Computación Cuántica: ¿el futuro de los procesadores?

Dr. Raúl Rossignoli
Profesor Titular de la UNLP
Investigador Principal CIC
raul.rossignoli@gmail.com

La Mecánica Cuántica es una teoría física fundamental que se desarrolló a comienzos del siglo XX para explicar varios fenómenos que contradecían las predicciones de la Mecánica Clásica, y fue revolucionaria desde un primer momento. Su mismo nombre ya lo delata: proviene de que en ella, magnitudes físicas tales como la energía, pueden estar *cuantizadas*, es decir, pueden tomar sólo ciertos valores discretos, determinados por la ecuación de *Schrödinger*, en lugar de valores continuos como en la mecánica clásica. Introduce también otros conceptos revolucionarios difíciles de asimilar, tales como dualidad onda-partícula, principio de incertidumbre, superposición y entrelazamiento, que generaron en su momento profundas controversias pero cuyas consecuencias fueron finalmente siempre verificadas en los experimentos. Y son estos mismos conceptos, en cuyo desarrollo participaron, además de Schrödinger, otros físicos como Planck, Einstein, De Broglie, Heisenberg y Dirac, los que están generando hoy una nueva revolución en el campo de la computación e informática.

Destaquemos antes que en base a estas osadas ideas, la Mecánica Cuántica logró predecir los niveles de energía atómicos, proporcionando la base para explicar la tabla periódica de elementos y esencialmente toda la química. Se convirtió luego en el marco general para describir sistemas físicos, desde partículas elementales (electrones, quarks, etc.), núcleos atómicos, átomos y moléculas, hasta la estructura estelar. Su campo de aplicación es universal e incluye a la mecánica clásica como caso límite, aunque es en sistemas de dimensiones muy pequeñas donde sus predicciones difieren radicalmente de las proporcionadas por la física clásica.

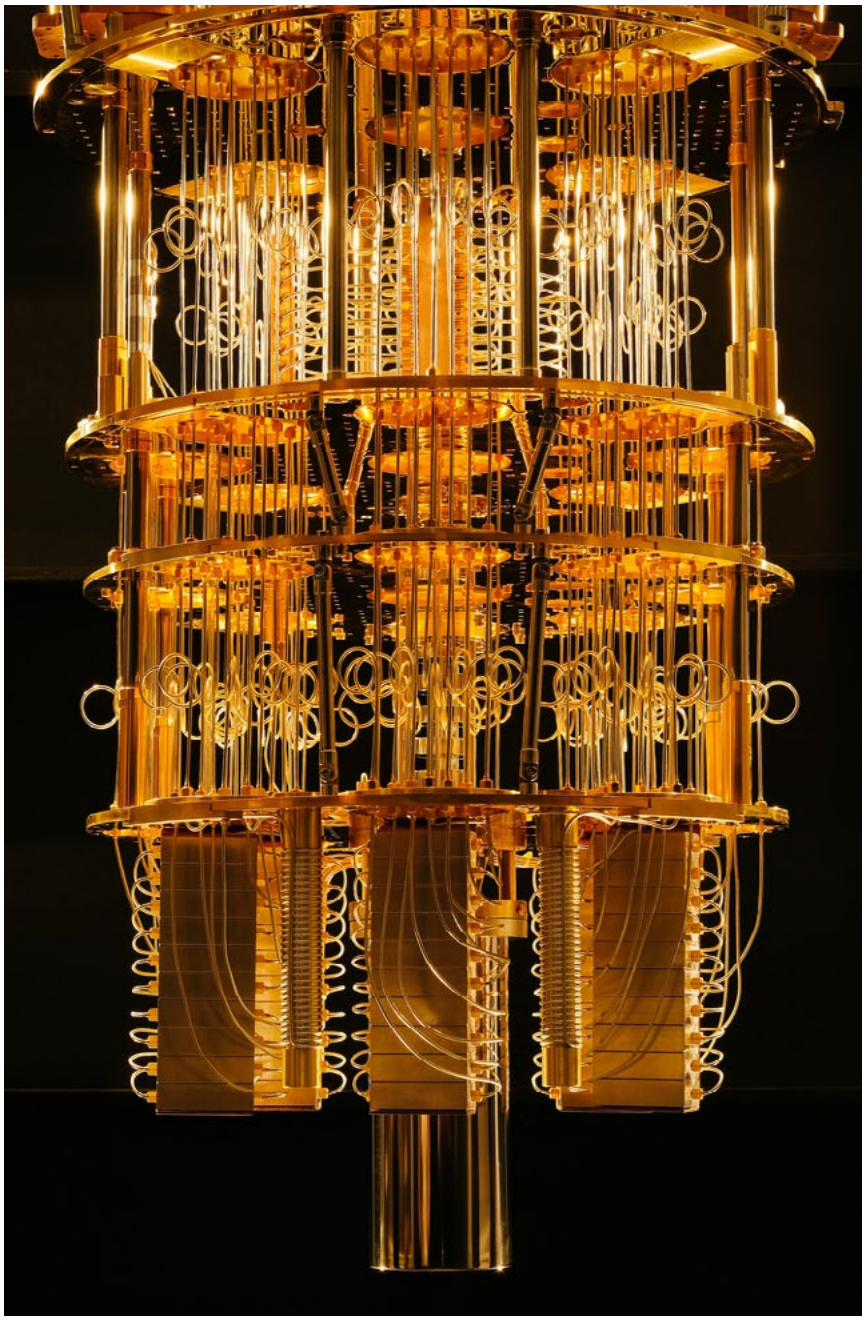
La mecánica cuántica ha sido así fundamental para el desarrollo de nuevas y revolucionarias tecnologías de uso hoy corriente. Podemos mencionar el láser, la resonancia magnética, y en particular el *transistor* (desarrollado por los físicos Bardeen, Brattain y Shockley en 1947), el cual, recordemos, es el componente básico de todo dispositivo electrónico (un microprocesador actual contiene del orden de diez mil millones de transistores). Puede entonces afirmarse que sin la mecánica cuántica, no existirían las computadoras electrónicas actuales.

Sin embargo, hasta el momento su influencia en la informática estuvo limitada al hardware. La codificación y procesamiento de la información en una computadora actual sigue siendo *totalmente clásica*, basada esencialmente en bits, que pueden tomar únicamente dos valores definidos: 0 y 1.

La *computación cuántica*, en cambio, es una nueva forma de representar y procesar la información, basada *expresamente* en las leyes de la mecánica cuántica. A diferencia de la computación clásica, se basa en *qubits (quantum bits)*, que pueden estar no sólo en dos estados dados, digamos 0 y 1, sino también en *cualquier superposición* de ellos, de acuerdo a uno de los principios básicos de la mecánica cuántica. Esta propiedad es justamente la que habilita el *paralelismo cuántico:* una computadora cuántica puede procesar dos entradas distintas, digamos 0 y 1, naturalmente en un solo paso, mediante la superposición de ambas entradas en una sola. Y la superposición puede también aplicarse a un número arbitrario de entradas. Los qubits pueden implementarse físicamente-te de distintas formas, por ejemplo mediante la polarización de un fotón. En este caso, si 0 y 1 corresponden a polarización vertical y horizontal, la superposición de ambos corresponde simplemente a otro tipo de polarización (también fácil de generar), que dependerá del peso relativo de cada estado en la superposición.

Utilizando el paralelismo cuántico, el físico David Deutsch y el matemático Richard Josza desarrollaron en 1992 (a partir de un algoritmo previo de Deutsch de 1985) un primer algoritmo cuántico determinista para un problema específico, que es *exponencialmente más veloz que el mejor algoritmo clásico:* Para n bits reduce el número de pasos de 2n-1 + 1 a solamente *uno*. Si bien el problema no es particularmente útil (determinar si una función binaria de n bits es constante o balanceada), el resultado no deja de ser impactante. Muestra que la mecánica cuántica es capaz de reducir, al menos en este caso, la complejidad algorítmica posibilitando un algoritmo *que no puede ser simulado eficientemente por un algoritmo clásico.*

El gran salto lo dio luego el matemático Peter Shor en 1994, cuando, inspirado por el resultado anterior, desarrolló su famoso algoritmo cuántico de factorización. Este algoritmo logra factorizar (en términos de sus factores primos) un número entero de n bits en un número de pasos que es esencialmente *polinomial* en n, mientras que el mejor algoritmo clásico conocido requiere un número de pasos esencialmente *exponencial* en n. A diferencia del anterior, este sí es un



problema de gran importancia, ya que gran parte de la criptografía de clave pública utilizada corrientemente (RSA) se basa precisamente en la dificultad de factorizar un número entero. El esquema propuesto por Shor, quien también introdujo luego la teoría cuántica de corrección de errores, se basa en un algoritmo cuántico desarrollado por él para la evaluación de la transformada de Fourier discreta, que logra una reducción exponencial del número de pasos y posee además otras importantes aplicaciones. Estos algoritmos violan entonces la llamada Tesis *extendida* de Church-Turing, según la cual todo algoritmo puede ser simulado *eficientemente* por una máquina de Turing (en general probabilística). Al menos algunos algoritmos cuánticos no cumplen este enunciado, dando lugar en la teoría de la complejidad a la nueva categoría BQP: la clase de problemas que pueden ser resueltos eficientemente en una computadora cuántica.

Siguió luego el famoso algoritmo cuántico de búsqueda desarrollado por Lov Grover (informático de origen hindú) en 1995. Explicado en forma simple, este algoritmo logra encontrar un elemento en una base de n datos desordenados (un problema también de gran importancia) mediante un número de evaluaciones proporcional a *la raíz cuadrada de n*, que es mucho menor (para n grande) que los n/2 pasos requeridos en promedio por cualquier algoritmo clásico. Si bien la reducción no es exponencial, el resultado muestra la posibilidad cuántica de mejorar la eficiencia aún en un caso en principio "imposible", que es NP completo según la teoría de la complejidad.

Estos notables algoritmos desencadenaron entonces la carrera para construir la primera computadora cuántica que pueda implementarlos, lo cual plantea un enorme desafío tecnológico. Su funcionamiento exige un altísimo grado de control sobre los sistemas cuánticos: se deben preparar los qubits en un

estado inicial determinado, hacerlos evolucionar e interactuar en forma controlada sin decoherencia y luego medirlos individualmente. No obstante, ya están disponibles algunos prototipos: Desde 2016 IBM ofrece la posibilidad de usar online una computadora cuántica, que primero constaba de 5 qubits, y desde 2017 de 16 qubits. Y en diciembre de 2017 anuncia la disponibilidad de un procesador cuántico de 20 qubits y un prototipo con 50 qubits. Notemos que la capacidad aumenta exponencialmente con el número de qubits, duplicándose cada vez que se agrega un qubit. Por otro lado, ya en 2007 la compañía canadiense D-Wave anunciaba un procesador cuántico con 28 qubits, y en 2017 presentó uno con 2048 qubits. No obstante, a diferencia de los anteriores, estos son en realidad "quantum annealers", que sirven para ciertos problemas y simulaciones específicas, siendo su eficiencia tema de controversias. En esta carrera, en marzo de 2018 Google también anunció un procesador cuántico de 72 qubits.

Más allá de sus limitaciones (deben funcionar a bajas temperaturas y por el momento soportan tiempos de operación muy reducidos), estas primeras realizaciones parecen indicar que una computadora cuántica eficiente con un número de qubits suficiente como para alcanzar la denominada *supremacía cuántica*, puede ser una realidad en un futuro no muy lejano. Cabe destacar además que una computadora cuántica resulta especialmente apta para simular eficientemente otros sistemas cuánticos. Estos no admiten, en general, una simulación clásica eficiente, ya que el número de parámetros necesarios para describirlos aumenta exponencialmente con el número de componentes. Este uso, sugerido por el físico Richard Feynman ya en 1981, tiene un gran potencial y abre grandes posibilidades en ciencias de materiales y química cuántica, constituyendo uno de los principales objetivos de la computación cuántica.

Luego del algoritmo de Grover, se introdujeron también otros modelos de computación cuántica, entre ellos el DQC1, que a diferencia de los algoritmos cuánticos anteriores, se basa expresamente en estados cuánticos *no puros* (es decir, con ruido). Si bien no es universal, logra resolver eficientemente ciertos problemas para los que no existe un algoritmo clásico polinomial. También fue introducido en 2012 el modelo de "boson sampling" (muestreo bosónico), que permite determinar en forma eficiente una cierta distribución que es clásicamente intratable (problema de categoría "sharp P" o #P en teoría de la complejidad), requiriendo nuevamente menores recursos cuánticos. Estos modelos son en principio más fáciles de implementar que una computadora cuántica universal.

Finalmente, es importante destacar que el desarrollo de la computación cuántica no se dio en forma aislada, sino en el marco de la nueva revolución cuántica, surgida durante la última década del siglo XX, en la que se comenzó a develar el potencial de la mecánica cuántica para nuevas formas de transmisión y procesamiento de la información. En 1993 se introdujo la *teleportación cuántica*, la cual, a partir del entrelazamiento (una característica fundamental de las correlaciones en sistemas cuánticos que no posee análogo clásico) permite transferir el estado de un sistema cuántico a otro sistema remoto. Esto originó una nueva forma de comunicación y convirtió al entrelazamiento, que hasta entonces era considerado como una peculiaridad de la mecánica cuántica, en un recurso. La primera implementación física data ya de 1997, y en 2017 un equipo chino logró teletransportar el estado de polarización de fotones entre una estación en el Tibet y un satélite en órbita, separados nada menos que por 1400 km, batiendo todos los records anteriores.

Asimismo, mientras que el algoritmo de Shor puede destruir la criptografía de clave pública convencional basada en RSA, la mecánica cuántica posibilita al mismo tiempo una criptografía cuántica, basada en lo que se denomina distribución cuántica de claves (QKD en inglés). El primer protocolo QKD data ya de 1984, y en 1991 Artur Ekert desarrolla un protocolo QKD basado en el entrelazamiento. Su característica principal puede resumirse (en forma simplificada) en que no es posible "espiar" o "interceptar" la distribución sin destruirlas y sin que las partes lo detecten. Existen varias compañías que ofrecen sistemas criptográficos cuánticos y también varias redes de distribución cuántica de claves en uso. Al mismo tiempo, la creciente posibilidad de existencia de una computadora cuántica generó ya la denominada criptografía post-cuántica, enfocada en generar esquemas de criptografía clásica de clave pública que no pueden ser quebrados por una computadora cuántica.

Existen asimismo otros desarrollos cuánticos recientes radicalmente nuevos que emplean el entrelazamiento y otras propiedades cuánticas como ingrediente esencial, tales como metrología cuántica, radares cuánticos (que pueden detectar objetos invisibles para los radares convencionales), *quantum machine learning* (aprendizaje automático cuántico), etc. Existen varios grupos en el país, y también en el Depto. de Física de la UNLP, dedicados a la investigación en información cuántica, computación cuántica y otros aspectos fundamentales de la mecánica cuántica, tanto en forma teórica como experimental. Por otro lado, el apoyo que se le está dando a estas investigaciones en otros países es actualmente enorme, habiéndose creado recientemente varios institutos dedicados exclusivamente a las ciencias de la información cuántica.