

# Computación cuántica en la nube: un laboratorio en tu portátil

Alba Cervera Lierta y Alejandro Pozas Kerstjens

Los avances tanto a nivel teórico como experimental auguran un gran futuro para la computación cuántica. En un afán de acelerar el progreso, los desarrolladores de ordenadores cuánticos han puesto sus infraestructuras a disposición del público.

© Freepik

La idea de codificar información en sistemas cuánticos y procesar ésta de una manera más eficiente mediante el aprovechamiento de propiedades, como la superposición y el entrelazamiento, se remonta a la década de 1980. El campo de la computación cuántica se mantuvo en un ámbito casi exclusivamente académico hasta la década de 2010, momento en el cual grandes empresas comenzaron a participar activamente en el desarrollo de ordenadores cuánticos. En contraste con otras revoluciones tecnológicas, el desarrollo de la computación cuántica se está caracterizando por una estrecha colaboración entre el mundo académico y el empresarial, en la cual las compañías han dado libre acceso a sus plataformas a los investigadores y promueven el desarrollo abierto de nuevas ideas mediante la enseñanza y la organización de concursos.

## Introducción

Hace aproximadamente ciento veinte años descubrimos una de las teorías físicas más bellas y fundamentales de la naturaleza: la mecánica cuántica. Durante la primera mitad del siglo xx los esfuerzos se centraron en la formalización de la teoría, y a partir de los años cincuenta de ese siglo, comenzaron a surgir las aplicaciones. El desarrollo de dispositivos como el transistor, el láser, el GPS o la resonancia magnética marcaron el inicio de lo que ahora conocemos como la *primera revolución cuántica*. Aprendimos a aplicar los fenómenos cuánticos colectivos para mejorar nuestro día a día. Ahora, setenta años después, la *segunda revolución cuántica* es posible gracias a los numerosos avances en el control de sistemas cuánticos individuales, que permiten explotar fenómenos como la superposición, el entrelazamiento y la interferencia. Esto supone tener a nuestra disposición todos los recursos que nos proporciona la mecánica cuántica para realizar medidas más sensibles, computaciones más sofisticadas o comunicaciones más seguras.

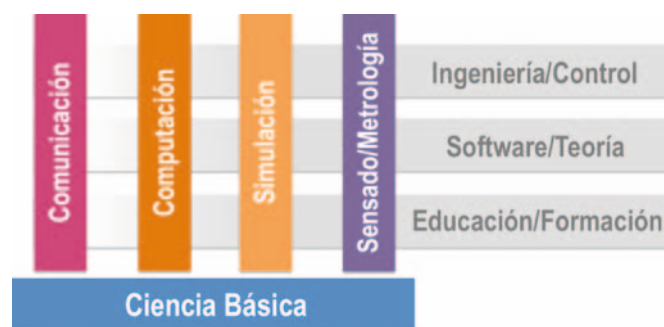
En los últimos años, un gran número de instituciones han puesto en marcha programas para habilitar el desarrollo teórico, experimental e industrial de dispositivos cuánticos. Con el ánimo de impulsar esta revolución, la Unión Europea ha

lanzado el programa *Quantum Flagship* [1]: 1.000 millones de euros para que las tecnologías cuánticas sean una realidad antes de 2028. El *Quantum Flagship* se basa en cuatro pilares fundamentales donde se espera que las tecnologías cuánticas tengan un gran impacto a corto y medio plazo: comunicación, computación, simulación y metrología. En este artículo nos vamos a centrar en una de ellas, la computación cuántica, que permite realizar cálculos que pueden llegar a ser prohibitivamente costosos en ordenadores clásicos.

## La carrera por el ordenador cuántico

La computación cuántica utiliza las propiedades que esta teoría física nos brinda para realizar cálculos de un modo totalmente diferente a la de los ordenadores convencionales. Esto supone un nuevo paradigma en la computación, pues dichas propiedades hacen replantearnos el modo en que diseñamos los algoritmos.

Los ladrillos de esta nueva computación son los *bits cuánticos*, comúnmente llamados *qubits*. Del mismo modo que en computación clásica usamos los transistores para generar los bits, hemos de buscar sistemas cuánticos que funcionen como



**Figura 1.** Esquema del *Quantum Flagship*. El programa prevé destinar 1.000 millones de euros al desarrollo de tecnologías cuánticas que afecten a los campos de la comunicación (incluyendo criptografía), la computación, las simulaciones de sistemas cuánticos y materiales y la metrología. Todo ello va a estar soportado por una inversión en investigación básica en todos los niveles de desarrollo, desde la formación de las nuevas generaciones de científicos a la mejora de sistemas de control experimental.

qubits. Estos deben ser sistemas de dos niveles bien definidos (el del 0 y el del 1) que puedan interactuar entre sí conservando las propiedades cuánticas que les hacen característicos. Y es que una de las principales ventajas de la computación cuántica es la capacidad de los qubits de hallarse en una superposición de estados coherente que permite, entre otras cosas, aplicar una misma operación a todos los elementos de dicha superposición simultáneamente. Si a todo ello le añadimos entrelazamiento entre los qubits y la posibilidad de interferencia, generamos una serie de correlaciones sofisticadas imposibles de reproducir clásicamente.

A pesar del gran reto tecnológico que implica la fabricación de estos dispositivos, los ordenadores cuánticos son ya una realidad. Muchos grupos de investigación de todo el mundo hace años que tienen pequeños prototipos. Pero, sin duda, este campo ha experimentado una gran expansión cuando compañías privadas han decidido apostar por él. En 2010, IBM decidió tomar la delantera y empezar a desarrollar prototipos experimentales. Su anuncio salió tres años después que la compañía canadiense D-Wave asegurara tener un chip cuántico de 16 qubits. Aunque el tipo de computación que realiza D-Wave no es universal, y por tanto sus qubits son muy diferentes a los de IBM y de otras compañías, este anuncio probablemente dio el pistoletazo de salida a la carrera cuántica empresarial. Después de IBM, otras compañías se sumaron a esta carrera: Google, Intel, Microsoft, Alibaba..., además de crearse nuevas empresas salidas directamente de aquellas universidades que llevaban años investigando en este campo. Un ejemplo es Rigetti Computing, nacida en la Universidad de Yale y ahora una de las principales competidoras en el área. A nivel local, otro ejemplo es Qilimanjaro, una empresa recién creada en Barcelona cuyo objetivo es construir el primer ordenador cuántico del sur de Europa.

La gran motivación de la computación cuántica es ejecutar algoritmos o simulaciones imposibles de llevar a cabo por ordenadores clásicos. Ese objetivo recibe el nombre de ventaja cuántica. El límite de la ventaja cuántica varía con la mejora de los superordenadores clásicos y con el desarrollo de nuevos métodos para simular sistemas cuánticos. Aun así, en el mejor de los casos, un ordenador clásico no será capaz de gestionar suficiente memoria como para simular más de 100 qubits. Recientemente, Google ha afirmado haber alcanzado la ventaja cuántica, utilizando un chip de 53 qubits para, en 200 segundos, tomar muestras de una distribución de probabilidad que requeriría del orden de 10.000 años de cómputo en los mayores superordenadores clásicos [2]. Además de Google, IBM acaba de lanzar un chip de 53 qubits, y Rigetti Computing tiene planeado construir uno de 128 qubits. En el transcurso de la redacción de este artículo, nuevas empresas se han sumado a la carrera desarrollando

otras alternativas a los circuitos superconductores, como son las trampas iónicas. La era de la computación cuántica es ya una realidad.

Sin embargo, todos los dispositivos mencionados siguen siendo prototipos debido a que son “ruidosos”. Para realizar un algoritmo cuántico correctamente es necesario que los qubits mantengan la coherencia y que las puertas lógicas cuánticas se implementen de forma perfecta. Esto es experimentalmente muy difícil, por lo que se asume que se van a necesitar códigos de corrección de errores cuánticos. Dichos códigos necesitan del orden de 100 qubits para corregir el estado de uno solo, lo que hace materialmente imposible, actualmente, tener un ordenador cuántico sin fuentes de error. Por todo ello, se ha bautizado a esta primera fase de la computación cuántica como NISQ (*Noisy Intermediate-Scale Quantum computation* [3]), en contraposición a la *Fault-tolerant Quantum computation*, que nos permitirá trabajar con qubits perfectos (llamados “lógicos”). Cabe mencionar otras propuestas de algoritmos cuánticos que, en principio, no necesitan corregir errores. Son los llamados *algoritmos variacionales* o híbridos, por usar tanto computación cuántica como clásica para sortear el problema del ruido.

En esta carrera para alcanzar la ventaja cuántica las empresas privadas se han dado cuenta de que la colaboración de todos va a ser fundamental. Al fin y al cabo, la computación cuántica es un campo relativamente nuevo y los conocimientos necesarios para pensar e implementar algoritmos cuánticos se enseñan casi exclusivamente en las universidades. Por este motivo, algunas compañías ofrecen acceso a sus ordenadores cuánticos de forma gratuita a través de la nube. Cada empresa está desarrollando su propio lenguaje de programación para enviar instrucciones a su chip cuántico, de modo que no sea necesario tener el ordenador enfrente [4, 5]. Cualquier persona puede instalarse estos lenguajes (normalmente en forma de “packages” de algún lenguaje conocido, como Python), programar su conjunto de instrucciones cuánticas en su portátil y ejecutar el programa en la nube. Éste es corrido en el chip cuántico en cuestión y los resultados son enviados al usuario para que los procese y analice como desee. El sueño de muchos científicos teóricos se hace realidad: tener acceso directo al experimento desde el despacho.

En la Figura 2 se muestran los diferentes niveles de programación de un ordenador cuántico junto con una tabla con las diferentes empresas que ofrecen en abierto sus lenguajes cuánticos.

En 2018 la empresa IBM convocó una serie de cuatro premios con el objetivo de fomentar el uso de sus dispositivos cuánticos y explorar sus posibles aplicaciones. El premio “Teach Me QISKit” se otorgó al mejor algoritmo cuántico programado usando su lenguaje que demostrara en forma de tutorial alguna aplicación interesante. El premio

“Best Paper” se otorgó a las mejores publicaciones científicas que hicieran uso de alguno de sus ordenadores cuánticos. El premio “Teach Me Quantum” se otorgó al mejor material para realizar un curso introductorio en computación cuántica y el premio “QISKit Developer Challenge” al mejor compilador cuántico. Los autores del presente artículo fueron galardonados con los dos primeros premios. En las siguientes secciones, presentamos un resumen de nuestros trabajos, que a la vez sirven de ejemplo de uso y aplicaciones de un ordenador cuántico.

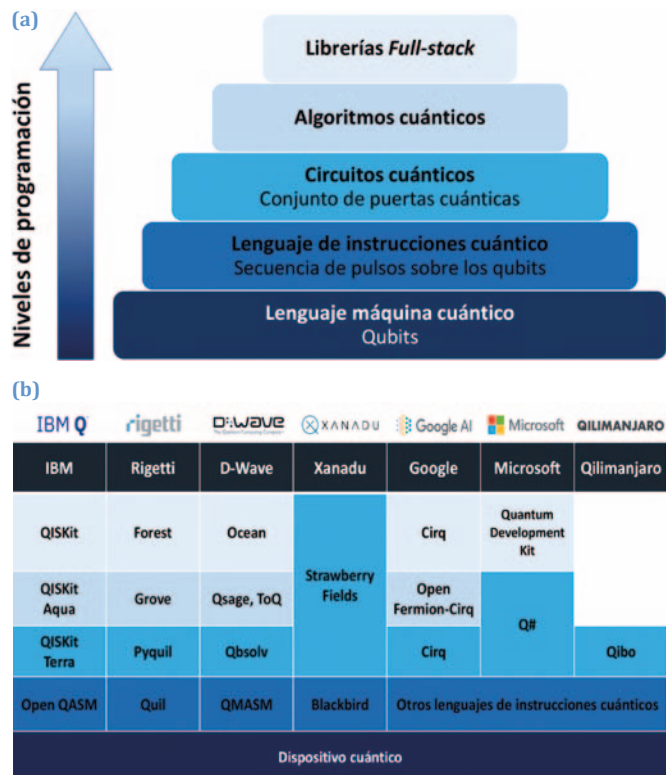
### Transición de fase cuántica en un ordenador cuántico

Una de las primeras personas en proponer la construcción de un ordenador cuántico fue el físico Richard Feynman. En su artículo publicado en 1982 “Simulando la física con ordenadores” [6], puso de manifiesto el coste exponencial de la simulación de sistemas cuánticos. Feynman planteó: ¿por qué no construir un ordenador, las piezas del cual se comporten de forma cuántica también? Eso simplificaría enormemente el coste computacional, pues cada uno de los qubits de este ordenador podría albergar el estado de una partícula, y la interacción entre ellos podría describir una interacción real de un sistema cuántico. La primera aplicación de un ordenador cuántico es, precisamente, la simulación cuántica.

Desde que se propuso hace más de un siglo, el modelo de Ising ha sido usado como modelo simplificado para explicar el magnetismo a nivel microscópico. Además de su versión clásica, existe el modelo de Ising cuántico, el cual presenta una transición de fase bajo un campo externo transversal. Esta transición es cuántica, es decir, el estado fundamental pasa de ser paramagnético a ferromagnético por fluctuaciones cuánticas, a temperatura cero.

Es posible encontrar un circuito cuántico que simule de forma exacta el modelo de Ising unidimensional. Podemos entonces simular con un ordenador cuántico las características más importantes de este modelo, en especial su transición de fase cuántica. El circuito cuántico en cuestión nos da acceso no solo al estado fundamental, sino también a cualquier estado del espectro de Ising. Esto implica la posibilidad de simular la evolución temporal o estados térmicos, elementos de especial interés en el campo de la física de la materia condensada. El modelo de Ising en una dimensión es integrable, es decir, podemos obtener el espectro de energías y estados cuánticos analíticamente. Con ello, podemos comparar los resultados obtenidos con el ordenador cuántico con las expresiones teóricas y así comprobar cómo de bueno es el dispositivo.

Como hemos dicho anteriormente, los ordenadores cuánticos de hoy en día están compuestos de pocos qubits. Sin embargo, esto no supone una barrera para ejecutar pequeños experimentos y ver así cómo se comportan. Podemos entonces

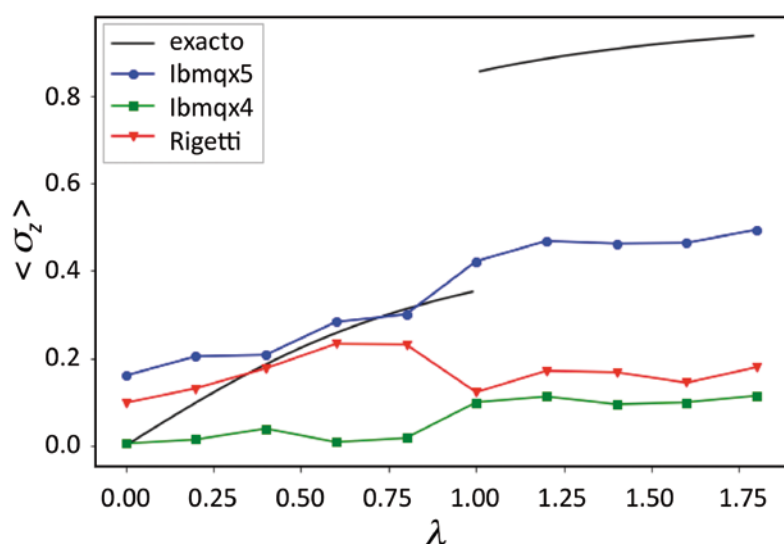


**Figura 2.** (a) Los diferentes niveles de programación de un ordenador cuántico. El más bajo corresponde al estado cuántico de los qubits, en analogía al lenguaje máquina de los bits clásicos. Los qubits son manipulados con un conjunto de pulsos y operaciones físicas que implementan las puertas lógicas cuánticas. Un circuito cuántico es el conjunto de puertas y qubits que forman parte de un algoritmo cuántico. En un nivel más alto de programación, se están desarrollando librerías “full-stack”, que permiten construir tanto circuitos como usar algoritmos ya programados. (b) Una tabla con las diferentes empresas que ofrecen en abierto sus lenguajes cuánticos. Algunas de ellas disponen de prototipos propios de ordenadores, como es el caso de IBM, Rigetti, D-Wave, Xanadu y Google.

construir un pequeño circuito cuántico que simule el modelo de Ising para una cadena de cuatro espines, representando con un qubit el estado de cada uno de ellos. Este circuito se puede enviar a los ordenadores cuánticos, como los que ofrecen en la nube IBM o Rigetti Computing. El resultado de dicho experimento se presenta en la Figura 3, donde se muestra el valor esperado del campo magnético en función del campo transversal  $\lambda$ . A medida que dicho campo aumenta, los espines tienden a alinearse hasta que sucede la transición de fase cuántica y se produce un salto en la magnetización. El lector interesado puede consultar la referencia [7] y encontrar el tutorial para implementar este algoritmo cuántico y otros en [4].

Aunque el resultado pueda parecer descorazonador al alejarse tanto de la predicción exacta, pueden encontrarse varias explicaciones. Primero, los qubits son “ruidosos”, es decir, varios factores pueden provocar que cada uno de ellos no se encuentre en el estado que le tocaría al terminar el algoritmo. La coherencia cuántica de los qubits es fundamental en este tipo de computación. Sólo si éstos se encuentran en un estado coherente, sus propiedades cuánticas pueden ser explota-





**Figura 3.** Resultados de la simulación cuántica exacta del modelo de Ising. El gráfico muestra la magnetización transversal en función de la intensidad del campo magnético externo  $\lambda$ . A medida que dicho campo aumenta, los espines tienden a alinearse con él, provocando una transición de fase cuántica en  $\lambda = 1$ , de una fase paramagnética a una ferromagnética. El resultado experimental se aleja del esperado en algunas zonas debido en gran parte a la facilidad que tienen los qubits de perder su coherencia cuántica.

das para la realización correcta del algoritmo. El tiempo de coherencia es limitado, lo que nos da un cierto margen de tiempo para implementar todas las puertas lógicas necesarias antes de terminar la computación. Si nos pasamos de ese tiempo, todo lo que hagamos no tendrá el efecto deseado, provocando numerosos errores.

En segundo lugar, las puertas lógicas cuánticas son operaciones físicas que hay que programar de un modo muy preciso y que dependen de las características físicas de cada qubit. Hay todo un sistema de control cuántico de estas puertas que debe ser sumamente sofisticado, y las limitaciones experimentales nos impiden estar libres de errores. Éstos se van propagando a medida que aplicamos más y más puertas. Ambos factores se corregirán en un futuro cuando sea posible aplicar códigos de corrección de errores a nuestros ordenadores cuánticos.

El hecho de que podamos observar el comportamiento de un sistema cuántico real, a pesar de todas estas fuentes de error y de la gran dificultad técnica que entraña el control de sistemas cuánticos individuales, es un salto tecnológico muy importante. Experimentos como éste son pruebas de concepto, es decir, pequeñas demostraciones de nuestro poder experimental que sientan las bases de lo que seremos capaces de hacer.

### Computación cuántica para inteligencia artificial

Otro ámbito en el cual se espera que el uso de ordenadores cuánticos presente un gran avance con respecto al uso ordenadores tradicionales es en el aprendizaje automático o *machine learning*. Actualmente, los algoritmos de aprendizaje automático se encargan de manejar y analizar cantidades ingentes de datos para encontrar patrones a través de los cuales nueva información pueda ser clasificada, predicha, o generada. Actualmente, los algoritmos de *machine learning* están detrás de las recomendaciones de Amazon y Netflix, de los

sistemas de control de coches autónomos, o de los aparatos de reconocimiento facial de los aeropuertos. El mundo de la investigación no se ha quedado atrás, y recientemente el aprendizaje autónomo ha sido noticia en áreas tan diversas como el reconocimiento temprano de enfermedades o en el descubrimiento de exoplanetas.

La característica principal de la mayoría de los algoritmos utilizados actualmente (conocidos como algoritmos de *deep learning* o aprendizaje profundo) es la gran cantidad de parámetros utilizados para modelar el conjunto de datos estudiado. Esto hace que sea muy complicado conocer cuál es la característica específica que determina la predicción, siendo estos algoritmos tratados como *cajas negras* que solamente arrojan resultados, sin explicaciones. Además, los métodos de entrenamiento de dichos algoritmos dificultan la obtención de información adicional a la de la predicción en sí. Esto hace que preguntas como “¿cuán seguro se está de que la predicción realizada es la correcta?” o “¿cuál es la diferencia de confianza entre la primera y la segunda opción?” sean muy complicadas de responder. Dado que se espera que en los próximos años estos algoritmos tengan cada vez más y más relevancia en nuestras vidas, es importante desarrollar herramientas que nos permitan “abrir la caja” y obtener información acerca del proceso de predicción [8].

Una de las maneras de obtener más información acerca de los funcionamientos internos de los algoritmos es el cambio de paradigma en el entrenamiento, transitando del cálculo y la optimización de funciones a la teoría de la probabilidad y el teorema de Bayes. En este paradigma, el objeto central no es la predicción en sí, sino la distribución de probabilidad de predicciones condicionada en el conjunto de datos de entrenamiento. Esto permite que preguntas como las planteadas anteriormente sean fáciles de responder.

Sin embargo, las técnicas de entrenamiento bayesiano de algoritmos de aprendizaje automático tienen un alto coste computacional. Es justo aquí donde la computación cuántica resulta una gran aliada. Suponiendo que uno pueda codificar de manera eficiente la información a analizar en sistemas cuánticos, es posible aprovechar la superposición cuántica para reducir drásticamente los costes computacionales.

El problema de resolver sistemas lineales de ecuaciones es un claro ejemplo donde la computación cuántica puede ofrecer una ventaja. Dados una matriz de coeficientes  $A$  y un vector de valores  $b$ , el problema consiste en obtener el vector solución  $x$  que cumple  $Ax = b$ . La resolución de este problema viene dada por  $x = A^{-1}b$ , lo cual necesita del cálculo de la inversa de la matriz  $A$ . Si esta matriz tiene dimensión  $n$ , son necesarias del orden de  $n^3$  operaciones para calcular su inversa. Sin embargo, en caso de poder crear un sistema cuántico en el estado  $|b\rangle$  y un operador cuyos coeficientes ven-

gan determinados por la matriz  $A$ , existe un algoritmo cuántico que permite evolucionar el sistema hacia el estado  $|x\rangle = A^{-1}|b\rangle$  realizando del orden de  $\log(n)$  operaciones [9].

Con esta motivación, en [10] se desarrolló un algoritmo cuántico para llevar a cabo entrenamiento de redes neuronales utilizando una técnica bayesiana denominada “*Procesos Gaussianos*”. Dicha técnica requiere de la inversión de matrices que son de un tamaño comparable a la cantidad de datos que estudiar. En el caso de aplicaciones en aprendizaje profundo, el coste computacional de esta operación es prohibitivo en ordenadores clásicos. Como parte del proyecto, se estudió cuán factible es la inversión de matrices en los ordenadores cuánticos actuales de las compañías IBM y Rigetti Computing.

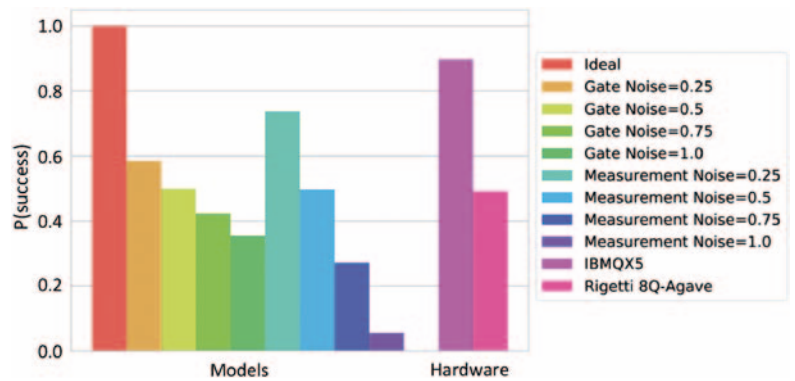
Pronto fueron patentes los dos problemas más acusados de los ordenadores NISQ. Por un lado, la limitada conectividad entre qubits provoca que en muchas ocasiones sea necesario reservar algunos para cálculos intermedios, de modo que no se puedan resolver problemas muy grandes. Por otro lado, el corto tiempo de coherencia de los qubits, comentado anteriormente, aleja el resultado final del esperado. A pesar de esto, se observó que, para el caso de inversión de pequeñas matrices, los ordenadores de IBM consiguen preparar estados razonablemente satisfactorios. El lector interesado que quiera probar los programas ejecutados en dicho estudio desde su casa, experimentar o, incluso, sugerir mejoras puede encontrarlos en [11].

### Ciencia abierta y colaborativa

A pesar de los desafíos experimentales que conlleva la computación cuántica, los ordenadores cuánticos han llegado para quedarse. Estamos viviendo una revolución tecnológica como lo fue en su día el desarrollo de la computación clásica. El ordenador cuántico es una nueva herramienta de cálculo que promete aplicaciones en gran variedad de ámbitos: química, finanzas, machine learning, ciencia de materiales, etc.

Una vez más, la ciencia avanza más rápido gracias a las grandes colaboraciones. La computación cuántica ya no es patrimonio único de los físicos. Arquitectos de sistemas, desarrolladores de software e ingenieros electrónicos, entre muchas otras profesiones, son necesarios para abandonar los prototipos y construir un ordenador cuántico universal. Del mismo modo, son necesarios investigadores de áreas tan diversas como sea posible, para así explorar qué problemas pueden hallar la solución en el uso de la mecánica cuántica.

Desde aquí, nos gustaría hacer un llamamiento a la ciencia abierta, que pone a la libre disposición de los usuarios e investigadores los avances científicos más punteros. Los retos tecnológicos que plantean las tecnologías cuánticas en general, y la computación cuántica en particular, exigen un gran esfuerzo colaborativo que será sobradamente



te compensado con las aplicaciones que nos ofrece esta nueva tecnología.

### Referencias

- [1] Quantum Flagship webpage: <https://qt.eu/>
- [2] F. ARUTE *et al.*, “Quantum supremacy using a programmable superconducting processor”, *Nature* **574**, 505-510 (2019).
- [3] J. PRESKILL, “Quantum Computing in the NISQ era and beyond”, *Quantum* **2**, 79 (2018)
- [4] IBMQ, Quantum Instruction Set, <https://qiskit.org/>.
- [5] Rigetti Computing full-stack library, <https://www.rigetti.com/forest>.
- [6] R. P. FEYNMAN, “Simulating physics with computers”, *Int. J. Theor. Phys.* **21**, 467- 488 (1982).
- [7] A. CERVERA-LIERTA, “Exact Ising model simulation on a quantum computer”, *Quantum* **2**, 114 (2018).
- [8] Guía ética para una IA confiable, <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.
- [9] A. W. HARROW, A. HASSIDIM y S. LLOYD, “Quantum algorithm for solving linear systems of equations”, *Phys. Rev. Lett.* **103**, 150502 (2008). arXiv:0811.3171 [quant-ph]
- [10] Z. ZHAO, A. POZAS-KERSTJENS, P. REBENTROST y P. WITTEK, “Bayesian Deep Learning on a Quantum Computer”, *Quantum Machine Intelligence* **1**, 41-51 (2019).
- [11] Repositorio *bayesian-dl-quantum*, GitLab, <https://www.gitlab.com/apozas/bayesian-dl-quantum>.

**Figura 4.** Comparación entre simulaciones con diferentes tipos de ruido y ejecuciones en ordenadores cuánticos reales de la resolución del problema  $\{3x_1 + x_2 = 2, x_1 + 3x_2 = 0\}$ . En el eje vertical se representa la probabilidad de éxito en un *swap test*, que se relaciona con la distancia entre el resultado obtenido y el deseado,  $|x\rangle = \frac{4}{\sqrt{10}}\left(\frac{3}{4}|0\rangle - \frac{1}{4}|1\rangle\right)$ .

**Alba Cervera Lierta**  
Matter Lab group,  
University of Toronto



**Alejandro Pozas Kerstjens**  
Facultad de Matemáticas,  
Universidad Complutense de Madrid

