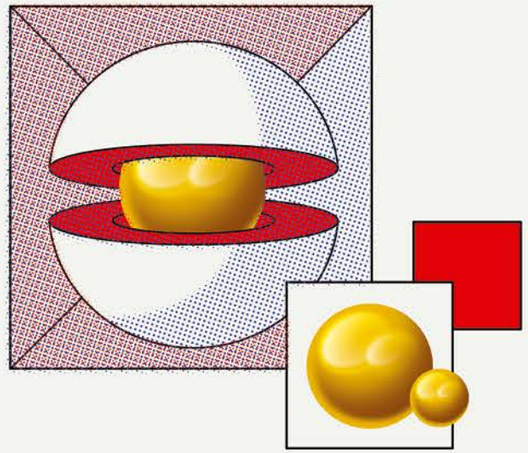


Palabras clave: computación cuántica, supremacía cuántica, criptografía, inteligencia artificial, simulación.

ELÍAS F. COMBARRO

Las verdaderas capacidades de los ordenadores cuánticos

COMPUTACIÓN CUÁNTICA: MITOS Y REALIDADES

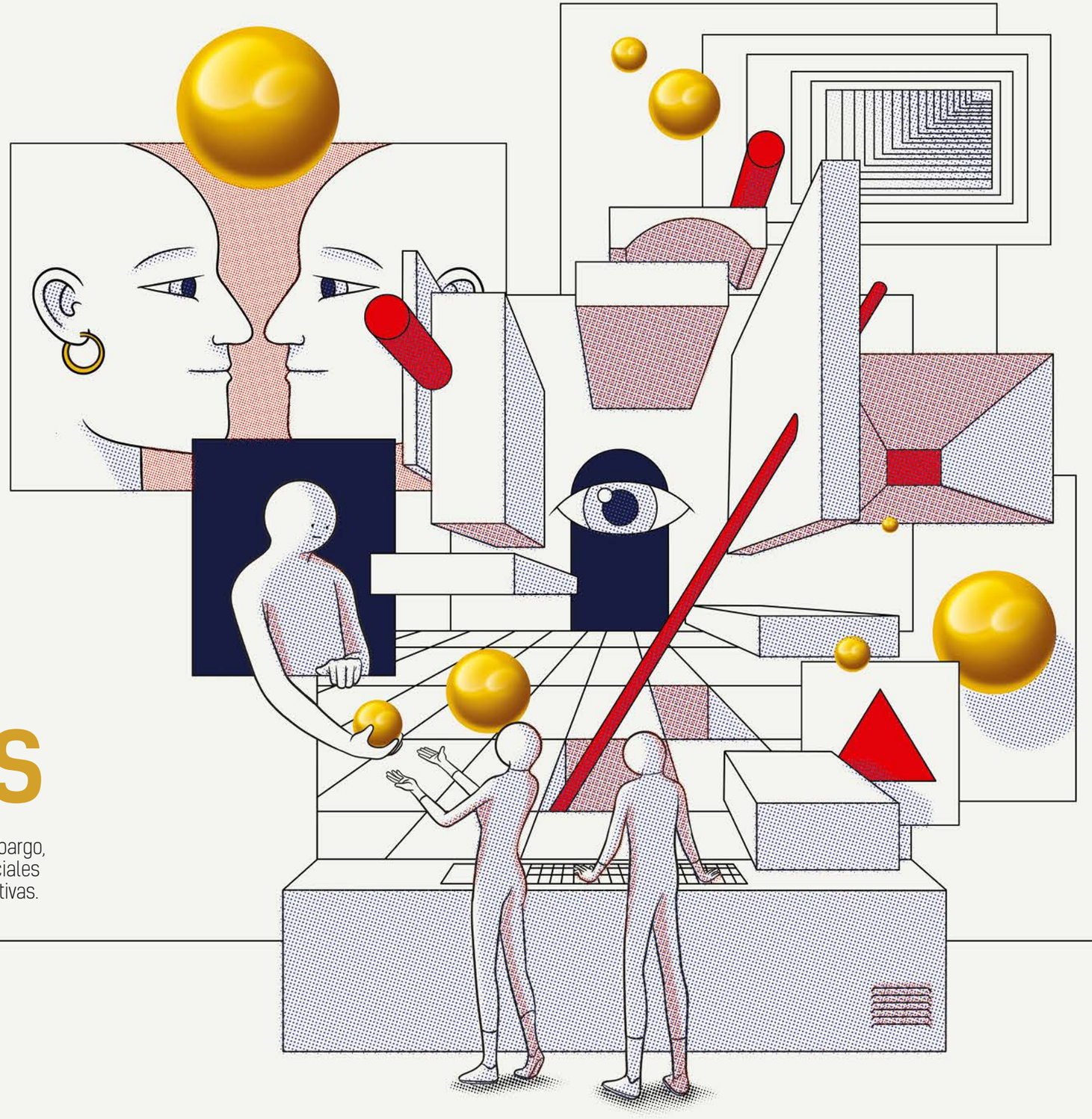
La computación cuántica es una tecnología llamada a transformar nuestra sociedad. Sin embargo, sus verdaderas capacidades son a menudo incomprendidas y mitificadas. Explicar las potenciales aplicaciones de los ordenadores cuánticos ayuda a disipar dudas y a desterrar falsas expectativas.

The true capabilities of quantum computers

QUANTUM COMPUTING: MYTHS AND REALITIES

Quantum computing is a technology that is set to transform our society. However, its true capabilities are often misunderstood and mythologized. Explaining the potential applications of quantum computers helps to dispel doubts and banish false expectations.

Keywords: *quantum computing, quantum supremacy, quantum supremacy, cryptography, artificial intelligence, simulation.*



En octubre de 2019, la computación cuántica acaparó durante varios días titulares de noticias en todo el mundo. Un equipo de investigadores del gigante tecnológico Google había conseguido alcanzar la supremacía cuántica, venciendo a los supercomputadores más grandes del planeta con un ordenador cuántico. No solo eso, sino que la diferencia de tiempos resultaba sencillamente apabullante: unos pocos minutos frente a los miles de años necesarios para realizar el mismo cálculo con un ordenador tradicional.

Decenas de artículos y reportajes en prensa, radio y televisión se hicieron eco de este hito histórico e intentaron explicar al público no especializado en qué consistía realmente el logro de Google y qué eran esos misteriosos ordenadores cuánticos que se habían utilizado para conseguirlo. Pese a su buena intención, la mayor parte de estas explicaciones deben haber sembrado más dudas que las que consiguieron aclarar.

Y es que en los artículos de divulgación sobre computación cuántica es habitual encontrar una serie de analogías e imágenes recurrentes que no se corresponden con la realidad y que contribuyen a crear falsos mitos alrededor de las verdaderas capacidades de los ordenadores cuánticos. Una de las más repetidas es aquella de que "un ordenador cuántico encuentra la solución a un problema probando simultáneamente todas las opciones posibles". Esta explicación no simplifica en demasía el funcionamiento de los computadores cuánticos, sino que parece dotarlos de fantásticos superpoderes mediante los que completar cualquier cálculo es cuestión de pulsar un botón y esperar unos pocos segundos.

Pero, entonces, ¿no es cierto que un ordenador cuántico usa un paralelismo masivo para explorar, al mismo tiempo, todas las soluciones de un problema? Como en muchas cosas que tienen que ver con el mundo cuántico, la respuesta es, a la vez, sí y no. Es verdad que una de las principales propiedades en las que se apoyan los algoritmos cuánticos es la superposición, esa misteriosa tendencia de ciertos sistemas físicos a encontrarse en una combinación de varios estados distintos. Pero esa es únicamente una parte, y bastante pequeña, de toda la historia.

Podríamos definir la computación cuántica como la disciplina que estudia el uso de las propiedades de las partículas subatómicas para realizar cálculos. Entre estas propiedades se encuentra, sí, la superposición, pero también el entrelazamiento y la interferencia. En cierta forma, podríamos decir que un algoritmo cuántico primero crea una superposición de muchas posibilidades a explorar, luego entrelaza estas posibilidades con sus resultados y, finalmente, consigue que las soluciones malas interfieran entre sí para que solo sobrevivan aquellas que nos interesan.

Esta fase de aniquilar opciones desfavorables es la parte más difícil y delicada de todo el proceso, una especie de compleja coreografía matemática, por usar las palabras de Scott Aaronson y Zach Weinersmith[1], que solo sabemos llevar a cabo en algunos problemas concretos. Es más, hace tiempo que se ha demostrado que en determinadas tareas no es posible aprovechar la computación cuántica para conseguir acelerar los cálculos con respecto a los ordenadores tradicionales.

Un ordenador cuántico no es, por tanto, ese dispositivo mágico capaz de resolver al instante cualquier problema que a veces nos quiere vender la prensa sensacionalista. Pero tampoco es, simplemente, un ordenador más rápido.

1 **Scott Aaronson** y **Zach Weinersmith** trabajaron en un maravilloso proyecto educativo para explicar la mecánica cuántica y la computación cuántica mediante cómics.

Podríamos definir la computación cuántica como la disciplina que estudia el uso de las propiedades de las partículas subatómicas para realizar cálculos

No solo más rápidos

Otra de las falacias que es habitual encontrar en los artículos populares sobre ordenadores cuánticos es la reducción de todas sus capacidades a un mero incremento de velocidad. He perdido la cuenta de la cantidad de ocasiones en las que me he encontrado explicaciones como "científicos desarrollan un ordenador cuántico un millón de veces más rápido que los ordenadores tradicionales". Por llamativas que puedan resultar estas afirmaciones, son totalmente erróneas.

Estamos acostumbrados a que, cada pocos meses, los grandes fabricantes de microchips anuncien nuevos desarrollos que consiguen ser un veinte, un treinta o un cincuenta por ciento más veloces que sus predecesores. Pero un ordenador cuántico no basa su funcionamiento en un simple avance en la tecnología que permita hacer las mismas operaciones de forma más rápida.

Por un lado, es posible que para algunas tareas un ordenador cuántico no supere en velocidad a un ordenador clásico. Pero es que en los casos en los que un computador cuántico ofrece una ventaja sobre los dispositivos tradicionales, las diferencias no se pueden medir con un único número. Un ordenador cuántico ejecuta algoritmos radicalmente diferentes de los que usa un ordenador clásico, lo que hace que la ventaja del dispositivo cuántico crezca más cuanto más grande sea el tamaño del problema que queremos resolver. Por ejemplo, para problemas de búsqueda en listas, un ordenador cuántico será cinco veces más rápido que uno tradicional con cien datos, cincuenta veces más rápido con diez mil elementos y quinientas veces más rápido con un millón de registros.

Aplicaciones

Es precisamente este aumento de la ventaja de los ordenadores cuánticos al crecer el tamaño de los datos a procesar lo que los hace especialmente atractivos a la hora de abordar problemas que son intratables con ordenadores tradicionales. Es el caso de tareas como encontrar los factores de números

enteros muy grandes, en cuya dificultad se basa la seguridad de muchos de los protocolos de cifrado que se usan en nuestras comunicaciones digitales. El tiempo necesario para resolver este problema utilizando los mejores algoritmos clásicos disponibles crece casi exponencialmente con la longitud de los números, por lo que aumentar en unas pocas decenas de bits el tamaño de una clave la haría millones de veces más segura. Sin embargo, el matemático Peter Shor[2] demostró hace más de veinte años que romper este tipo de cifrado sería viable en la práctica si se usaran algoritmos cuánticos.

La criptografía no es el único campo en el que los ordenadores cuánticos pueden ofrecer una gran ventaja con respecto a la computación tradicional. Por ejemplo, la simulación de nuevos materiales o el estudio de compuestos químicos son dos de las aplicaciones más prometedoras de la computación cuántica. Se trata, nuevamente, de tareas extremadamente difíciles para los ordenadores clásicos porque el número de parámetros que describen el comportamiento de los sistemas físicos y químicos crece exponencialmente con la cantidad de partículas que los componen. Pero las propiedades cuánticas de este tipo de sistemas hacen que su simulación con ordenadores cuánticos resulte natural, como señaló el físico Richard Feynman[3] incluso antes de que la computación cuántica existiera como disciplina científica.

Así, son muchos los investigadores que en los últimos años han desarrollado algoritmos específicamente pensados para estudiar propiedades de moléculas químicas mediante ordenadores cuánticos. Uno de los más famosos es el llamado *Variational Quantum Eigensolver* (VQE), que presenta la particularidad de poder ser usado incluso con los ordenadores cuánticos, pequeños y sensibles al ruido, de los que disponemos hoy en día. Con este método, se ha conseguido simular en *hardware* cuántico real algunas moléculas de tamaño reducido, alcanzando una precisión equivalente a la de los cálculos clásicos. Aunque aún estamos lejos de superar a los ordenadores tradicionales en esta tarea, el ritmo de crecimiento de las capacidades de los computadores cuánticos y las mejoras en los algoritmos que se utilizan nos hacen suponer que posiblemente esta sea una de las primeras aplicaciones prácticas de la tecnología.

Computación cuántica e IA

Otros campos en los que la investigación de las aplicaciones de la computación cuántica es especialmente intensa en la actualidad son la inteligencia artificial y la optimización. En concreto, son varios los algoritmos cuánticos que se han propuesto para acelerar las tareas implicadas en el entrenamiento de modelos de *machine learning* a partir de grandes colecciones de datos.

En algunos casos, con técnicas parecidas a las empleadas por Shor en el desarrollo de su algoritmo de factorización, se consigue una ganancia exponencial con respecto al correspondiente método clásico. Sin embargo, puesto que debemos trasladar uno a uno los datos al ordenador cuántico desde los ficheros en que se almacenan, el cuello de botella se encontraría no en el procesamiento de la información, sino en la lectura de la misma. Posibles soluciones serían el uso de datos captados directamente con sensores cuánticos, lo que evitaría tener que cargarlos desde un dispositivo externo, o el desarrollo de memorias cuánticas que permitan leer datos en superposición.

Además del estudio de técnicas para acelerar los procesos del aprendizaje automático clásico, también se investigan modelos puramente cuánticos como, por ejemplo, las llamadas redes neuronales cuánticas. Puesto que estas propuestas son relativamente recientes, no se conocen aún todas sus capacidades, pero se dispone de evidencias que muestran que su rendimiento es superior al de los métodos clásicos con ciertos conjuntos de datos creados de forma artificial.

Como bien ha señalado John Preskill, uno de los mayores expertos en computación cuántica del mundo, del mismo modo que las aplicaciones de las redes neuronales clásicas se han ido desarrollando sin necesidad de tener, en todos los casos, una teoría sólida y exhaustiva que las sustentara, el aumento en la disponibilidad de ordenadores cuánticos en los que ejecutar y ajustar redes neuronales cuánticas muy posiblemente conducirá a encontrar casos de uso que hoy no podemos prever.

Los ordenadores cuánticos no son la solución a todos los problemas computacionales y de tratamiento de datos que podamos plantear. No son dispositivos mágicos con los que se pueda realizar instantáneamente cualquier cálculo. Pero tampoco son solamente versiones más rápidas de los ordenadores de los que disponemos hoy. En las tareas en las que es posible obtener una ventaja mediante el uso de la computación cuántica, la ganancia en tiempo de ejecución aumenta cuando el tamaño del problema se hace más grande.

Si tenemos en cuenta que las aplicaciones de los ordenadores cuánticos incluyen campos de tanta relevancia como la ciberseguridad, la simulación de procesos físicos y químicos o la inteligencia artificial, el hecho de que la computación cuántica no sea una herramienta que sirva para todo no disminuye su valor sino que simplemente lo matiza. Disponer de ordenadores cuánticos no significará el fin de nuestras limitaciones de cómputo, pero podemos dar por seguro que supondrá un profundo cambio en nuestra forma de calcular y procesar datos y, por tanto, una transformación radical de nuestra sociedad.

Un ordenador cuántico ejecuta algoritmos radicalmente diferentes de los que usa un ordenador clásico

2 **Peter Shor** es un profesor estadounidense de matemáticas aplicadas en el MIT, reconocido por su trabajo en computación cuántica. Es el artífice del algoritmo de Shor, uno de los algoritmos cuánticos más famosos.

3 **Richard P. Feynman** fue un físico teórico estadounidense conocido por sus trabajos en la formulación por integrales de camino en la mecánica cuántica. Está considerado uno de los artífices del desarrollo de la bomba atómica durante la Segunda Guerra Mundial.

Bibliografía

Arute, F.; Arya, K.; Babbush, R. *et al.* (2019): "Quantum supremacy using a programmable superconducting processor" en *Nature*. Disponible en: https://www.nature.com/articles/s41586-019-1666-5

Aaronson, S. y **Weinersmith, Z.**: "The Talk" en *SMBC Comics*. Disponible en: https://www.smbc-comics.com/comic/the-talk-3

Feynman, R. (1982): "Simulating physics with computers" en *International Journal of Theoretical Physics*.

Preskill, J. (2018): "Quantum computing in the NISQ era and beyond" en *Quantum*. Disponible en: https://quantum-journal.org/papers/q-2018-08-06-79/