hasta el momento son:

- Ya superamos el umbral de la supremacía cuántica: Ya puedo hacer cosas más rápidas con computadoras cuánticas que con tradicionales. En 2019 Google e IBM declararon haberlo conseguido resolviendo un problema en 3:20 minutos que en un supercomputador clásico de 200 petaflops pudiera haberle tomado 10.000 años (4).

- Se están usando para resolver problemas prácticos como la simulación de la hemocianina (5) en una investigación de vacunas contra el cáncer

- Nos despediremos de nuestro querido ciframiento: Un equipo de investigadores de la Universidad de Shanghái (China) anunció que había vulnerado con éxito el cifrado militar. Fue rápidamente desmentido pero la alarma ha sonado: hay equipos trabajando en esto tanto en la vulneración como en la construcción del universo de cifrado cuántico (8).

Lo que no es tan chévere

- Temperatura: Desde el punto de vista de la mecánica estadística, la temperatura no es más que el promedio de velocidad de las partículas. Entonces la temperatura es el peor enemigo ya que introduce variabilidad en los resultados y aumenta la producción de errores. Los computadores cuánticos suelen operar a temperaturas cercanas al cero absoluto lo que introduce costos bastante altos en energía e infraestructura para poder conseguir la temperatura de operación. Es exactamente el mismo problema

de llevar la superconductividad al mundo real: la conocemos hace décadas, pero aún no tengo un tren maglev de superconductores.

- La decoherencia cuántica. Los sistemas cuánticos son extremadamente temperamentales, y mantienen sus estados por períodos cortos de tiempo dependiendo de una infinidad de factores. Esto nos lleva a que "repentinamente" un par de partículas entrelazadas pueden "desconectarse" y olvidar a su compañera, lo que produce el fenómeno de decoherencia cuántica y, por lo tanto, errores en mis cálculos.

- Hijo del anterior, viene la Corrección de Errores: Técnicamente aislar un sistema a nivel cuántico es cercano a imposible y si a esto le agregamos un poco de temperatura, la cuestión se vuelve un sancocho. En computación cuántica esto implica tener un sistema de corrección de errores. Pero no nos engañemos, no lo podemos heredar de ningún protocolo de comunicación, esto es cuántico, lo que implica nuevas tecnologías que aún están en pruebas y desarrollo.

- Tengo que hacer todo de cero: Los cubits no son bits, lo que implica que nada es re-utilizable, ni el álgebra booleana, ni las compuertas, ni los transistores, ni las memorias, ni los algoritmos, ni NADA parecido. Muy parecido a lo que ocurrió en los principios de la mecánica cuántica que fue necesario inventar una notación de bra-kets o formalidad de Dirac. O sea, toca volver a aprender.

Estos problemas eventualmente serán resueltos o al menos mitigados y nos dejarán un mundo completamente nuevo. Esta situación me hace recordar al emérito profesor José Rafael Toro de Uniandes cuando la Universidad decidió adquirir un mini supercomputador Cray J-90 en los años 90s, Y muy preocupado nos decía ... "*¿En que nos metimos? ... Ahora no es el momento de hacer lo mismo más rápido, llegó el momento de cambiar de problemas*…". Lo mismo ocurre con la computación cuántica, una vez esto se normalice iniciaremos a confrontar problemas más complejos de los que hemos venido enfrentando hasta ahora partiendo de nuevos algoritmos hasta nuevas matemáticas. Por ejemplo, la referencia (1) es uno de los casos de sistemas supremamente complejos que harían muy buen uso de la nueva capacidad: usar computadores cuánticos para resolver sistemas cuánticos. Divertido y natural.

Por otro lado, este nuevo mundo trae amenazas que antes consideramos inexistentes. Considerar que el cifrado moderno es vul-nerable, afecta fundamentalmente

uno de los pilares de nuestro universo digital, poniendo en peligro todo lo que consideramos "seguro": las comunicaciones, las transacciones financieras, mis compras, mi privacidad, etc., etc. Y si el cifrado clásico es superfluo, quizá enfrentemos un mundo sin ciframi-ento como ocurre en países en donde está prohibido cifrar (como lo estuvo en Francia durante muchos años) y busquemos asegurar de otra forma o muy seguramente vendrá la siguiente generación de algoritmos basados y ejecutados en computación cuántica lo que obligará a que todos tengamos acceso a ella (la NIST ya está liberando estándares nuevos (8)). ¿O quizá no?, y el gran hermano tome el control.

Referencias

1. Se ha simulado el tiempo que toma el entrelazamiento cuántico y no es instantáneo, pero define attosegundos, o sea, solo 10 a la -18 (10-18) segundos. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.133.163201

2. Redes cuánticas y transmisión instantánea e invulnerable en revista Nature. https://www.nature.com/articles/s41586-020-2401-y

3. Teletransporte cuántico. https://www.xataka.com/investigacion/teleportacion-cuantica-funciona-promete-revolucionar-manera-que-transferimos-informacion

4. Google claims to have reached quantum supremacy. https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17

5. Quantum Embedding of Non-local Quantum Many-body Interactions in Prototypal Anti-tumor Vaccine Metalloprotein on Near Term Quantum Computing Hardware. https://arxiv.org/abs/2410.12733

6. Algoritmo de ataque criptográfico de clave pública basado en procesado cuántico con la ventaja de D-Wave. http://cjc.ict.ac.cn/online/onlinepaper/wc-202458160402.pdf

7. Royal Navy Successfully Tests Quantum-Sensing Technology. https://www.royalnavy.mod.uk/news/2024/october/31/20241101-royal-navy-successfully-tests-quantum-sensing-technology

8. NIST libera 3 estándares de ciframi-ento Post-Cuántico. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Jaime Enrique Gómez Hernández (Pato). *Físico, Ing. Mecánico MSc. Universidad de Los Andes; PhD. Mecánica Computacional Universidad de Gales UK; Becario de Colfuturo, BID, Colciencias y FCO-British Council (Chevening), Profesor Asistente Uniandes en Física e Ing. Mecánica del 1998 a 2002; Coordinador portales de software libre como LinuxCOL y OrfeoLibre; fundador de empresas de tecnología como Azuan, Skina, Simulmax y SkinaTech; Creador y patrocinador de proyectos de software como Orfeo NG, Check, Entregalo, Legacy, Efica y Kuine Linux. Y al final, cocinero, artista marcial, skater, lector. incansable de ciencia ficción y cacharrero permanente de software y hardware.*