
HACIA LA COMPUTACIÓN CUÁNTICA UNIVERSAL

JUAN MIGUEL IBÁÑEZ DE ALDECOA QUINTANA

Un ordenador cuántico universal es una máquina que, en teoría, podría realizar cualquier cálculo que pueda ser descrito por un algoritmo cuántico. En efecto, los ordenadores cuánticos universales son una nueva clase de computadores que aprovechan los principios de la mecánica cuántica para realizar cálculos de una manera fundamentalmente diferente a los ordenadores clásicos. Sin embargo, su construcción plantea numerosos desafíos, entre los que se encuentran la dificultad de mantener la coherencia de los cúbits, el desarrollo de técnicas eficientes de corrección de errores y la escalabilidad ya que aumentar el número de cúbits es otro de los retos de los ordenadores cuánticos universales. En el presente trabajo se realizará un recorrido por la simulación y la computación cuántica, con el objeto de distinguir entre simulación y computación cuántica y entre simulación y computación cuántica analógicas y digitales, hasta llegar a los ordenadores cuánticos universales.

Un ordenador cuántico universal es una máquina con un potencial revolucionario, pero aún se encuentra en una etapa temprana de desarrollo. Aunque se han logrado avances significativos en los últimos años, todavía existen numerosos desafíos por superar antes de que los ordenadores cuánticos universales puedan ser utilizados de manera generalizada. Varias empresas y laboratorios de investigación han desarrollado prototipos de ordenadores cuánticos con un número creciente de cúbits. Estos sistemas son capaces de realizar cálculos

cuánticos básicos y han demostrado su potencial para resolver ciertos problemas de forma más eficiente que los ordenadores clásicos. Se ha presenciado un progreso notable en los últimos años, con empresas como IBM, Google y muchas otras invirtiendo fuertemente en esta tecnología.

Las siglas NISQ (Noisy Intermediate-Scale Quantum) definen de manera precisa la etapa actual de desarrollo de la computación cuántica. ¿Pero qué significa NISQ?

- N de Ruidoso (Noisy): los cúbits son extremadamente sensibles a las perturbaciones del entorno, lo que introduce ruido en los cálculos y limita la precisión.
- I de Intermedio (Intermediate): los ordenadores cuánticos actuales tienen un número limitado de cúbits, lo que los sitúa en una escala intermedia entre los pequeños sistemas de prueba y los grandes ordenadores cuánticos universales que aún están por llegar.
- S de Escala (Scale): se refiere al tamaño de los sistemas cuánticos actuales, que, aunque están creciendo rápidamente, todavía no han alcanzado la escala necesaria para resolver problemas que están fuera del alcance de los supercomputadores clásicos.

En cualquier caso, a pesar de que la computación cuántica se encuentra en la era NISQ se presentan oportunidades, como, por ejemplo, el desarrollo de algoritmos cuánticos específicos, diseñados para aprovechar las capacidades de los ordenadores

NISQ y resolver problemas específicos, en finanzas, diseño de materiales y simulación de moléculas, entre otros. Además, los ordenadores NISQ permiten a los investigadores explorar nuevas aplicaciones de la computación cuántica y aprender a programar y utilizar estos sistemas. Como desafíos es necesario señalar la corrección de errores ya que la presencia de ruido limita la precisión de los cálculos por lo que es necesario desarrollar técnicas de corrección de errores más eficientes. Otro desafío es la escalabilidad ya que aumentar el número de cúbits permite avanzar hacia ordenadores cuánticos más grandes y potentes.

A medida que se avance en la era NISQ es de esperar que los fabricantes de hardware cuántico continuarán aumentando el número de cúbits, una mejora en la calidad de los cúbits ya que se desarrollarán nuevas tecnologías para reducir el ruido y aumentar la coherencia de los cúbits y la comunidad científica continuará explorando nuevas aplicaciones de la computación cuántica y desarrollando algoritmos más eficientes.

Predecir con precisión cuándo se superará la etapa NISQ es un desafío, ya que depende de múltiples factores tecnológicos y científicos que aún están en desarrollo. La transición a una era post-NISQ, caracterizada por ordenadores cuánticos capaces de realizar cálculos tolerantes a fallos y a gran escala, requerirá avances significativos en varias áreas. Entre estos avances se encuentran el aumento del número de cúbits, la reducción del ruido para permitir cálculos más largos y complejos, y la corrección de errores cuánticos a gran escala, esencial para garantizar la fiabilidad de los cálculos. Asimismo, la búsqueda de nuevos materiales y arquitecturas cuánticas podría revolucionar la construcción de ordenadores cuánticos, además del desarrollo de algoritmos cuánticos más eficientes y adaptados a las características de los ordenadores cuánticos de próxima generación.

Existen opiniones divergentes con respecto a la transición a la era post-NISQ. Algunos estiman que podría ocurrir en una década, mientras que otros creen que podrían pasar varias décadas. El tiempo exacto dependerá de la velocidad a la que se resuelvan los

desafíos técnicos mencionados anteriormente y de la inversión en investigación y desarrollo. Es probable que la transición a la era post-NISQ sea gradual, con mejoras incrementales en el rendimiento de los ordenadores cuánticos a lo largo de los años. A medida que los ordenadores cuánticos se vuelvan más potentes, se abrirán nuevas posibilidades en campos como la ciencia de materiales, la medicina, la inteligencia artificial y la criptografía. Y, además, es muy probable que los ordenadores cuánticos y los clásicos coexistan durante mucho tiempo, complementándose en diferentes tareas.

En cualquier caso, la computación cuántica es un campo en constante evolución y determinar cuál es el ordenador cuántico más potente en un momento dado puede ser complicado, ya que las métricas de potencia pueden variar y las tecnologías están en constante desarrollo. No obstante, algunas empresas y laboratorios destacan por sus avances en esta área. Entre los principales competidores encontramos a:

- IBM: ha sido un líder en la computación cuántica durante años, y regularmente anuncia nuevos procesadores cuánticos con un mayor número de cúbits. Por ejemplo, a finales de 2022, IBM presentó Osprey, un procesador cuántico de 433 qubits.
- Google: también es un jugador clave en este campo, y ha logrado algunos hitos importantes, como la demostración de la "supremacía cuántica".
- Rigetti Computing: esta empresa se enfoca en el desarrollo de procesadores cuánticos modulares y escalables.
- IonQ: Utiliza iones atrapados para construir sus cúbits y ha demostrado una alta fidelidad en sus operaciones cuánticas.
- Xanadu: Se enfoca en la computación cuántica fotónica y ha desarrollado procesadores cuánticos basados en fotones.

Sin embargo, la primera empresa en comercializar un ordenador cuántico, en concreto, un ordenador cuántico analógico, o quantum annealer fue la compañía ca-

nadiense D-Wave Systems. En el presente trabajo, se realizará un recorrido por los distintos simuladores y ordenadores cuánticos, analógicos y digitales y se mostrarán las diferencias entre ambos, hasta llegar al ordenador cuántico universal, así como se hará mención también a las diferentes plataformas para la construcción de chips cuánticos.

SIMULADOR CUÁNTICO

Un simulador cuántico es, en esencia, un ordenador diseñado para imitar el comportamiento de sistemas cuánticos. Por ejemplo, una máquina que pueda recrear y estudiar las propiedades de átomos, moléculas o incluso materiales a nivel cuántico. Esto es precisamente lo que un simulador cuántico permite. Un simulador cuántico utiliza sistemas cuánticos controlados (como átomos individuales, iones o fotones) para representar el sistema que se quiere simular. Al manipular estos sistemas cuánticos de manera precisa, se pueden simular las interacciones y evoluciones del sistema original.

En definitiva, un simulador cuántico, es un dispositivo diseñado específicamente para emular o replicar el comportamiento de un sistema cuántico particular. Los simuladores cuánticos no buscan ser máquinas universales; en su lugar, están optimizados para modelar fenómenos cuánticos específicos, como la interacción de electrones en un material o las reacciones químicas en moléculas complejas.

Muchos sistemas naturales, desde la superconductividad hasta la fotosíntesis, se basan en principios cuánticos. Los simuladores cuánticos nos permiten explorar estos fenómenos de una manera que los ordenadores clásicos no pueden. Al simular el comportamiento de nuevos materiales a nivel atómico, se pueden diseñar materiales con propiedades específicas, como superconductores a temperatura ambiente o materiales más eficientes para almacenar energía. Además, simular el comportamiento de moléculas complejas podría acelerar el descubrimiento de nuevos medicamentos. También, los simuladores cuánticos pueden ayudar a probar teorías

fundamentales de la física, como la gravedad cuántica.

Los simuladores cuánticos pueden ser digitales o analógicos: los primeros son como ordenadores cuánticos de propósito general, pero optimizados para realizar simulaciones cuánticas, los segundos están diseñados para simular sistemas cuánticos específicos, y suelen ser más eficientes para tareas concretas.

La diferencia con un ordenador cuántico es que mientras un ordenador cuántico está diseñado para realizar una amplia gama de cálculos, un simulador cuántico está especializado en simular sistemas cuánticos. Un simulador cuántico puede ser considerado como un tipo específico de ordenador cuántico.

EMULADOR CUÁNTICO

Un emulador cuántico es un software o sistema clásico diseñado para simular el comportamiento de un sistema cuántico. Es una herramienta utilizada en computación cuántica para probar y analizar algoritmos cuánticos en un entorno clásico (sin necesidad de usar un hardware cuántico real). Los emuladores cuánticos permiten a los investigadores, ingenieros y científicos experimentar con algoritmos cuánticos y entender cómo funcionarían en una computadora cuántica real antes de tener acceso a hardware cuántico de gran escala o para validar resultados de computadoras cuánticas en pequeña escala.

Los emuladores cuánticos son capaces de simular circuitos cuánticos en un sistema clásico. Pueden emular el comportamiento de cúbits, puertas cuánticas y operaciones cuánticas, y producen resultados de simulación como si estuvieran siendo ejecutados en un ordenador cuántico real. Aunque se simula un sistema cuántico, todo el proceso de simulación se realiza en hardware clásico (como computadoras convencionales). A pesar de que no pueden replicar la superposición cuántica o el entrelazamiento cuántico de forma auténtica, los emuladores cuánticos permiten obtener una aproximación a los resultados

que se esperarían de un ordenador cuántico. Los emuladores cuánticos clásicos enfrentan limitaciones debido al exponencial crecimiento de los recursos necesarios para simular sistemas cuánticos a medida que aumentan los cúbits. Para sistemas cuánticos con muchos cúbits, la cantidad de recursos de memoria y poder de cálculo requerido crece rápidamente, haciendo que la simulación sea inviable más allá de cierto número de cúbits.

Los emuladores cuánticos pueden ser simuladores de estado, circuito o ruido:

- **Simuladores de Estado Cuántico.** Estos emuladores simulan el estado cuántico completo del sistema. Esto significa almacenar el vector de estado cuántico de todos los cúbits involucrados, lo que puede ser extremadamente costoso en términos de memoria para sistemas grandes debido al crecimiento exponencial del tamaño del estado cuántico con el número de cúbits.
- **Simuladores de Circuito Cuántico.** Estos emuladores simulan los circuitos cuánticos, que consisten en operaciones cuánticas aplicadas a cúbits. Aquí se calcula cómo las puertas cuánticas afectan a los cúbits y cómo se transforman los estados durante la ejecución del circuito. Son eficientes para circuitos cuánticos más pequeños y para la simulación de algoritmos cuánticos específicos.
- **Simuladores de Ruido Cuántico.** A medida que las computadoras cuánticas reales no son completamente perfectas, los emuladores cuánticos también pueden modelar sistemas cuánticos con ruido (errores cuánticos), lo que es útil para estudiar cómo los algoritmos cuánticos se comportan en condiciones no ideales.

Ejemplos de Emuladores Cuánticos serían los siguientes:

- Qiskit Aer (de IBM). Qiskit Aer es un conjunto de herramientas de simulación cuántica dentro del ecosistema Qiskit de IBM, diseñado para emular circuitos cuánticos. Ofrece simuladores de alta fidelidad para ejecutar algoritmos

cuánticos y evaluar el rendimiento sin necesidad de acceso a hardware cuántico.

- Cirq (de Google). Cirq es una biblioteca de simulación cuántica desarrollada por Google, que permite diseñar, simular y ejecutar circuitos cuánticos en emuladores antes de ejecutarlos en hardware cuántico real.
- Forest (de Rigetti). Forest es una plataforma de simulación cuántica creada por Rigetti Computing, que incluye simuladores cuánticos para emular circuitos cuánticos y algoritmos cuánticos en entornos clásicos.
- QuTiP. QuTiP es una biblioteca de simulación cuántica escrita en Python, utilizada principalmente para simular sistemas cuánticos abiertos y dinámicas cuánticas, que es útil para estudiar la evolución de sistemas cuánticos complejos, incluida la interacción con el entorno.

Como ventajas de los emuladores cuánticos señalaríamos que permiten probar y desarrollar algoritmos sin la necesidad de hardware cuántico físico, son herramientas de bajo coste y más accesibles para la mayoría de los investigadores y facilitan la exploración de ideas y experimentación en la computación cuántica.

Como desventajas es necesario señalar que la escala de la simulación está limitada por la capacidad de la computadora clásica, ya que el número de cúbits que pueden simular crece exponencialmente. En la práctica una computadora clásica puede simular 40-50 cúbits de manera razonable en términos de memoria y tiempo. A medida que se aumenta el número de cúbits, la memoria necesaria se vuelve prohibitiva debido al crecimiento exponencial del espacio de estados. Para simular 60 cúbits se necesitaría más de 1 petabyte de memoria. Además, los emuladores cuánticos no replican totalmente la mecánica cuántica ya que, aunque pueden emular resultados cuánticos, no pueden reproducir con exactitud todos los efectos cuánticos como la interferencia cuántica de manera fundamental.

Este es uno de los principales motivos por los que la computación cuántica es tan prometedora: para problemas cuánticos complejos, las computadoras cuánticas pueden manejar sistemas con muchos más cúbits, algo que sería inviable para las computadoras clásicas debido a las restricciones exponenciales de la simulación.

DIFERENCIA ENTRE LA SIMULACIÓN Y LA EMULACIÓN CUÁNTICA

La simulación cuántica se refiere a la simulación auténtica de sistemas cuánticos usando computadoras cuánticas, mientras que la emulación cuántica implica tratar de imitar o aproximar el comportamiento cuántico, usualmente en plataformas clásicas. De la misma forma, se puede definir el software cuántico como aquellos programas, algoritmos y sistemas que están diseñados para ser ejecutados en computadoras cuánticas reales o en plataformas cuánticas que aprovechan los principios de la mecánica cuántica como la superposición, el entrelazamiento y la interferencia cuántica mientras que el software de inspiración cuántica se refiere a algoritmos y métodos de optimización y aprendizaje automático que se basan en conceptos de la mecánica cuántica pero que no requieren hardware cuántico para su ejecución. Aunque estos algoritmos no utilizan cúbits ni puertas cuánticas están inspirados en ideas cuánticas como superposición, entrelazamiento y estados cuánticos.

ORDENADOR CUÁNTICO

Un ordenador cuántico es un dispositivo de computación que utiliza los principios de la mecánica cuántica para realizar cálculos. A diferencia de los ordenadores clásicos, que utilizan bits para representar información (0 o 1), los ordenadores cuánticos utilizan cúbits. Un cúbit puede estar en un estado de superposición, es decir, puede ser 0, 1 o una combinación de ambos al mismo tiempo. Los cúbits pueden estar en múltiples estados a la vez, lo que permite a los ordenadores cuánticos realizar muchos cálculos simultáneamente. Esto les otorga

una potencia de cálculo exponencialmente mayor que los ordenadores clásicos para ciertas tareas. Los cúbits pueden estar entrelazados, lo que significa que el estado de un cúbit está instantáneamente correlacionado con el estado de otro, sin importar la distancia que los separe. Esta propiedad permite realizar cálculos a gran escala de manera más eficiente.

Entre los tipos de ordenadores cuánticos cabría distinguir:

- **Ordenadores cuánticos digitales.** Se basan en la implementación de puertas lógicas cuánticas, lo que permite realizar una amplia gama de cálculos. Estos ordenadores son los más cercanos a la computación clásica digital, aunque operan con cúbits en lugar de bits. Un ordenador cuántico digital podría considerarse una implementación especializada de una computadora cuántica universal, si tiene la capacidad de realizar cualquier tipo de algoritmo cuántico. Sin embargo, no todos los ordenadores cuánticos digitales alcanzan este nivel de universalidad, ya que muchos están diseñados con un enfoque específico, como la simulación de materiales o procesos químicos. Los ordenadores cuánticos universales, en principio, podrían resolver problemas mucho más generales, basándose en el concepto de compiladores cuánticos universales, que permiten ejecutar una gama de algoritmos cuánticos sin limitación en los tipos de cálculos que pueden realizar. En resumen, la diferencia principal radica en la versatilidad y capacidad de resolución de problemas complejos en una variedad más amplia de contextos computacionales. Un ordenador cuántico digital no necesariamente es universal, aunque puede formar parte de una implementación más general de computación cuántica.
- **Ordenadores cuánticos analógicos.** Son un tipo de computación cuántica que, a diferencia de los ordenadores cuánticos digitales, no se basan en la manipulación de cúbits discretos (como los 0 y 1 en los sistemas digitales), sino que emplean sistemas cuánticos continuos para modelar y resolver problemas

específicos. En lugar de realizar cálculos basados en un algoritmo cuántico digital, los ordenadores cuánticos analógicos explotan las propiedades cuánticas de ciertos sistemas físicos para simular directamente los problemas, a menudo utilizando fenómenos como la interferencia cuántica y la superposición. Estos ordenadores están diseñados para simular sistemas cuánticos específicos y no tienen un conjunto universal de puertas lógicas.

En resumen, la computación cuántica analógica representa una alternativa valiosa para problemas de simulación cuántica específica, aunque no tiene la misma capacidad general de un ordenador cuántico digital. Sin embargo, puede ofrecer soluciones más eficientes para aplicaciones donde las aproximaciones y simulaciones rápidas son adecuadas.

Un ejemplo de ordenador cuántico analógico es el *quantum annealer*, que está especializado en resolver problemas de optimización combinatoria. Mientras que muchas empresas se centran en construir ordenadores cuánticos de propósito general, D-Wave con la construcción de *quantum annealers* tomó un enfoque más especializado. Sus máquinas están diseñadas para resolver problemas de optimización, como la planificación de rutas y la asignación de recursos. De hecho, el modelo de computación de D-Wave ha sido objeto de debate en la comunidad científica. Algunos argumentan que sus máquinas no son "verdaderamente cuánticas", mientras que otros creen que representan un avance significativo en la computación cuántica. En cualquier caso, los *quantum annealers* son herramientas poderosas para resolver problemas de optimización, y los algoritmos que se ejecutan en ellos están en constante desarrollo. A medida que la tecnología avanza, se pueden esperar ver aplicaciones aún más innovadoras de los *quantum annealers* en un futuro cercano.

Los *quantum annealers* son especialmente útiles para resolver problemas de optimización combinatoria que son difíciles o imposibles de resolver de manera eficiente con computadoras clásicas. Algunos ejemplos de estos problemas incluyen:

- Logística y planificación: optimización de rutas de entrega, asignación de recursos, etc.
- Finanzas: optimización de carteras de inversión, gestión de riesgos, etc.
- Ciencia de materiales: diseño de nuevos materiales con propiedades específicas.
- Inteligencia artificial: aprendizaje automático, reconocimiento de patrones, etc.

Las principales ventajas de los *quantum annealers* sobre las computadoras clásicas para resolver problemas de optimización combinatoria incluyen:

- Mayor velocidad: los *quantum annealers* pueden encontrar soluciones óptimas o cercanas a la óptima en un tiempo significativamente menor que las computadoras clásicas para problemas complejos.
- Mejor escalabilidad: los *quantum annealers* tienen el potencial de escalarse a problemas más grandes y complejos que los que pueden ser abordados por las computadoras clásicas.
- Capacidad para encontrar soluciones no obvias: los *quantum annealers* pueden explorar el espacio de soluciones de manera más eficiente que las computadoras clásicas, lo que les permite encontrar soluciones innovadoras o inesperadas.

A pesar de sus ventajas, los *quantum annealers* también tienen algunas limitaciones:

- Tecnología aún en desarrollo: la tecnología de los *quantum annealers* todavía está en sus primeras etapas de desarrollo y existen desafíos técnicos que deben superarse para mejorar su rendimiento y confiabilidad.
- Costes elevados: los *quantum annealers* son actualmente dispositivos costosos y su acceso está limitado a un número reducido de instituciones de investigación y empresas.

- No son una solución universal: los *quantum annealers* no son adecuados para todos los tipos de problemas de optimización combinatoria. Algunos problemas pueden ser más difíciles de resolver con un *quantum annealer* que con métodos clásicos.

En la actualidad, existen varias empresas que están desarrollando y comercializando *quantum annealers*, como D-Wave Systems, Rigetti Computing y Google. Se han realizado avances significativos en los últimos años, pero la tecnología aún está en desarrollo y se espera que continúe mejorando en términos de rendimiento, confiabilidad y accesibilidad.

La naturaleza de los *quantum annealers* en términos de analógico o digital es un tema complejo y con matices.

En algunos aspectos, los *quantum annealers* pueden considerarse analógicos. Los cúbits, la unidad básica de información en un ordenador cuántico, pueden existir en estados de superposición, representando valores intermedios entre 0 y 1. Además, la evolución del sistema cuántico durante el proceso de *annealing* se asemeja a un flujo continuo. Sin embargo, los *quantum annealers* también exhiben características digitales. La información se codifica en los estados de los cúbits, que son discretos (0 o 1). Además, los algoritmos de optimización utilizados en los *quantum annealers* son de naturaleza digital.

Clasificar los *quantum annealers* como puramente analógicos o digitales es una simplificación excesiva. Su naturaleza combina elementos de ambos paradigmas. La superposición cuántica y la evolución continua del sistema les otorgan un carácter analógico, mientras que la codificación de información y el uso de algoritmos digitales los acercan al mundo digital. Para ilustrarlo mejor, podemos compararlos con el cerebro humano. El cerebro procesa información de forma analógica, utilizando señales neuronales que varían en intensidad. Sin embargo, el resultado final del procesamiento, como la toma de decisiones o la generación de pensamientos, es de naturaleza discreta.

En resumen, los *quantum annealers* son sistemas híbridos que combinan características analógicas y digitales. Esta combinación única les permite resolver problemas de optimización combinatoria de manera eficiente, aprovechando las ventajas de ambos paradigmas.

A diferencia de los computadores cuánticos universales, que operan mediante la aplicación de puertas lógicas cuánticas a cúbits individuales, los *quantum annealers* utilizan un enfoque diferente para resolver problemas de optimización combinatoria. En lugar de realizar cálculos paso a paso como los computadores cuánticos universales, los *quantum annealers* se basan en la analogía del *annealing físico*. En este proceso, un material se calienta y luego se enfría lentamente para que alcance un estado de mínima energía. De manera similar, los *quantum annealers* utilizan un sistema cuántico, como un conjunto de cúbits superconductores, para representar el problema de optimización. A medida que el sistema cuántico evoluciona, se “enfría” gradualmente, buscando la configuración que minimice la “energía” del sistema, que en este caso representa la solución óptima del problema. Este enfoque se inspira en principios de la física como la mecánica estadística y la termodinámica. No se basan en la aplicación precisa de puertas lógicas cuánticas, sino que aprovechan los fenómenos cuánticos como la superposición y el entrelazamiento para explorar múltiples soluciones potenciales de forma simultánea.

Las ventajas de este enfoque *quantum annealers* son la eficiencia para problemas de optimización donde se busca la mejor solución entre un conjunto de opciones, teniendo en cuenta diversas restricciones y el potencial de escalar a problemas más grandes y complejos que los que pueden ser abordados por computadores cuánticos universales basados en puertas.

ORDENADOR CUÁNTICO ADIABÁTICO

Un ordenador cuántico adiabático es un tipo específico de computadora cuántica

que aprovecha un principio fundamental de la mecánica cuántica: la evolución adiabática. En lugar de realizar cálculos a través de una secuencia de puertas lógicas (como en los ordenadores cuánticos de puerta), estos dispositivos resuelven problemas encontrando el estado de menor energía de un sistema cuántico específico.

Los ordenadores cuánticos adiabáticos son especialmente prometedores para resolver problemas de optimización combinatoria, como el problema del viajante de comercio o la búsqueda de la configuración de menor energía de un material. Estos problemas son extremadamente difíciles de resolver para los ordenadores clásicos, incluso para los más potentes.

Las ventajas de los ordenadores cuánticos adiabáticos son la especialización en optimización –son muy eficientes para resolver ciertos tipos de problemas– y su relativamente simple hardware –su arquitectura puede ser más sencilla que la de los ordenadores cuánticos de puerta–. Entre sus desventajas, su propósito específico –no son máquinas de propósito general como los ordenadores clásicos–, dificultades técnicas –controlar la evolución adiabática de un sistema cuántico es un desafío experimental–, y escalabilidad limitada –aumentar el número de cúbits y la complejidad de los problemas que pueden resolver es un desafío importante–.

Estos ordenadores cuánticos adiabáticos los desarrolla la empresa canadiense D-Wave Systems, sin embargo, muchos otros grupos de investigación en todo el mundo también están trabajando en este campo.

Los ordenadores cuánticos adiabáticos representan una vía prometedora para aprovechar la potencia de la computación cuántica para resolver problemas específicos. Aunque aún se encuentran en una etapa temprana de desarrollo, tienen el potencial de revolucionar campos como la inteligencia artificial, la química computacional y la ciencia de materiales. En esencia, un ordenador cuántico adiabático y un *quantum annealer* son lo mismo. Ambos términos se refieren a un tipo específico de ordenador cuántico diseñado para resolver problemas de optimización combinatoria,

aprovechando el principio de la evolución adiabática en sistemas cuánticos.

Resumiendo, el término “ordenador cuántico adiabático” describe el proceso general de cómo funciona la máquina: evolucionando un sistema cuántico adiabáticamente desde un estado inicial simple a un estado final que codifica la solución al problema. Por su parte, el término *Quantum annealer* se refiere a la implementación física y al algoritmo específico utilizado en estos ordenadores. El “*annealing*” (recocido) es un término tomado de la metalurgia y se refiere al proceso de enfriamiento lento de un material para reducir defectos y aumentar su orden. En el contexto de la computación cuántica, se refiere a la evolución adiabática del sistema cuántico. Se utilizan dos nombres, porque adiabático enfatiza el proceso físico subyacente, mientras que *quantum annealer* hace hincapié en la aplicación práctica y el algoritmo utilizado. Como ejemplo está el problema de encontrar la ruta más corta entre varias ciudades. Un ordenador cuántico adiabático podría representar cada posible ruta como un estado cuántico. Al evolucionar el sistema adiabáticamente, el ordenador “descenderá” hacia el estado de menor energía, que corresponderá a la ruta más corta.

La promesa de la computación cuántica ha generado un gran interés y expectativas. Dentro de este campo fascinante, la computación cuántica adiabática emerge como una de las metodologías más prometedoras y revolucionarias. La computación cuántica adiabática es un enfoque alternativo a la computación cuántica basada en puertas lógicas, que utiliza la teoría cuántica adiabática para resolver problemas computacionales. En lugar de manipular cúbits individuales a través de operaciones lógicas, la computación cuántica adiabática utiliza un proceso gradual y controlado para transformar un sistema cuántico desde un estado inicial a un estado final que representa la solución del problema.

El principio fundamental detrás de la computación cuántica adiabática es el teorema adiabático, que establece que un sistema cuántico permanecerá en su estado base si se cambian lentamente las condiciones externas. En el contexto de la computación

cuántica adiabática, este teorema se utiliza para diseñar algoritmos que encuentran el estado base de un sistema cuántico que codifica la solución a un problema computacional.

En un algoritmo de computación cuántica adiabática, el sistema cuántico se inicializa en un estado cuántico simple y se evoluciona lentamente bajo la influencia de un hamiltoniano que codifica el problema a resolver. A medida que el sistema evoluciona, su estado se transforma gradualmente hasta que alcanza un estado final que representa la solución del problema. La clave para el éxito de este enfoque radica en diseñar cuidadosamente el hamiltoniano para garantizar una evolución adiabática y minimizar los errores.

La computación cuántica adiabática muestra un gran potencial para abordar una amplia gama de problemas computacionales difíciles, incluida la optimización combinatoria, el diseño de fármacos, el aprendizaje automático y la criptografía. Su capacidad para encontrar soluciones aproximadas a problemas NP-completos en tiempo polinómico la hace especialmente atractiva para aplicaciones del mundo real donde la eficiencia computacional es esencial.

A pesar de su promesa, la computación cuántica adiabática todavía enfrenta varios problemas, incluida la necesidad de desarrollar hardware cuántico más robusto y escalable, así como algoritmos más eficientes y precisos. Sin embargo, con el rápido avance de la tecnología cuántica y la investigación en curso, el futuro de la computación cuántica adiabática parece brillante, con el potencial de revolucionar la informática y resolver algunos de los problemas más desafiantes de nuestra era digital.

Aunque en esencia los ordenadores cuánticos adiabáticos y los *quantum annealers* son lo mismo, sin embargo, representan dos enfoques diferentes dentro del paradigma de la computación cuántica, que tienen muchas similitudes, ya que ambos aprovechan principios de la mecánica cuántica para resolver problemas de optimización. Las principales diferencias y similitudes entre ellos son:

- Definiciones y funcionamiento básico. La Computación Cuántica Adiabática es un enfoque de computación cuántica que se basa en el teorema adiabático. Según este principio, si un sistema cuántico se inicia en el estado fundamental (de mínima energía) de un Hamiltoniano inicial simple y luego se cambia gradualmente a un Hamiltoniano final complejo, el sistema permanecerá en su estado fundamental si el cambio es lo suficientemente lento. Este cambio lento permite que el sistema "evolucione" hacia la solución de un problema, porque el estado final del sistema cuántico representará la respuesta (o una buena aproximación) al problema de optimización planteado.

El *Quantum Annealing* es una técnica inspirada en el recocido simulado (*simulated annealing*) de la computación clásica, que aplica conceptos cuánticos para mejorar la eficiencia. En lugar de ir probando posibles soluciones al azar, el *quantum annealer* utiliza la superposición y el tunelamiento cuántico para explorar muchas posibles soluciones simultáneamente. El sistema comienza en un estado que representa una solución inicial y, mediante un proceso de "enfriamiento" controlado, va convergiendo hacia un estado de baja energía que representa una solución aproximada al problema de optimización.

- Uso del Teorema Adiabático vs. Tunelamiento Cuántico. En un ordenador adiabático, la evolución del sistema se basa directamente en el teorema adiabático. Si el sistema cambia de manera suficientemente lenta, puede garantizarse que el sistema encontrará la solución óptima (o un buen mínimo global) al final de la evolución. En general, el cambio de un Hamiltoniano a otro debe ser extremadamente lento, lo que a veces puede ser un inconveniente en la práctica debido a las restricciones de tiempo.

Los *quantum annealers* también aplican el teorema adiabático en alguna medida, pero su funcionamiento se centra más en el tunelamiento cuántico. Este tunelamiento permite que el

sistema atraviese barreras de energía para encontrar mínimos de energía que representan soluciones de buena calidad, lo que puede ser más rápido que un proceso puramente adiabático. Debido a esto, los *quantum annealers* no siempre alcanzan el mínimo global (la mejor solución posible), pero sí son capaces de obtener buenas soluciones en tiempos relativamente cortos.

Los Ordenadores Cuánticos Adiabáticos están diseñados para una amplia gama de problemas de optimización, pero debido a la complejidad de mantener el cambio adiabático, suelen estar limitados a problemas específicos donde se puede diseñar un Hamiltoniano que permita representar eficientemente el problema. Estos ordenadores pueden ofrecer ventajas en problemas teóricos o académicos donde el proceso adiabático es esencial.

La computación adiabática cuántica puede implementar la computación cuántica por circuitos cuánticos en un tiempo y memoria polinomial con el número de variables. El problema inverso también es cierto, se puede simular la computación adiabática con un circuito cuántico. Esto se puede demostrar a partir de Hamiltonianos locales, que, mediante una asignación a cadenas de Márkov, se puede encontrar la dependencia polinomial mencionada.¹

Las condiciones requeridas por la computación adiabática, por ejemplo, temperatura cero, son complicadas de obtener físicamente, por lo que han surgido algoritmos inspirados en este tipo de computación que relajan estas condiciones a cambio de perder la universalidad de la computación adiabática. *El annealing cuántico* es uno de estos procedimientos, y permite encontrar mínimos de Hamiltoniano aprovechando el efecto túnel. Aunque lo ideal es que el sistema evolucione entorno al mínimo de energía, en algunos casos la probabilidad de que permanezca en el mínimo es pequeña (aun así, el algoritmo devolverá estados de baja energía que pueden ser útiles).

¹ Computación adiabática cuántica - Wikipedia, la enciclopedia libre

COMPUTADOR CUÁNTICO UNIVERSAL

Un ordenador cuántico universal es un tipo de computadora cuántica que puede simular cualquier otra computadora cuántica. En otras palabras, es una computadora cuántica lo suficientemente poderosa como para ejecutar cualquier algoritmo cuántico posible. La idea de un computador cuántico universal fue introducida por primera vez por David Deutsch en 1985. Deutsch demostró que cualquier computador cuántico que pudiera realizar un conjunto finito de puertas lógicas cuánticas básicas también podría simular cualquier otra computadora cuántica.

Los computadores cuánticos universales son todavía un objetivo lejano, pero tienen el potencial de revolucionar muchos campos, incluyendo la ciencia de materiales, la química, la criptografía y la inteligencia artificial.

Las características de un computador cuántico universal serían las de universalidad –puede simular cualquier otra computadora cuántica–, escalabilidad –puede ampliarse para realizar cálculos más complejos– y coherencia –debe mantener la coherencia cuántica durante el cálculo–.

Para lograr un computador cuántico universal habría que resolver los siguientes desafíos científicos y técnicos:

- Corrección de errores cuánticos: los cúbits son extremadamente sensibles a su entorno, lo que puede causar errores en los cálculos. Desarrollar métodos eficientes para detectar y corregir estos errores es crucial.
- Escalabilidad: actualmente, los ordenadores cuánticos funcionan con un número limitado de cúbits. Para resolver problemas complejos, necesitamos sistemas que puedan manejar miles o incluso millones de cúbits.
- Coherencia cuántica: mantener la coherencia de los cúbits durante el tiempo suficiente para realizar cálculos útiles es un gran desafío. Los cúbits tienden

- a perder su estado cuántico debido a la interacción con el entorno.
- Interconexión de cúbits: es necesario desarrollar tecnologías que permitan la comunicación eficiente entre cúbits en diferentes partes del sistema, lo que podría implicar el uso de enlaces cuánticos de fibra óptica o microondas.
- Materiales y fabricación: encontrar materiales adecuados y métodos de fabricación que permitan la creación de cúbits estables y reproducibles es esencial.
- Algoritmos cuánticos: aunque se han desarrollado algunos algoritmos cuánticos, necesitamos más algoritmos que puedan aprovechar plenamente las capacidades de los ordenadores cuánticos para resolver problemas prácticos.

Los computadores cuánticos universales se diferencian de los computadores clásicos en varios aspectos importantes. Así, los computadores cuánticos utilizan cúbits, mientras que los computadores clásicos utilizan bits. Los cúbits pueden estar en un estado de superposición, lo que significa que pueden ser 0 y 1 al mismo tiempo, y lo que permite a los computadores cuánticos realizar cálculos que son imposibles para los computadores clásicos. Asimismo, los computadores cuánticos realizan cálculos utilizando puertas lógicas cuánticas –las puertas lógicas cuánticas son operaciones que se pueden realizar en cúbits–. Por último, los computadores cuánticos son propensos a la decoherencia: proceso en el que los cúbits pierden su estado de superposición y se convierten en bits clásicos, lo que supone un gran desafío para la construcción de computadores cuánticos universales.

Los computadores cuánticos universales tienen el potencial de revolucionar muchos campos, incluyendo:

- Ciencia de materiales: Los computadores cuánticos podrían utilizarse para diseñar nuevos materiales con propiedades superiores.
- Química: Los computadores cuánticos podrían utilizarse para simular reacciones químicas y desarrollar nuevos medicamentos.

- Criptografía: Los computadores cuánticos podrían utilizarse para romper los sistemas de cifrado actuales.
- Inteligencia artificial: Los computadores cuánticos podrían utilizarse para desarrollar nuevos algoritmos de aprendizaje automático.

ALGORITMOS CUÁNTICOS

Hay varios algoritmos cuánticos importantes que han sido desarrollados para aprovechar las capacidades únicas de los computadores cuánticos:

- **Algoritmo de Shor:** diseñado por Peter Shor en 1994, este algoritmo es famoso por su capacidad para factorizar números enteros en tiempo polinómico, lo cual tiene implicaciones significativas para la criptografía, especialmente en la ruptura de los sistemas de cifrado RSA.
- **Algoritmo de Grover:** propuesto por Lov Grover en 1996, este algoritmo permite realizar búsquedas en una base de datos no ordenada cuadráticamente más rápido que los algoritmos clásicos. Es particularmente útil para problemas de búsqueda y optimización.
- **Transformada Cuántica de Fourier:** similar a la transformada de Fourier clásica, pero implementada en un computador cuántico. Es un componente clave en muchos otros algoritmos cuánticos, incluyendo el algoritmo de Shor.
- **Simulación cuántica:** utiliza computadores cuánticos para simular sistemas cuánticos, lo cual es particularmente útil en física y química. Richard Feynman fue uno de los primeros en proponer la idea de usar computadores cuánticos para simular sistemas físicos.
- **Algoritmo de HHL (Harrow, Hassidim y Lloyd):** un algoritmo cuántico para resolver sistemas de ecuaciones lineales. Tiene el potencial de ofrecer una aceleración exponencial para ciertos tipos de problemas lineales.

Estos algoritmos muestran el potencial de la computación cuántica para abordar problemas que son intratables para los computadores clásicos. No hay un número exacto de algoritmos cuánticos ya que la investigación en este campo está en constante evolución, además de los más conocidos que incluyen el algoritmo de Shor, el algoritmo de Grover, la Transformada cuántica de Fourier y el algoritmo HHL hay muchos otros algoritmos cuánticos que se están desarrollando para aplicaciones específicas en áreas como la criptografía, la optimización, la simulación cuántica y la inteligencia artificial. La cantidad de algoritmos sigue creciendo a medida que la tecnología cuántica avanza.

En realidad, los algoritmos son los que implementan los casos de uso de los ordenadores cuánticos, entre los que se encuentran:

- **Optimización de Procesos.** Los ordenadores cuánticos son especialmente efectivos en problemas de optimización, ya que pueden explorar múltiples soluciones simultáneamente y encontrar la óptima en menos tiempo. Esto es útil en logística y Transporte –optimización de rutas y gestión de flotas, como en aerolíneas o empresas de reparto–, gestión de la Cadena de Suministro –optimización del inventario y la distribución de recursos– y Finanzas –optimización de carteras de inversión y estrategias de trading–.
- **Desarrollo de Nuevos Materiales y Medicamentos.** La simulación molecular es un área en la que la computación cuántica puede aportar avances revolucionarios. Esto es crucial en la industria Farmacéutica –simulación de interacciones moleculares para diseñar fármacos más efectivos y con menos efectos secundarios–, materiales avanzados –desarrollo de materiales con propiedades específicas, como superconductores, o baterías de alta capacidad– y Ciencias de la Salud –estudio de proteínas y plegamiento de proteínas para entender enfermedades complejas–.
- **Inteligencia Artificial y Machine Learning.** La computación cuántica puede mejorar algoritmos de aprendizaje automático al acelerar el procesamiento de grandes volúmenes de datos y encontrar patrones complejos, es aspectos propios como el Entrenamiento de Modelos –reducción del tiempo necesario para entrenar modelos de machine learning complejos–, Análisis de Grandes Datos –procesamiento rápido de datos en tiempo real para la toma de decisiones– o el Reconocimiento de Patrones –aplicaciones en procesamiento de lenguaje natural, reconocimiento de imágenes y análisis predictivo–.
- **Ciberseguridad y Criptografía.** La computación cuántica plantea tanto una amenaza como una oportunidad para la criptografía, ya sea en Desencriptación de Claves Actuales –los algoritmos cuánticos, como el algoritmo de Shor, pueden romper en teoría muchos de los sistemas de encriptación actuales (por ejemplo, RSA)– o Criptografía Post-Cuántica –desarrollo de sistemas de encriptación resistentes a ataques cuánticos, algo esencial para la seguridad de datos en el futuro–.
- **Simulación de Sistemas Cuánticos y Fenómenos Naturales.** Los sistemas cuánticos son intrínsecamente complejos de modelar con computadoras clásicas, pero la computación cuántica permite una simulación directa y precisa de estos fenómenos, como en Simulación de Reacciones Químicas –modelado preciso de reacciones químicas complejas en diversas industrias–, Astrofísica y Física Cuántica –estudio de sistemas astrofísicos complejos, agujeros negros y teorías del universo– o Clima y Medio Ambiente –modelado del cambio climático y predicción de fenómenos meteorológicos extremos con mayor precisión–.
- **Búsqueda y Procesamiento de Datos en Grandes Bases de Datos.** La computación cuántica puede acelerar la búsqueda y el procesamiento de datos en bases de datos masivas en áreas como Análisis Financiero –escaneo de grandes volúmenes de transacciones para detectar fraudes y analizar riesgos–, Análisis Biológico y Médico –pro-

cesamiento de datos genéticos para personalizar tratamientos médicos– o Inteligencia y Seguridad Nacional –análisis rápido de grandes volúmenes de datos para la detección de patrones en temas de seguridad–.

- **Energía y Sostenibilidad.** La computación cuántica puede contribuir al desarrollo de soluciones más sostenibles en materia de Optimización de Redes Energéticas –mejora en la gestión de la distribución de energía en redes inteligentes–, Modelado de Reacciones de Fusión Nuclear –estudio de las condiciones óptimas para la fusión nuclear como una fuente de energía limpia– u Optimización del Consumo Energético –mejoras en la eficiencia de procesos industriales para reducir el consumo energético–.
- **Finanzas Cuánticas.** La computación cuántica también se proyecta como un recurso clave en las finanzas, en aplicaciones como Modelos de Valoración Complejos –análisis de derivados y otros productos financieros de manera más rápida y precisa– o Gestión de Riesgos y Predicciones de Mercado –predicción de precios de activos y evaluación del riesgo de inversiones en mercados complejos–.
- **Telecomunicaciones y Redes Cuánticas.** El desarrollo de redes cuánticas y tecnologías de comunicación es otro ámbito en crecimiento que abarca el Internet Cuántico –creación de una red ultra-segura mediante la distribución de claves cuánticas– o la Comunicación Cuántica Segura –transmisión de información altamente segura y resistente a la interceptación–.

TIPOS DE ORDENADORES CUÁNTICOS EN FUNCIÓN DE LAS DIFERENTES PLATAFORMAS DE CÚBITS

Existen diferentes tipos de plataformas de cúbits para la construcción de los chips cuánticos que se integran en los ordenadores cuánticos, cada una de ellas con sus

propias ventajas e inconvenientes. Las más comunes se basan en diferentes tecnologías para implementar los cúbits, la unidad básica de información en un ordenador cuántico. Entre las plataformas más destacadas encontramos:

- **Cúbits superconductores.** Utilizan circuitos superconductores enfriados a temperaturas cercanas al cero absoluto para mantener el estado de los cúbits. Son uno de los tipos más comunes y ofrecen tiempos de coherencia relativamente largos. Ejemplo: IBM presentó su procesador cuántico Osprey con 433 cúbits, uno de los avances más significativos en computación cuántica hasta la fecha. Aunque IBM no ha especificado públicamente el tiempo de coherencia exacto de los cúbits de Osprey, en general, los tiempos de coherencia son fundamentales para la estabilidad y eficiencia de los procesadores cuánticos. En los chips cuánticos anteriores de IBM, como el “Eagle” de 127 cúbits, se reportaron tiempos de coherencia en el rango de unos pocos microsegundos, que aún es breve para mantener estados cuánticos complejos, aunque el avance en tecnología busca mejorar esta medida en cada nuevo procesador. Con cada modelo, IBM trabaja en reducir el ruido y aumentar la estabilidad de los cúbits mediante mejoras en la arquitectura y la infraestructura de refrigeración, necesarias para mantener el estado de superposición cuántica. Estas mejoras son críticas, ya que los cúbits deben permanecer coherentes el mayor tiempo posible para realizar cálculos complejos de forma efectiva y confiable en entornos prácticos.
- **Cúbits de iones atrapados.** Suspenden iones individuales en vacío y utilizan campos eléctricos para controlar sus estados cuánticos. Ofrecen alta precisión y control individual de los cúbits. Ejemplo: La computadora cuántica IonQ, con 32 cúbits. Para los sistemas de IonQ de 32 cúbits, los tiempos de coherencia suelen ser del orden de varios segundos o incluso más, a diferencia de los sistemas superconductores donde los tiempos de coherencia suelen ser del orden

de microsegundos. En investigaciones previas, se ha reportado que algunos sistemas de iones atrapados pueden tener tiempos de coherencia superiores a los 10 minutos, aunque el valor específico puede variar según las condiciones de operación y las técnicas de aislamiento implementadas.

- **Cúbits semiconductores.** Se basan en la manipulación de electrones en semiconductores, como el silicio. Prometen una mayor escalabilidad y potencial para la integración con la electrónica actual. Todavía se encuentran en una etapa temprana de desarrollo. Un ejemplo destacado de ordenador cuántico basado en cúbits semiconductores es el sistema desarrollado por Intel llamado “Horse Ridge”, el cual utiliza cúbits de espín en semiconductores de silicio. Además de Intel, otras empresas y centros de investigación están explorando cúbits semiconductores en silicio. Google, IBM y el Centro de Computación Cuántica de la Universidad de Nueva Gales del Sur (UNSW) en Australia han trabajado en modelos experimentales que utilizan cúbits de espín en semiconductores, con el objetivo de avanzar hacia computadoras cuánticas más prácticas y escalables.
- **Cúbits fotónicos.** Utilizan fotones (partículas de luz) para codificar información cuántica. Permiten una comunicación rápida y eficiente entre cúbits distantes. Se enfrentan a desafíos en cuanto a la creación y control de fuentes de fotones individuales. Un ejemplo destacado de ordenador cuántico basado en cúbits fotónicos es el sistema desarrollado por la empresa PsiQuantum. Otro ejemplo es la empresa canadiense Xanadu, que también está desarrollando computadoras cuánticas fotónicas utilizando una plataforma fotónica integrada. Su sistema, Borealis, es un procesador cuántico que utiliza fotones en un chip fotónico para realizar cálculos cuánticos. Borealis es capaz de realizar tareas como la simulación de sistemas cuánticos que son inalcanzables para las computadoras clásicas. De hecho,

es capaz de resolver en 36 microsegundos un problema que al ordenador más avanzado le llevaría más de 9.000 años.

- **Cúbits basados en Centros de Nitrógeno Vacante (CNV).** Aprovechan defectos en diamantes para almacenar y manipular cúbits. Combinan alta precisión con tiempos de coherencia relativamente largos. Se encuentran en una etapa intermedia de desarrollo. Una de las aplicaciones más prominentes de los centros de nitrógeno-vacante en la computación cuántica es el trabajo de varias empresas y centros de investigación, incluidos Quantum Diamond Technologies, que desarrollan sistemas cuánticos basados en estos defectos.
- **Cúbits topológicos.** Explotan propiedades topológicas de materiales para proteger los cúbits de la decoherencia. Son teóricamente muy robustos, pero su implementación práctica es compleja. Todavía se encuentran en una etapa temprana de investigación. Una de las investigaciones más prometedoras en este campo es el uso de grafeno para crear cúbits topológicos. El grafeno, una capa de átomos de carbono, puede ser manipulado para exhibir tanto superconductividad como magnetismo, dos propiedades esenciales para la formación de cúbits topológicos.²

Además de los mencionados anteriormente, existen otras tecnologías en desarrollo, como los cúbits basados en moléculas, los cúbits cuánticos de efecto Hall y los cúbits cuánticos de superconductividad topológica.

La elección del tipo de ordenador cuántico más adecuado para una aplicación específica depende de varios factores, como la precisión requerida, la velocidad de procesamiento, la escalabilidad y el coste. Es importante destacar que la tecnología de computación cuántica todavía está en sus primeras etapas de desarrollo. Se están realizando importantes avances, pero aún queda mucho camino por recorrer antes de que los ordenadores cuánticos sean ampliamente utilizados.

2 <https://www.uam.es/uam/noticias/cubits-topologicos-grafeno>

CONCLUSIONES

200 segundos frente a 10.000 años. Ordenador cuántico frente a ordenador clásico. En 2019, Google logró un hito en la historia de la computación pulverizando los registros de velocidad obtenidos hasta esa fecha. Por primera vez, una máquina cuántica era capaz de resolver en un cortísimo espacio de tiempo una tarea imposible de realizar para la mejor tecnología digital disponible. El procesador cuántico del gigante tecnológico, llamado Sycamore, tardó poco más de tres minutos en marcar territorio.

La llamada supremacía cuántica rompía con los paradigmas de la informática clásica tradicional. “Aquella fue una primera demostración. Se sigue teniendo, hoy en día, procesadores cuánticos experimentales que pueden hacer cosas muy interesantes a nivel científico, pero en la actualidad la computación cuántica sigue siendo un área de experimentación. Para llegar a un impacto comercial o más práctico, hace falta conseguir la corrección de errores”, asegura Sergio Boixo, miembro de Google Quantum IA.

Pasar de proyectos experimentales a la construcción de un procesador cuántico propiamente dicho libre de errores es una tarea que llevará años. “La ventaja es que pueden hacer cosas que son imposibles para los ordenadores normales”, explica el físico Adán Cabello.³

Supremacía cuántica, sí. Pero con poca utilidad real, por el momento, y reducida a tareas muy concretas. “Los ordenadores cuánticos no están lo suficientemente desarrollados como para poder sacarles todo el provecho. De hecho, solo se ha podido demostrar la ventaja en problemas académicos y utilizando unos prototipos muy básicos”, puntualiza el experto en tecnologías cuánticas Juan Ignacio Cirac.⁴ Actualmente el término que se utiliza es el de ventaja cuántica en vez el de supremacía cuántica.

El camino hacia un ordenador cuántico universal requiere entre otras cosas, de ingentes inversiones en investigación y desarrollo, empresas como Google, IBM, AWS, AQT o IonQ siguen profundizando en estas investigaciones, pero lo cierto es que las grandes promesas y expectativas generadas por este tipo de computación aún están lejos de cumplirse.

De hecho, algunos expertos como Giuseppe Carleo, profesor de física computacional en la Escuela Politécnica Federal de Suiza (EPFL), han expresado dudas sobre si la computación cuántica llegará a ser tan revolucionaria como se espera.⁵ Carleo argumenta que los avances en inteligencia artificial y simulaciones cuánticas podrían resolver muchos de los problemas que se espera que la computación cuántica aborde. Además, hay quienes señalan que los desafíos técnicos y la necesidad de un número exponencialmente mayor de cúbits para superar las supercomputadoras clásicas hacen que la transformación completa del mundo por la computación cuántica sea menos probable en el corto plazo.⁶

Uno de los críticos más conocidos sobre la computación cuántica es Gil Kalai, matemático israelí y profesor en la Universidad de Yale. Kalai argumenta que el incremento del número de estados de los sistemas cuánticos y su complejidad provocará que acaben comportándose como los ordenadores clásicos, por lo que la superioridad de los primeros acabará evaporándose.⁷

William Daniel Phillips, premio Nobel de Física en 1997, opina que la computación cuántica supone un salto tecnológico sin comparación a los que hemos vivido hasta ahora, más grande incluso que el existente entre el ábaco y la informática actual.⁸

Aunque el futuro de la computación cuántica es prometedor resulta muy difícil calibrar el impacto que tendrá la computación cuántica en el futuro y, además, aún no es

3 Computación cuántica, ¿la próxima revolución tecnológica? | Empresas | Cinco Días

4 <https://cincodias.elpais.com/companias/2023-09-18/computacion-cuantica-la-proxima-revolucion-tecnologica.html>

5 Por qué la IA podría devorar a la computación cuántica | MIT Technology Review

6 Una investigación avanza hacia la supremacía cuántica con resultados imposibles en la computación clásica | Tecnología | EL PAÍS

7 Los ordenadores cuánticos, explicados: cómo funcionan, qué problemas pretenden resolver y qué desafíos deben superar para lograrlo

8 <https://elpais.com/tecnologia/2021-04-03/computacion-cuantica-un-salto-tan-grande-como-el-que-hubo-entre-el-abaco-y-la-informatica-actual.html>

posible poner un plazo concreto en el tiempo y si será posible conseguir un ordenador cuántico universal plenamente funcional, capaz de ejecutar cualquier algoritmo cuántico, al igual que lo que sucede en la computación clásica, cuyos ordenadores pueden ejecutar cualquier algoritmo clásico.

Un ordenador cuántico universal tendría el potencial de ejecutar cualquier algoritmo cuántico que sea teóricamente posible dentro de los límites de la física cuántica. Esto se debe a que un ordenador cuántico universal está diseñado para ser turing-completo, lo que significa que, en teoría, puede simular cualquier proceso cuántico computacional que pueda ser descrito en términos de algoritmos cuánticos. Sin em-

bargo, en la práctica, todavía estamos en las primeras etapas del desarrollo de estos sistemas, y existen importantes desafíos técnicos, como la corrección de errores y la escalabilidad, que deben ser superados para que las computadoras cuánticas universales sean funcionales a gran escala.

En efecto, la computación cuántica se encuentra actualmente en el TRL 4-5⁹. Esto significa que ya se han realizado pruebas en laboratorio y se están validando componentes en entornos relevantes. Aunque no está completamente lista para su uso comercial generalizado, la computación cuántica, ha avanzado significativamente en los últimos años.

SOBRE EL AUTOR

Juan Miguel Ibáñez de Aldecoa Quintana es ingeniero industrial (especialidad electrónica) por la Universidad Pontificia Comillas (ICAI-ICADE). Actualmente ejerce su labor profesional como Ingeniero Industrial del Estado. Cuenta también con un Máster en Dirección de Sistemas y Tecnologías de la Información y las Comunicaciones por la Universidad Politécnica de Madrid.

9 Niveles de madurez de la tecnología/*Technology readiness levels-TRLs*