REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS, QUÍMICAS Y NATURALES DE ZARAGOZA

LA SEGUNDA REVOLUCIÓN CUÁNTICA

DISCURSO DE INGRESO LEÍDO POR EL ACADÉMICO ELECTO

Ilmo. Sr. D. FERNANDO MARÍA LUIS VITALLA

EN EL ACTO DE SU RECEPCIÓN SOLEMNE
CELEBRADO EL DÍA 25 DE ENERO DEL AÑO 2023

Y

DISCURSO DE CONTESTACIÓN POR EL

Ilmo. Sr. D. JUAN BARTOLOMÉ SANJOAQUÍN

ACADÉMICO NUMERARIO

ZARAGOZA

2023

Depósito legal: Z zzz-2023

Imprime:
Servicio de Publicaciones. Universidad de Zaragoza

LA SEGUNDA REVOLUCIÓN CUÁNTICA

POR EL

Ilmo. Sr. D. FERNANDO MARÍA LUIS VITALLA

Excmo. Sr. Presidente

Ilmos. Sras. y Srs. Académicos

Señoras y Señores

Quiero expresar mi enorme gratitud a la Real Academia de Ciencias de Zaragoza por pensar en mí para formar parte de ella. Es un honor inesperado, y probablemente exagerado. Sólo puedo decir que trataré de estar a la altura y de contribuir a los fines de la institución lo mejor que pueda.

Saber que voy a ocupar la plaza que dejó vacante Víctor Orera añade emoción y un sentimiento de responsabilidad a este paso. Le conocí como estudiante, hace más años de los que querría reconocer, y me impresionó su energía y su contagiosa ilusión por lo que hacía. Con esa ilusión consiguió crear y liderar durante mucho tiempo un excelente grupo de investigación dedicado a desarrollar materiales con interés para almacenamiento de la energía, siguiendo una vocación de hacer ciencia de calidad, pero también capaz de mejorar el bienestar de la sociedad. Compartir centro y departamento con él, aunque en ámbitos alejados de la física, me hizo admirar su trabajo, pero aún más su calidad humana y la sabiduría y mesura con la que ha cumplido responsabilidades institucionales: fue director del ICMA, representante del CSIC en Aragón y vicepresidente de esta institución, por citar sólo algunas. Más adelante, hizo uso de estas dos cualidades, y de un ánimo difícil de imitar, al afrontar adversidades de la vida.

También querría recordar aquí a personas que han sido clave en mi carrera y a las que debo lo bueno que haya podido resultar de ella. Primero, mis maestros. Juan Bartolomé me introdujo de la mano en este mundo, me ayudó a dar mis primeros pasos en un laboratorio y a apreciar el valor de los experimentos, y me hace el honor de recibirme en la academia. Julio Fernández me enseñó a resolver problemas de física teórica y, sobre todo, a crear un pensamiento crítico. Por último, Javier Tejada y Jos de Jongh han sido una constante fuente de inspiración y un ejemplo para mí. Segundo, y no menos importante, mis estudiantes de doctorado. Sé que me han dado mucho más de lo que han podido recibir de mí. Y no me refiero sólo al fruto de muchas horas de trabajo sin las que muchos resultados no habrían visto la luz, sino sobre todo a su estímulo y entusiasmo. Sé también que he sido muy afortunado y, por eso, quiero expresar mi afecto y agradecimiento a todos ellos: Fabian Mettes, Román López, 'Pepa' Martínez-Pérez, Enrique Burzurí, Mark Jenkins, Ana Repollés, Nacho Gimeno, Marcos Rubín, Sergio Martínez y Sebastián Roca. Compartir horas, trabajo y encuentros personales con unos y otros es seguramente lo mejor que me ha dado este oficio.

Para esta ocasión, he elegido hablar de la llamada segunda revolución cuántica, que engloba un renovado interés por estudiar y controlar fenómenos cuánticos en diversos sistemas y por explotar sus potenciales aplicaciones, especialmente en el campo de las tecnologías de la información. Además de su relevancia, que ya ha trascendido el ámbito científico, lo he elegido por dos razones, vinculadas tanto a mi pasado científico como a mi actividad presente. La posibilidad de que efectos cuánticos modifiquen las propiedades de nanomateriales, o incluso den lugar a comportamientos completamente nuevos, ha sido un hilo conductor de mi trabajo desde mi tesis doctoral, dedicada a estudiar el efecto túnel en magnetismo. En esa época, la exploración de estos fenómenos en materiales magnéticos corría en paralelo con estudios análogos realizados sobre circuitos superconductores, los mismos que hoy en día constituyen la base de los procesadores cuánticos más desarrollados. Aunque algo más tarde, las moléculas magnéticas que permitieron descubrir el efecto resonante de espín y crear superposiciones cuánticas a escala mesoscópica se han convertido también en prometedores candidatos para el hardware cuántico, con el potencial de contribuir a resolver algunas de las limitaciones a las que se enfrentan otras aproximaciones. Creo, por estos motivos, que es un área de investigación fascinante, que va a generar resultados notables y sorpresas durante mucho tiempo, y que puede influir enormemente en la sociedad. Un campo en el que el entorno cercano a la Academia, nuestra universidad y el INMA, pueden jugar un papel relevante. Espero que esto justifique mi elección y que sea también de su agrado.

1. Introducción

La primera década del siglo XX trajo consigo cambios trascendentales para la física. Tanto la relatividad como la física cuántica constituyeron profundas revoluciones científicas. Y aunque la primera, con sus implicaciones cosmológicas, probablemente atrae más vocaciones y fascinación social, la segunda ha tenido una mayor influencia sobre nuestro día a día. Gracias a ella hemos comprendido la naturaleza discreta de la radiación electromagnética y la estructura de los átomos que forman la materia y a nosotros mismos, y comprendemos las propiedades térmicas, eléctricas y magnéticas de los sólidos. Quizás el cambio más trascendental se puede resumir en el principio de incertidumbre de Heisenberg [Hei27, WZ83]

$$\Delta x \Delta p \geq \hbar \tag{1.1}$$

que establece la existencia de una mínima indeterminación en la medida de pares de magnitudes conjugadas (en este caso posición x y momento p), dada por el valor de la constante de Planck $\hbar$. La ecuación (1.1) establece, por vez primera en la historia de la ciencia, un límite al conocimiento humano que no proviene de nuestra capacidad técnica, sino que es inherente a la naturaleza. Este principio nos obliga a abandonar la idea de trayectoria y a cambiarla por una función de onda cuya interpretación es probabilista. A pesar de que no forma parte de los postulados, es una piedra angular de la teoría cuántica de la cual se derivan muchos de sus principios.

El comienzo del siglo XXI está siendo testigo de un renacido interés en la investigación de fenómenos cuánticos que se ha venido en denominar la 'segunda revolución cuántica', expresión que he tomado prestada para mi título [Gib14, ABB+18, Deu20]. A menudo se asocia con el desarrollo de aplicaciones basadas en dichos fenómenos, es decir, con la transición hacia una tecnología cuántica [MRN+17]. Siendo en parte cierta, esta definición es incompleta y algo injusta. Conviene recordar que la electrónica de consumo, el láser o los superconductores, que llevan varias décadas influyendo en la sociedad y en diversos mercados, se basan en fenómenos cuánticos.

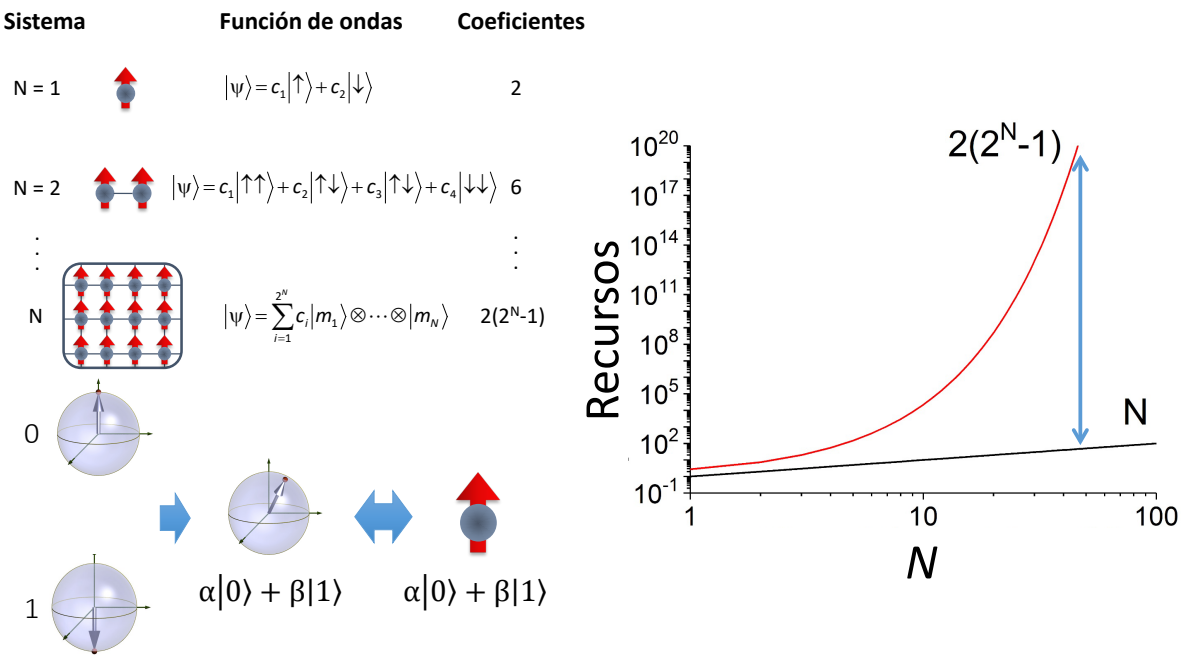

Figura 1: La descripción de la función de ondas de un sistema de N partículas cuánticas involucra un número de coeficientes que crece exponencialmente con N. Es éste un ejemplo de problema computacionalmente 'duro' para un ordenador convencional, basado en unidades de información, los bits, que sólo pueden encontrarse en los estado '0' y '1'. Sin embargo, un ordenador cuántico, basado en qubits cuyos estados pueden ser, al igual que los del sistema problema, superposiciones arbitrarias de $|0\rangle$ y de $|1\rangle$, puede codificar dicha función de onda con sólo N qubits.

Una forma más pragmática de motivar este campo de investigación, y que tiene la ventaja de apoyarse en una figura icónica de la física, hace referencia al avance casi exponencial de las tecnologías de la información. No es un secreto que estos avances han sido posibles, en gran parte, gracias a la miniaturización continua de componentes electrónicos. En su famoso artículo 'There is plenty of room at the bottom' [Fey92] Richard Feynman vaticinaba que es posible crear y aprovechar estructuras de dimensiones diminutas. Sin duda, el tiempo le ha dado la razón. Quizás menos repetida, pero muy relevante en este contexto, es otra frase del mismo artículo en la que se argumenta que usar nuevas leyes, como las que gobiernan objetos microscópicos, nos puede ayudar a hacer cosas nuevas [1]. El mismo Feynman dio una idea de qué cosas podemos hacer, y de sus potenciales ventajas, con un ejemplo sencillo: la simulación de sistemas cuánticos con un ordenador [Fey82]. Basta recordar que la descripción de un sistema formado por N partículas cuánticas, por ejemplo una red de N espines $s = 1/2$, se vuelve computacionalmente muy costosa para valores relativamente modestos de N. De hecho, el número de unidades de información, o bits, necesarios para representar la función de ondas aumenta exponencialmente con el número de componentes. La razón de este aumento es que la computación convencional, que llamaré a partir de ahora 'clásica', utiliza solamente dos estados lógicos '0' y '1' mientras que la función de ondas que se pretende describir incluye fases y pesos relativos. Es fácil apreciar entonces la ventaja de contar con bits cuánticos, o qubits, que hagan posible manipular estados superposición $\alpha|0\rangle + \beta|1\rangle$ y que, por tanto, puedan codificar de manera natural los estados cuánticos del sistema que queremos estudiar.

Las nuevas tecnologías cuánticas tratan de convertir una amenaza, la limitación que imponen las fluctuaciones cuánticas a la miniaturización de dispositivos convencionales, en una oportunidad. El objetivo de este nuevo paradigma es aprovechar ventajosamente el control de la función de ondas de qubits y, en particular, de los fenómenos de superposición y entrelazamiento. Son, por tanto, más el resultado del principio de incertidumbre (1.1) que de la mera cuantización de la energía. Lo que sigue trata de dar una visión, necesariamente incompleta, de este campo emergente, de su enorme potencial práctico, que no sólo promete cambiar la manera en la que procesamos, protegemos y comunicamos la información sino también crear nuevas posibilidades para el diseño de moléculas funcionales, fármacos y materiales, así como herramientas experimentales con sensibilidad

[1] En el original: *So as we go down and fiddle around with the atoms down there, we are working with different laws and we can expect to do different things.*

récord, y de sus retos y posible evolución futura. Al juicio del lector dejo la cuestión de si merece el calificativo de revolución. Como ya he mencionado antes, sólo espero que, al menos, le resulte interesante.

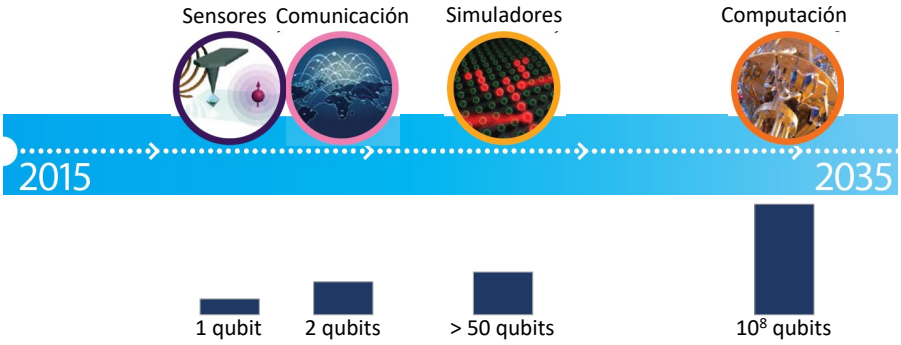

Figura 2: Hoja de ruta de la evolución de las tecnologías cuánticas establecida por la Unión Europea [ABB+18]. Debajo se indica el número típico de qubits que es preciso controlar y leer para llevar a cabo cada una de estas aplicaciones.

2. Tecnologías cuánticas

Existe un consenso entre la comunidad científica y los organismos que la financian en dividir las tecnologías cuánticas en cuatro áreas: sensores, comunicación, simuladores y computación [ABB+18]. Cada una de ellas se caracteriza no sólo por su ámbito de aplicación, sino también por los recursos que necesita para alcanzar una madurez tecnológica. Sensores cuánticos y protocolos de comunicación segura se basan en controlar los estados de una o dos partículas, mientras que plataformas con 50 o más qubits son necesarias para llevar a cabo simulaciones fuera del alcance de las mejores supercomputadoras. Describo brevemente estas tres en esta sección, y dedico las siguientes al considerablemente más complejo, pero también fascinante, reto de construir un ordenador cuántico de propósito general.

Los **sensores cuánticos** [DRC17] aprovechan la fragilidad de algunas funciones de onda, en particular los estados superposición, frente a perturbaciones externas. Lo que para el resto de aplicaciones introduce decoherencia y resulta una de las limitaciónes más serias, es en este caso un recurso. La idea no es totalmente nueva. Un ejemplo de sensor cuántico desarrollado hace décadas es el SQUID (del inglés 'Superconducting Quantum Interference Device') que se basa en la modificación por un flujo externo de la interferencia entre supercorrientes que se propagan en un anillo superconductor con una o dos uniones

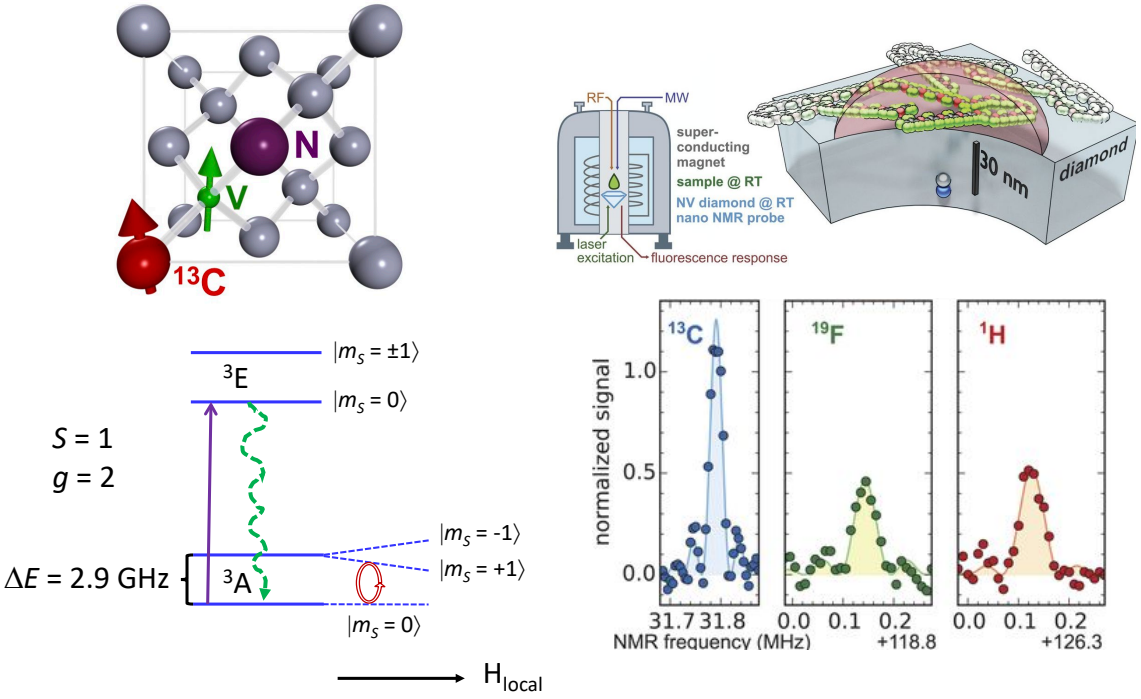

Figura 3: Izquierda: Estructura cristalina del diamante, que muestra un centro de color formado por un átomo intersticial de nitrógeno situado en la vecindad de una vacante de carbono. Debajo se muestra la estructura electrónica de este centro de color, cuyo estado fundamental, un singlete orbital con espín $S = 1$, permite codificar un qubit en los estados $|m_S = 0\rangle$ y $|m_S = +1\rangle$. La diferente fluorescencia asociada a excitaciones desde cada uno de ellos permite realizar una lectura óptica de este qubit. Derecha: Un centro NV^- situado cerca de la superficie del diamante puede utilizarse para detectar espines nucleares en su vecindad, y llevar a cabo medidas de resonancia magética con una elevadísima sensibilidad, basada en la coherencia cuántica de su espín.

Josephson. La diferencia de los avances realizados en los últimos años, como he mencionado antes, es la aparición de sensores basados en la detección de la función de ondas de objetos microscópicos individuales, que ofrecen una mayor capacidad de diseño y de adaptación a la medida de diversas magnitudes.

Un ejemplo ilustrativo son los centros NV^-, o centros de color, en diamante [DMD+13]. Estos centros se forman cuando un átomo intersticial de nitrógeno y una vacante de carbono coinciden en un punto de la estructura cristalina. El centro se caracteriza por un estado fundamental con espín $S = 1$ y una débil anisotropía magnética. Los estados del qubit se asocian a dos de las proyecciones del espín, siendo $|0\rangle \equiv |m = 0\rangle$, el estado fundamental, y $|1\rangle \equiv |m = +1\rangle$. El desdoblamiento entre sus energías se puede sintonizar mediante un campo magnético, mientras que superposiciones de ambos se pueden generar mediante la aplicación de pulsos de microondas, usando técnicas de resonancia magnética electrónica. La frecuencia de Larmor, o la fase de la función de ondas, depende del campo local en la posición de cada defecto, lo que permite usar este sistema como un sensor

magnético [JGP+04]. La extrema dureza del diamante conduce a una casi total ausencia de ruido asociado a vibraciones, incluso a temperatura ambiente, lo que se traduce en tiempos de coherencia de espín bastante largos. Sin embargo, lo que le confiere un interés especial es la posibilidad de leer la polarización de espín de cada centro midiendo su fluorescencia [GDT+97]. Estas medidas permiten reconstruir el campo generado por otros espines de su entorno, por ejemplo espines nucleares $I = 1/2$ del isótopo ^{13}C o bien de muestras colocadas en la vecindad del diamante. La aplicación de pulsos complejos y de técnicas de desacoplo diámico permite una detección selectiva en frecuencia, lo que abre la puerta a identificar diversas fuentes de campo magnético, por ejemplo núcleos de diversa naturaleza o espines en entornos diferentes [APN+17]. Existe un enorme interés en la aplicación de estos sensores para realizar resonancia magnética nuclear sobre células o incluso moléculas individuales, así como para desarrollar sistemas de geolocalización sin necesidad de satélites. Al igual que ocurre con otros sensores, cuánticos o no, la mayor limitación a la sensibilidad está asociada a la interfase con la muestra, que es difícil de optimizar al tratarse de diamante, y a aspectos del material como la modificación que sufren los centros situados cerca de la superficie del cristal. En años recientes, se ha realizado un esfuerzo para buscar otros centros magnéticos en materiales semiconductores, o incluso moleculares [BLM+20], que muestren propiedades similares a las de los centros de color sin algunas de sus limitaciones.

La seguridad de las comunicaciones es de crucial importancia no sólo en aspectos relacionados con la defensa sino también en actividades diarias como transacciones bancarias, compras online, etc. La codificación segura de un mensaje entre dos nodos, el emisor A ('Alice') y el receptor B ('Bob'), conectados por un canal de comunicación se basa en una clave compartida entre ambos y desconocida para terceros. El emisor usa la clave para codificar el mensaje, mediante una cierta transformación sobre los bits originales, y al receptor le permite realizar la transformación inversa y recuperar el mensaje original. El problema es, sin embargo, cómo intercambiar de forma segura la clave entre Alice y Bob. La protección frente a posibles espías ('Eve') ansiosos por apoderarse de la información confidencial o por manipular el mensaje se consigue asociando la clave a una operación que resulta imposible de invertir en términos prácticos. En el caso del muy extendido código RSA (de sus autores, Rivest, Shamir y Adleman, [RSA78]), la clave se protege gracias a la dificultad de factorizar un número que es producto de dos grandes números primos.

La idea de la **comunicación**, o criptografíıa, **cuántica** [BB84,Eke91,XMZ+20] es diferente. La clave se basa en compartir los estados de un cierto número de qubits. Su seguridad proviene del efecto que la medida de cada qubit compartido entre ellos por un tercero, como Eve, tiene sobre el estado del mismo. La intervención externa introduce cambios irreversibles y, por tanto, errores en el mensaje que pueden ser detectados por Alice y Bob. La idea se puede implementar de formas diversas. Por ejemplo, Alice puede enviar fotones con dos posibles estados de polarización, asociados a estados $|0\rangle$ y $|1\rangle$ del qubit, preparados según dos posibles sistemas de referencia. Al ignorar los ejes de polarización de cada qubit, Eve no puede medir su estado y, al mismo tiempo, restaurarlo para reenviarlo a Bob sin perturbar el mensaje. El método más utilizado, propuesto por Ekert [Eke91], se basa en compartir un par de fotones entrelazados. Cualquier interacción externa rompe el entrelazamiento de la función de ondas y puede ser detectado por ambos interlocutores.

Las mayores limitaciones a las que se enfrenta la distribución cuántica de claves son la generación de pares de fotones entrelazados a frecuencias suficientemente altas y las inevitables imperfecciones del canal, que introducen errores incluso en ausencia de un 'espía'. El efecto de la decoherencia limitó las primeras realizaciones experimentales a pruebas en condiciones de laboratorio y sobre distancias de unos pocos centímetros [BBB+92]. Sin embargo, en pocos años, se consiguieron llevar a cabo protocolos de comunicación entre puntos separados por distancias mucho mayores, incluso de varios kilómetros [RHR+07, PZY+07, YCY+16, XMZ+20, Y+20]. La implementación práctica de redes de comunicación interurbana se ha visto impulsada por el empleo de satélites artificiales que se benefician de la casi nula dispersión de la luz en el espacio. En 2021, un equipo del centro de investigación en información cuántica de Shangai (China) creó una red cuántica que combinaba transmisión por fibra óptica y mediante satélites para conectar de manera segura 32 ciudades en una distancia total superior a 4600 km [C+21]. Estos resultados muestran que la comunicación cuántica está a punto de hacerse una realidad práctica, capaz incluso de afectar al equilibrio estratégico entre China y el resto del mundo.

Uno de los retos más importantes de la ciencia consiste en el diseño de nuevos materiales a la carta, con funcionalidad prediseñada y adaptada a una aplicación concreta. Ejemplos relevantes hoy en día son moléculas fertilizantes, catalizadores, vacunas y antibióticos o incluso superconductores de alta temperatura crítica. La física cuántica nos permite escribir las ecuaciones que determinan la estructura electrónica y, en gran medi-

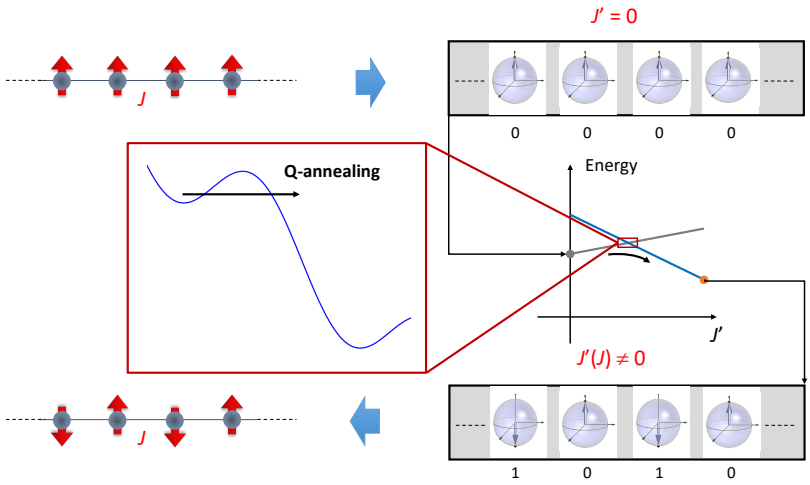

Figura 4: Esquema de un simulador cuántico adiabático. El sistema problema se codifica en otro sistema cuántico cuyas interacciones podemos controlar. En el instante $t = 0$, los qubits se inicializas en su estado fundamental en ausencia de interacciones. Dichas interacciones se activan gradualmente hasta el valor correspondiente al sistema problema y el registro de qubits se mantiene en su estado fundamental. La lectura del estado final proporciona información acerca del sistema problema. Los qubits son capaces de escapar de configuraciones metaestables por procesos de efecto túnel, por lo que a este proceso se le conoce también como templado cuántico (del inglés *quantum annealing*).

da, rigen el comportamiento de un material. Esas ecuaciones son, sin embargo, demasiado complejas para ser resueltas de manera rigurosa, incluso para sistemas de tamaño relativamente modesto (por ejemplo, una molécula que involucre más de 50 electrones).

La **simulación cuántica** analógica se basa en la idea original de Feynman [Fey82], descrita en la introducción, de codificar los estados del 'sistema problema', el que queremos resolver, en estados de otro sistema cuántico sobre el que tenemos un mayor grado de control. Este 'simulador cuántico' [CZ12] puede prepararse en un estado inicial, por ejemplo el estado fundamental de todos los qubits en ausencia de interacción entre ellos. A partir de este momento, se introducen progresivamente las interacciones hasta que se alcanza una situación equivalente a la del sistema problema y se estudia cómo evoluciona el estado fundamental del simulador. El estado final, una vez leído y decodificado, proporciona información acerca del sistema problema. Esta técnica de simulación se denomina también computación cuántica adiabática [AL18], porque el registro de qubits permanece en todo momento en su estado de mínima energía. Esto supone una ventaja frente a la computación basada en operaciones, ya que dicho estado fundamental es a menudo más resistente frente a decoherencia que los estados superposición de diferentes autoestados del Hamiltoniano. La física cuántica proporciona también vías efectivas para escapar de

estados metaestables a través de procesos de efecto túnel [DBI+16]. Otra ventaja es que es posible obtener información sobre el problema incluso a partir de medidas parciales, o incluso usando una medida global del estado del simulador.

La relativa sencillez y robustez de la simulación cuántica ha permitido llevar a cabo realizaciones experimentales con sistemas mucho más complejos que los usados en computación cuántica. Ejemplos notables son redes de átomos o iones enfriados hasta temperaturas próximas al cero absoluto [GB17] mediante luz láser y redes de qubits superconductores [BRI+14]. Otro aspecto muy atractivo de estos experimentos es la posibilidad de crear en el laboratorio nuevos estados de la materia, como nuevas fases magnéticas [RLZ21] o incluso los denominados 'cristales de tiempo' [M+22b]. El mayor reto al que se enfrentan reside en la dificultad de encontrar una codificación suficientemente aproximada de algunos modelos, en particular aquéllos relacionados con problemas de química cuántica que son especialmente relevantes en el diseño de nuevos materiales.

3. Computación cuántica

3.1. Paralelismo cuántico y algoritmos

Hoy en día resulta evidente el enorme progreso que ha experimentado la capacidad de computación, desde las primitivas máquinas de calcular, como Mark-II, que los aliados usaron para descifrar el código Enigma del ejército alemán en la Segunda Guerra Mundial hasta nuestros portátiles actuales. Se podría, sin embargo, argumentar que a pesar de que su 'cuerpo' ha cambiado de manera radical, su 'alma' sigue respondiendo al concepto que Alan Turing introdujo en 1937 [Tur37]. Todos comparten esencialmente el mismo esquema de operación, basada en tomar decisiones sobre cambiar o dejar intactos los estados ('0' ó '1') de un registro de bits según ciertas instrucciones previas. La computación cuántica supone un cambio de este paradigma, como lo es también la inteligencia artificial aunque de manera diferente. El concepto de 'máquina de Turing cuántica' fue introducido por David Deutsch y Roger Penrose a mediados de la década de los 80 del siglo XX [DP85]. En él se introduce la posibilidad de utilizar estados cuánticos del registro de qubits. Junto a las alternativas que maneja una máquina de Turing clásica, aparece entonces una tercera posibilidad en cada paso de operación: además de dejar el qubit con su estado anterior o invertirlo, podemos también ponerlo en un estado superposición.

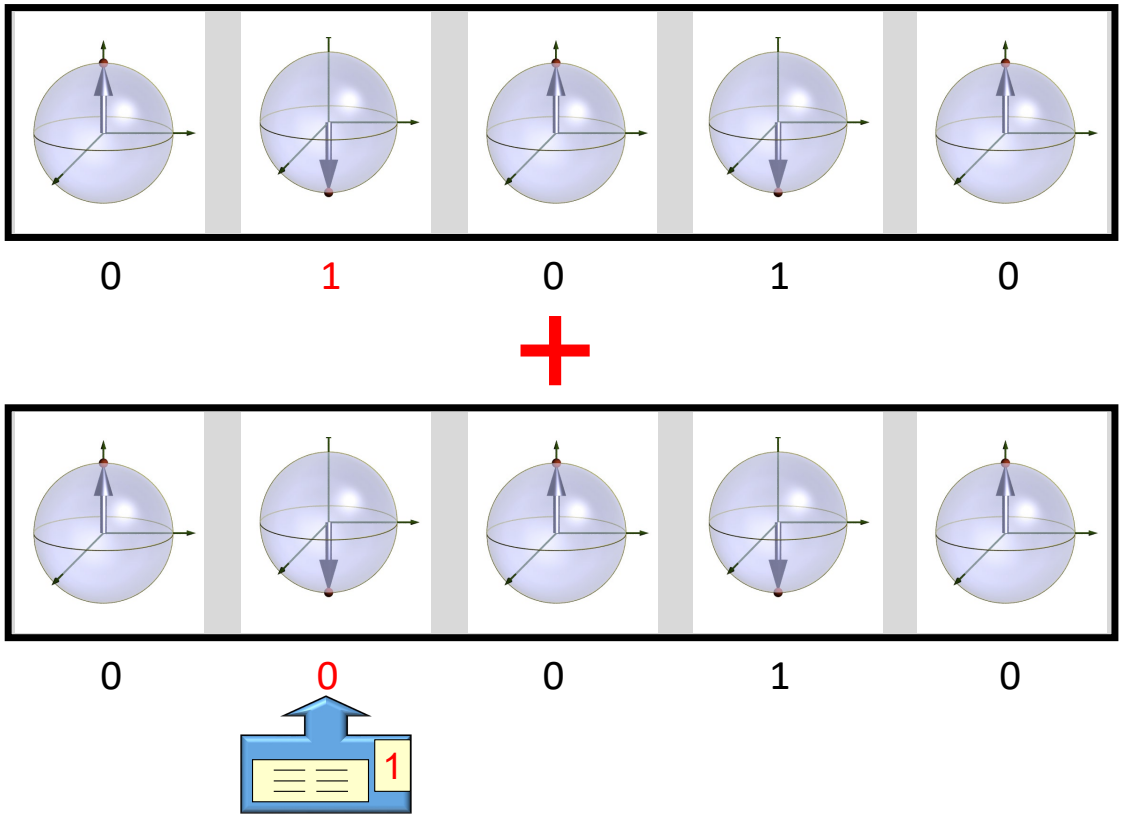

Figura 5: Imagen esquemática del paralelismo cuántico. Una máquina de Turing cuántica está formada por un registro de qubits y una cabeza lecto-escritora, que toma decisiones según unas ciertas instrucciones. A diferencia de una máquina clásica, la decisión puede suponer la creación de una superposición del estado original de cada qubit en el registro, en la figura $|1\rangle$ para el segundo qubit, y del estado opuesto ($|0\rangle$). Este proceso muestra como un ordenador cuántico aprovecha el principio de superposición para explorar diferentes soluciones en paralelo, de forma natural. También muestra que el procesado cuántico utiliza estados entrelazados.

Resulta esperable que el acceso a un conjunto infinitamente mayor de estados de información confiera nuevas posibilidades para resolver problemas. Las superposiciones cuánticas pueden verse como una forma de explorar en paralelo todas las soluciones a un problema dado que, al fin y al cabo, han de escribirse como estados clásicos del registro de qubits. A esta nueva capacidad de procesamiento se le ha llamado por ello 'paralelismo cuántico' [DP85]. No es evidente, sin embargo, que aporte una ventaja para resolver *cualquier* problema. De hecho, desde su concepción, se han encontrado relativamente pocos algoritmos cuánticos que, aprovechando esta posibilidad, mejoren significativamente el rendimiento de sus equivalentes clásicos.

El primero de ellos fue también descrito por Deutsch en su artículo original [DP85]. El problema que aborda es distinguir entre si una función $f(x)$ es constante, es decir, $f(x_i) = 1$ ó 0 para todo el rango de valores discretos de la variable x_i con i= 1 hasta $2N$, o si es equilibrada, es decir, $f(x_i) = 1$ ó 0 para i= 1 hasta N y $f(x_i) = 0$ ó 1, respectivamente,

para i= $N+1$ hasta $2N$. El número de operaciones necesarias para resolver este problema con un ordenador clásico ha de escalar linealmente con N. Sin embargo, un ordenador cuántico puede comparar la función en diversos puntos con una sóla evaluación. Aunque este algoritmo no tiene una aplicación práctica directa, salvo desenmascarar a un apostador fraudulento armado con una moneda de dos caras o dos cruces, resulta ilustrativo del potencial de la computación cuántica. En particular, muestra que dicho potencial no procede de un aumento en la velocidad de procesado ni de una mayor capacidad para almacenar datos. La cantidad de información de un registro de qubits, medida en términos de su entropía de von Neumann, es idéntica a la de su equivalente clásico. Es la capacidad del primero de utilizar estados que están vedados al segundo la que permite simplificar ciertos cálculos, es decir, reducir la complejidad de problemas, o más bien de clases de problemas, que son matemáticamente duros.

El segundo algoritmo cuántico, desarrollado por Shor [Sho94], ejemplifica de forma extrema esta ventaja cuántica. Es además, extremadamente interesante desde el punto de vista práctico. El algoritmo resuelve el problema de encontrar la descomposición de un número natural N en sus factores primos, el problema inverso a la multiplicación. Pero mientras multiplicar es sencillo, la descomposición es un problema matemáticamente muy complejo. Para los algoritmos clásicos conocidos, el número de operaciones necesarias escala exponencialmente con N, por lo que se vuelve prohibitivo en el caso de números de muchas cifras, incluso para las mejores supercomputadoras. El algoritmo de Shor usa la transformada de Fourier cuántica para destilar una solución al mismo problema en tiempo polinomial. Es decir, convierte un problema de clase NP en un problema de clase P. Este algoritmo supone, por este motivo, una amenaza para la mayor parte de los sistemas de seguridad informática que se basan en la distribución abierta de claves y cuya seguridad, como en el caso del código RSA mencionado antes, depende de la dificultad práctica de factorizar grandes números. En otras palabras, la computación cuántica supondría el fin de la criptografía tal y como la conocemos actualmente.

Otro algoritmo con interesantes perspectivas de aplicación es el desarrollado por Grover [Gro97] para la búsqueda en bases de datos no indexadas. Una ilustración de este problema, aunque en nuestros días algo caduca, es la búsqueda en una guía telefónica. Encontrar un número sabiendo el nombre del abonado es un problema sencillo, porque la guía ordena los nombres alfabéticamente. Sin embargo, el problema inverso, encontrar el abonado asociado a un número de teléfono, resulta más complejo. Para un procedimiento de búsqueda clásico, no hay más remedio que probar una a una las entradas de la guía,

por lo que el número de operaciones ha de escalar con el tamaño de la base de datos N. El algoritmo de Grover parte de una superposición $|\psi\rangle$ de todas las entradas de la base y utiliza la aplicación sucesiva de un operador unitario de difusión $\hat{D} \equiv 2|\psi\rangle\langle\psi| - \hat{I}$, donde $\hat{I}$ es el operador identidad sobre el registro de qubits, para amplificar gradualmente la probabilidad de medir el estado que cumple la condición requerida. Es posible demostrar que la solución se puede encontrar con un número de iteraciones que escala con $\sqrt{N}$. Aunque la ganancia no es exponencial, el algoritmo puede suponer una ventaja práctica en algunas situaciones, por ejemplo, en la búsqueda en grandes bases de datos o incluso en la comprobación de soluciones de problemas complejos. Variaciones de este método pueden también ayudar en el entrenamiento de redes neuronales, que forman la base de sistemas de inteligencia artificial, e incluso servir para romper ciertos códigos criptográficos, encontrando aquellos mensajes que tienen sentido gramatical.

Más recientemente se han propuesto algoritmos cuánticos para tareas tan diversas como la inversión de matrices [HHL09], base de la resolución de sistemas de ecuaciones lineales, la recomendación de productos a consumidores [KP16] y la simulación digital, es decir, programable y basada en operaciones, de sistemas cuánticos [WHW+15]. Asimismo, han aparecido algoritmos híbridos, que combinan operaciones clásicas y cuánticas, para abordar problemas de optimización [FGG14]. La trascendencia y amplio espectro de sus posibles aplicaciones justifica la expectación que este campo ha recibido. La siguiente cuestión es, por supuesto, cómo construir una 'máquina de Turing' cuántica, cuáles son los elementos necesarios y sus requisitos, y cómo hacerla realidad. Esas cuestiones se discuten en las secciones que restan.

3.2. Operaciones básicas y universalidad

Cuando un ordenador puede ser programado para realizar cualquier tarea computable se dice que es universal. La universalidad impone que exista un conjunto finito de operaciones básicas, o puertas lógicas, con las que construir cualquier otra. En lógica Booleana clásica, toda puerta se puede descomponer en secuencia de puertas NAND o de puertas NOR. En el caso de un procesador cuántico, la evolución temporal del registro de qubits es estrictamente unitaria, por tanto reversible, y las puertas lógicas son también operadores unitarios. La universalidad [BBC+95] se puede conseguir combinando operaciones sobre qubits individuales, capaces de generar estados superposición arbitrarios, y puertas

condicionales actuando sobre dos qubits, como la puerta CNOT, que invierte el estado del qubit 'diana' si y sólo si el qubit de control se encuentra en un estado específico, por ejemplo $|0\rangle$.

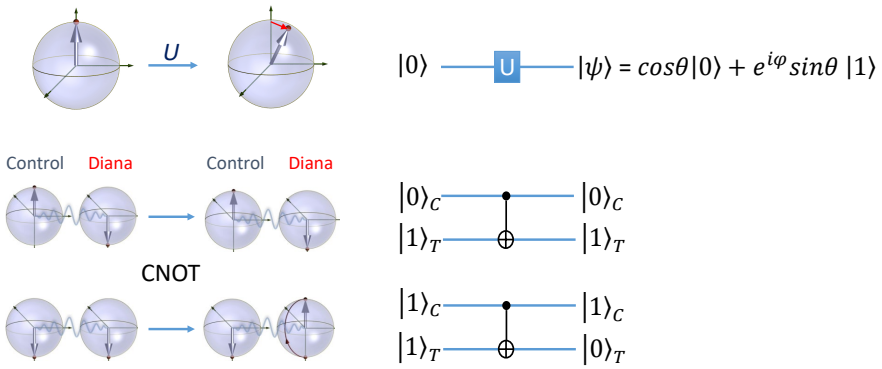

Figura 6: Ejemplo de operaciones lógicas cuánticas que forman un conjunto universal. Arriba: rotación coherente de cada qubit. Abajo: puerta condicional CNOT entre dos qubits.

El funcionamiento de estas puertas lógicas ayuda a introducir algunas señas de identidad de la computación cuántica. Consideremos la aplicación de una puerta CNOT sobre un par de qubits, uno de los cuales, el qubit control, se encuentra en un estado superposición.

$$(|0\rangle + |1\rangle)_C \otimes |0\rangle_T \rightarrow_{CNOT} |0\rangle_C \otimes |0\rangle_T + |1\rangle_C \otimes |1\rangle_T \tag{3.1}$$

El resultado es un estado que no se puede poner como producto de un estado del control y otro del diana y que es máximamente entrelazado. Este ejemplo muestra que la aplicación de operaciones lógicas sobre estados cuánticos de varios qubits conduce de manera natural a la aparición de estados entrelazados en los que la información se codifica en las correlaciones, por tanto de manera radicalmente diferente a la de un registro digital convencional.

La segunda consecuencia es la imposibilidad de realizar copias perfectas, o 'clones' de estados arbitrarios de un qubit [WZ09]. En principio, uno puede copiar los estados de base $|0\rangle$ y $|1\rangle$ usando el qubit como control de una operación condicional, como una puerta CNOT, actuando sobre un segundo qubit que se inicializa en su estado fundamental $|0\rangle$.

Sin embargo, la Ec. (3.1) muestra que esta operación no transfiere un estado superposición del primer al segundo qubit. De hecho, en el estado resultante es imposible asignar un estado definido a ninguno de los dos qubits por separado.

3.3. De la idea a la realidad: errores y su corrección

Aunque la evolución asociada a las diferentes operaciones es unitaria, existen dos procesos irreversibles en computación cuántica. El primero es la inicialización del registro de qubits, usualmente en un estado no entrelazado como $|00\ldots00\rangle$. El segundo es la lectura o medida de los resultados. La medida juega un papel central en física cuántica, muy diferente al concepto clásico. La interacción con el aparato de medida proyecta el estado de un qubit sobre el autoestado del operador que representa a la magnitud que se mide, de acuerdo con el famoso postulado de la medida y el colapso de la función de ondas [WZ83]. Una consecuencia es que el resultado de una computación cuántica ha de ser un estado 'clásico'. Sólo entonces la medida en la base operacional (definida por los proyectores sobre los estados lógicos $|0\rangle$ y $|1\rangle$ de cada qubit) da una información completa sobre el estado final. En el caso de un estado superposición, el resultado de la medida será bien uno u otro con la correspondiente amplitud de probabilidad.

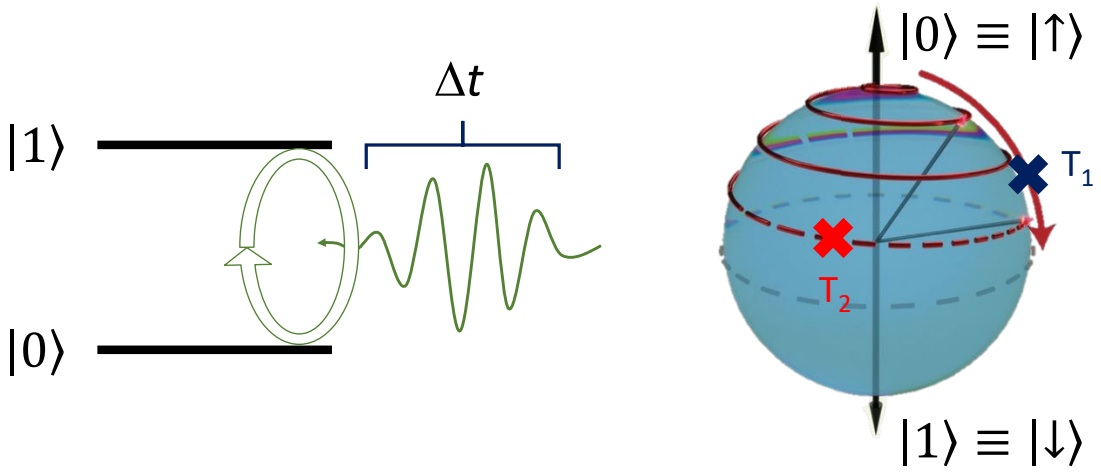

Figura 7: La rotación coherente de un qubit se puede llevar a la práctica mediante la aplicación de un pulso resonante sobre un sistema físico de dos niveles. Los estados accesibles mediante esta operación se pueden representar como puntos en la superficie de una esfera, conocida como 'esfera de Bloch' cuyos 'polos' Norte y Sur corresponden a los estados de la base computacional. La trayectoria cuántica corresponde a una evolución desde el estado inicial, en este caso $|0\rangle$, hacia el estado final, acompañada por la precesión de Larmor en torno al eje de cuantización. En esta representación, procesos de relajación hacia el equilibrio introducen saltos estocásticos en la latitud del estado, mientras que procesos de desfase provocan saltos estocásticos en su longitud, a energía constante.

Además de estos procesos, la evolución unitaria, o coherente, de los qubits puede romperse debido a perturbaciones causadas por su interacción con el entorno, un proceso conocido como decoherencia [Zur03]. El ruido es un problema también en información clásica, pero en la computación cuántica adopta nuevas formas, Más aún, resulta la amenaza más seria para su implementación práctica, debido a la necesidad de mantener de forma precisa estados superposición, habitualmente más frágiles que los estados puros. La naturaleza de los posibles errores de un qubit puede ilustrarse considerando la evolución temporal de un sistema de dos niveles, por ejemplo un electrón con espín $S = 1/2$ en un campo magnético. Los posibles estados del qubit forman los puntos de una esfera, denominada esfera de Bloch, cuyos polos 'Norte' y 'Sur' corresponden a $|0\rangle$ y $|1\rangle$, respectivamente. Partiendo del estado fundamental $|0\rangle$ es posible generar una superposición arbitraria mediante un término de control, por ejemplo una perturbación oscilante

$$\hat{W}(t) = \hat{W}_0 \cos \omega t \tag{3.2}$$

cuya frecuencia ω cumpla la condición de resonancia $\hbar\omega = \Delta E_{10}$ con el desdoblamiento ΔE_{10} entre los niveles del qubit. Tras un tiempo t, el estado evoluciona hacia [Rab37]

$$|\psi\rangle(t) = \cos \frac{\Omega_R t}{2}|0\rangle + e^{i\Phi(t)} \sin \frac{\Omega_R t}{2}|1\rangle \tag{3.3}$$

que corresponde a una rotación coherente desde $|0\rangle$ hacia $|1\rangle$ a la frecuencia de Rabi

$$\Omega_R = \frac{\langle 1|\hat{W}_0|0\rangle}{\hbar} \tag{3.4}$$

acompañada de una precesión alrededor del eje de cuantización a la frecuencia de Larmor ω, que determina la fase $\Phi(t)$ de la función de ondas.

Si el qubit no está completamente aislado, y ninguno lo está, existen términos adicionales a $\hat{W}$ que modifican la evolución con respecto a la predicha por la Ec. (3.3) de una forma que escapa a nuestro control. Por ejemplo, las interacciones que tienden a llevar el sistema hacia su equilibrio térmico inducen transiciones entre los estados del qubit. Estos errores, cuyo tiempo característico se denomina T_1, pueden verse como fluctuaciones en

la 'latitud' del estado sobre la esfera de Bloch y se denominan 'bit flips'. Por otra parte, pueden existir interacciones que sean diagonales en el Hamiltoniano del qubit, que introduzcan fluctuaciones en ω y, por tanto, cambios irreversibles en la fase de la función de ondas. Estos saltos estocásticos en la 'longitud' sobre la esfera de Bloch, se denominan 'phase shifts' y no necesitan cambiar la energía media del qubit. Su tiempo característico T_2 suele ser más corto que el tiempo de relajación T_1 y a menudo son estos procesos los que limitan el tiempo disponible para realizar operaciones sobre un qubit.

Una forma de combatir el efecto pernicioso de estos errores es aislar el registro de qubits de fuentes de ruido de fase y de relajación térmica. Sin embargo, la condición de aislamiento perfecto no existe y, además, entra en conflicto con la necesidad de acoplar los qubits con un sistema de control que permita realizar operaciones y leer los resultados de la computación. La alternativa natural es implementar un sistema que permita detectar los errores que se producen y corregirlos. El concepto de corrección de errores se basa en la codificación redundante de la información. Para entenderlo con un ejemplo, podemos pensar en la comunicación a través de un medio tan ruidoso como WhatsApp. A pesar de que existan cambios u omisiones de algunas letras, a veces adrede, es posible inferir el significado del mensaje debidos a que todos los idiomas incluyen más símbolos de los estrictamente necesarios. En computación clásica, y especialmente en sistemas que incluyen componentes muy pequeños y sensibles al ruido, la corrección se introduce creando copias de la información y realizando comparaciones entre ellas a intervalos regulares.

Este protocolo es, sin embargo, difícil de trasladar al caso cuántico por dos motivos que he mencionado anteriormente. El primero es que es imposible clonar un estado cuántico para realizar copias exactas de él. El segundo es que la lectura de un estado cuántico produce cambios irreversibles. Durante años, la aparente imposibilidad de corregir errores relegó la computación cuántica a la categoría de curiosidad científica, con una remota aplicación práctica. Esta situación cambió de manera radical cuando Peter Shor [Sho95] demostró que es posible detectar errores sin medir el estado del qubit y corregirlos sin duplicarlo.

La idea de cualquier protocolo de corrección de errores [Sho95, Ste96, Ter15] se basa en introducir una codificación redundante de los estados de la base computacional y en la posibilidad de comparar estados cuánticos sin realizar medidas proyectivas. Para ilustrarla, consideramos el código de Shor que permite corregir un 'bit flip'. El nuevo qubit lógico pasa a estar formado por tres qubits 'físicos', con los que se define una nueva base computacional

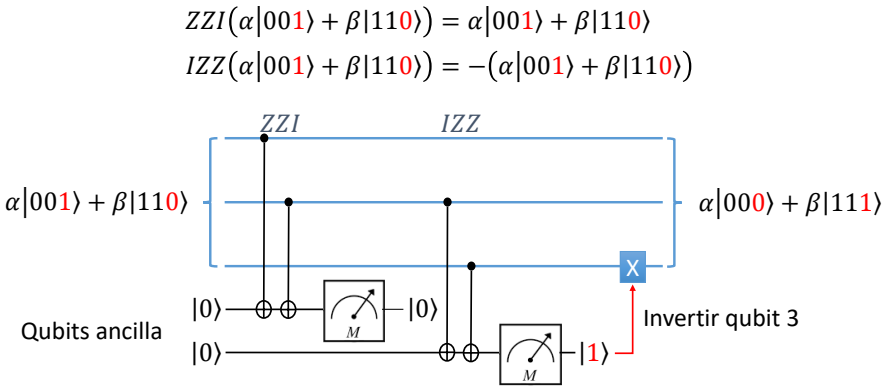

Figura 8: Circuito de un código de Shor que corrige errores que involucran la inversión de un qubit ('qubit flips').

(3.5)
$$|0\rangle_{L3} \equiv |000\rangle$$
$$|1\rangle_{L3} \equiv |111\rangle$$

La comparación entre estados, que permite detectar diferencias causadas por errores sin adquirir información sobre el estado en sí, se realiza mediante los llamados operadores estabilizadores. En este código, son productos del operador identidad actuando sobre uno de los tres qubits y de dos matrices de Pauli Z, tal que $Z|0\rangle = |0\rangle$ y $Z|1\rangle = -|1\rangle$, actuando sobre los otros dos. Estos operadores se caracterizan por dejar intactos tanto los estados de la base computacional como cualquier superposición de ellos. Por ejemplo

(3.6)
$$IZZ(\alpha|000\rangle + \beta|111\rangle) = \alpha|000\rangle + \beta|111\rangle$$
$$ZIZ(\alpha|000\rangle + \beta|111\rangle) = \alpha|000\rangle + \beta|111\rangle$$
$$ZZI(\alpha|000\rangle + \beta|111\rangle) = \alpha|000\rangle + \beta|111\rangle$$

mientras que su aplicación introduce un cambio de signo si alguno de los tres qubits ha invertido su estado. En la práctica, estos operadores se pueden implementar mediante dos puertas CNOT que tomen por control a dos de los qubits y que compartan como diana un qubit adicional, o ancilla. El error se traduce en un cambio del estado de esta ancilla que puede medirse sin perturbar al qubit lógico y que permite, por tanto, deshacer el error para obtener el estado original.

Extensiones de este código a espacios computacionales formados por 9 qubits más 8 qubits auxiliares permiten detectar y corregir 'phase flips' [Sho95]. Es también posible reducir el coste en recursos, es decir, el número de qubits adicionales, usando una codificación más apropiada de los estados lógicos. Por ejemplo, el código de Steane [Ste96] reduce el número de qubits físicos de la base a 7, igual que ocurre con los denominados códigos de color, que admiten una representación gráfica de los estados de información [BM06]. Además de aumentar el número de qubits todo código de corrección de errores implica también la realización de operaciones adicionales que son también proclives a sufrir errores. Para que estos códigos tengan un efecto netamente favorable es preciso que la probabilidad de error disminuya con su aplicación sucesiva. Esta condición de 'tolerancia frente a fallos' [KLZ98] impone un umbral máximo a la tasa relativa de errores por operación, que en el caso del algoritmo de Shor y otros similares es de 10^{-3}. Existen códigos topológicos, definidos sobre redes de qubits con geometrías específicas, que permiten aumentar este umbral notablemente, hasta valores del orden de 10^{-1}, pero a costa de aumentar el número de qubits necesarios para codificar cada qubit lógico. En el caso del código de superficie [BK98,FMMC12], la unidad mínima incluye 13 qubits físicos y 12 ancillas. La corrección de errores complica también la aplicación de operaciones sobre los qubits lógicos, en particular las puertas condicionales de dos qubits. Estas consideraciones determinan el tamaño de un procesador capaz de abordar la resolución de problemas prácticos. Por ejemplo, se estima que la implementación del código de factorización de Shor para números relevantes en criptografía podría requerir un procesador de hasta 10^8 qubits [FMMC12], en caso de utilizar un código de superficie.

4. Implementaciones

Las consideraciones anteriores determinan, en buena parte, los requisitos de posibles realizaciones de un 'hardware cuántico' [DiV00]. Necesitamos un registro de qubits, cuantos más mejor, cuyos estados puedan inicializarse y controlarse de manera coherente mediante estímulos externos, como pulsos electromagnéticos, y la posibilidad de comunicar entre sí dos de ellos cualesquiera para implementar puertas condicionales. Los candidatos para formar los qubits, sistemas físicos con al menos dos estados accesibles experimentalmente, incluyen desde entes microscópicos como espines nucleares hasta circuitos.

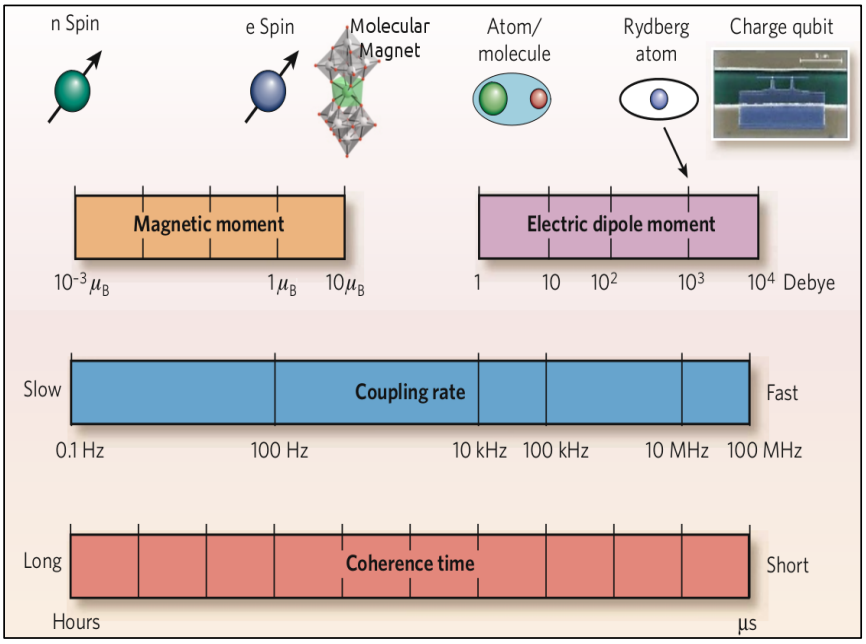

Figura 9: Candidatos para realizar qubits [SG08]. A la izquierda se agrupan qubits de espín, que responden a estímulos magnéticos. Suelen caracterizarse por tiempos de coherencia largos (escala inferior, en naranja) pero también por frecuencias de operación bajas (escala central, azul). A la derecha se muestran qubits de carga, tanto microscópicos como circuitos. Se caracterizan por más sensibilidad al ruido, y por tanto tiempos de coherecnia más cortos, pero también velocidades de operación más elevadas.

Un parámetro que permite evaluar y comparar entre sí las prestaciones de diversas aproximaciones es la fidelidad, que para una puerta lógica dada mide la distancia entre el estado final que se desea obtener $|\psi\rangle$ y el conseguido en realidad $|\psi_{\text{exp}}\rangle$

$$\mathcal{F} \equiv |\langle\psi_{\text{exp}}|\psi\rangle| \tag{4.1}$$

El objetivo de maximizar la fidelidad de las puertas universales, hasta el punto de llegar al límite de tolerancia a errores mencionado antes, depende del balance entre la velocidad de operación y la sensibilidad a perturbaciones externas que son fuente de decoherencia. Este difícil equilibrio entre la necesidad de acoplar fuertemente los qubits entre sí y a señales de control, al mismo tiempo que se mantienen aislados del ruido, resume buena parte de las dificultades a las que se enfrenta la construcción de ordenadores cuánticos reales y suficientemente potentes. Qubits que responden a estímulos eléctricos suelen ofrecer elevadas frecuencias de operación pero tiempos de coherencia más cortos mientras que a los que responden a estímulos magnéticos les sucede justo al revés [SG08]. Esto explica que, a pesar del éxito reciente de algunos esquemas, en particular los que se basan en qubits superconductores, quede todavía un margen muy amplio a la creatividad y la búsqueda de nuevas posibilidades.

A continuación, doy una breve descripción de algunos ejemplos relevantes, siguiendo una evolución aproximadamente histórica desde qubits microscópicos hasta sistemas más complejos y tratando de mostrar sus ventajas y potencial, así como los retos que afrontan para cumplir con los requisitos anteriores.

4.1. Qubits microscópicos: espines e iones

La física cuántica nació para explicar las propiedades de los componentes elementales de la materia, átomos y partículas subatómicas. Resulta, por ello, muy natural buscar entre ellos a posibles candidatos para realizar qubits. Los **espines de núcleos**, como los de Hidrógeno, Flúor o algunos isótopos de Carbono que se encuentran en moléculas orgánicas relativamente sencillas, como el cloroformo, proporcionan sistemas especialmente atractivos [VC05]. En disolución, los tiempos de coherencia de espín son muy largos, en ocasiones cercanos al rango de milisegundos o incluso más, y su manipulación coherente es casi estándar gracias a técnicas de resonancia magnética nuclear. En presencia de un campo magnético uniforme, espines asociados a diferentes elementos de cada molécula, o incluso del mismo elemento pero situados en entornos de coordinación diferentes, pueden distinguirse gracias a sus muy bien resueltas frecuencias de resonancia. Rotaciones coherentes de los qubits se inducen mediante pulsos de radiofrecuencia específicos. Asimismo, se han desarrollado secuencias más complejas para realizar puertas de dos qubits, que aprovechan las interacciones naturales, normalmente dipolares, entre los espines de una misma molécula. En ambos casos, se consiguen velocidades de operación del orden de kHz. Encadenando varias de ellas se llevaron a cabo las primeras pruebas de concepto experimentales de algoritmos cuánticos, entre ellos el algoritmo de Deutsch [CVZ+98] y la factorización del número 15 basada en el protocolo de Shor mencionado antes [VSB+01].

Sin embargo, esta aproximación presenta también importantes limitaciones técnicas. Los experimentos se realizan sobre conjuntos macroscópicos de moléculas cuyos niveles de espín nuclear presentan una inevitable distribución térmica de poblaciones (los experimentos se realizan a menudo a temperatura ambiente, mientras que la separación entre niveles es del orden de mK o menos). Esto impide una apropiada inicialización del registro de qubits, complica notablemente la interpretación de los resultados, que son en esencia promedios de evoluciones temporales desde estados diferentes y, sobre todo, imposibilita en la práctica escalar más allá de una molécula. A pesar de ello, estos experimentos

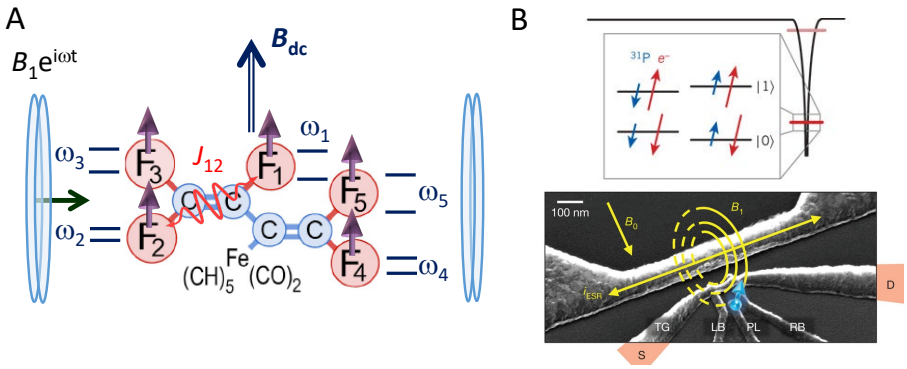

Figura 10: Qubits de espín. A) Espines nucleares de flúor en una molécula orgánica. El diferente entorno conduce a frecuencias de resonancia diferentes para los diferentes átomos en presencia de un campo magnético estático B_{dc}, lo que permite seleccionar cuál de ellos realiza una rotación coherente ajustando la frecuencia ω de la radiación externa. Las operaciones de dos qubits se implementan combinado pulsos de radiofrecuencia e interacciones entre espines nucleares próximos. B) Arriba: Un ion dopante de fósforo en silicio genera un defecto que tiene un espín electrónico $S = 1/2$ y un espín nuclear $I = 1/2$, cada uno de los cuales puede codificar un qubit. Abajo: Los estados de espín pueden leerse a partir de la conductividad de un transistor y controlarse mediante pulsos de microondas generados por una micro-antena.

abrieron la puerta del laboratorio a la computación cuántica y ayudaron a desarrollar numerosas técnicas de control que han sido más tarde adoptadas en otras situaciones muy diversas.

Otro ejemplo de espines muy bien aislados de su entorno lo constituyen **impurezas en ciertos materiales semiconductores** [ABD+13], como los centros de color en diamante mencionados antes o donantes de fósforo P^+ en silicio [Kan98]. A bajas temperaturas, cada donante tiene asociado un electrón de valencia extra, que no participa de los enlaces covalentes con otros átomos de Si. Además, el ion P^+ posee un espín nuclear $I = 1/2$. Este centro proporciona una aproximación a un átomo de hidrógeno aislado, que puede codificar un qubit en sus estados de espín electrónico y otro en sus estados de espín nuclear. El silicio es una matriz especialmente adecuada para albergarlos. Su bajo acoplamiento espín órbita da lugar a tiempos de relajación espín red muy largos mientras que la baja concentración de espines nucleares (sólo el 5 % del isótopo ^{29}Si tiene $I = 1/2$) y de otras impurezas magnéticas se refleja en elevados tiempos de coherencia. En muestras de silicio purificado isotópicamente y a temperaturas cercanas al cero absoluto, se han encontrado valores récord de T_2 para cualquier qubit de estado sólido, del orden de 0.5 s para el espín electrónico y de 30 s para el espín nuclear [MDL+14]. Pero probablemente su mayor atractivo se debe a la posibilidad de realizar un 'read-out' de los estados de espín usando una conversión de dichos estados a diferentes valores de conductividad eléctrica que, a diferencia de los primeros, pueden ser medidos con precisión suficiente. Esta posibili-

dad ha permitido la manipulación coherente y la detección de los estados de impurezas individuales [M$^+$10, PTD$^+$12]. Sin embargo su excelente aislamiento dificulta también la conexión coherente de dos o más impurezas, lo que ha impedido hasta muy recientemente demostrar puertas de dos qubits [M$^+$22a]. El limitado potencial de escalado constituye uno de los puntos débiles de los esquemas basados en semiconductores. A pesar de que dichas limitaciones se han conseguido resolver en parte usando sistemas artificiales, formados por puntos cuánticos que confinan estados de carga y de espín, los procesadores cuánticos más avanzados basados en esta tecnología no superan todavía los 4 qubits [HLR$^+$21].

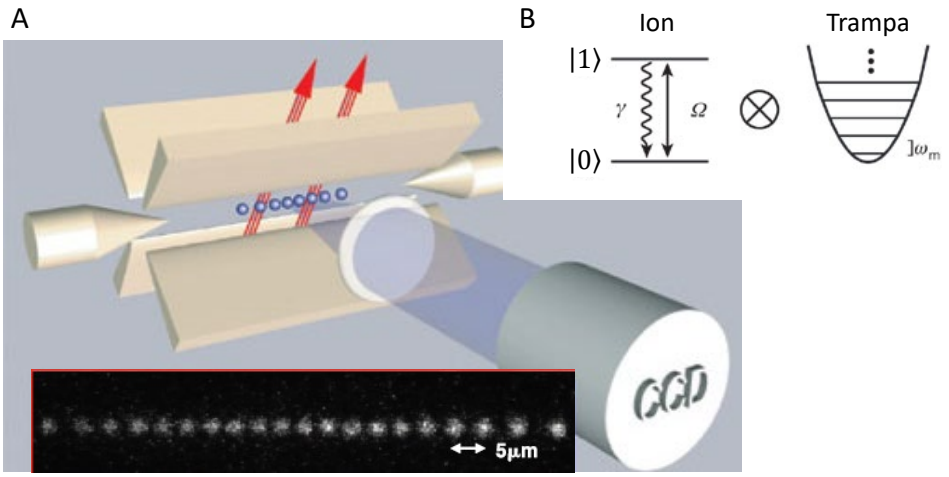

Figura 11: Iones atrapados y enfriados mediante campos eléctricos y haces de luz láser pueden codificar qubits. Pulsos láser o de micro-ondas permiten implementar rotaciones de cada qubit, mientras que la interacción con vibraciones de la trampa permite generar interacciones efectivas entre ellos, e implementar puertas condicionales.

La interacción cuasiresonante de luz láser con gases diluidos ha proporcionado una muy potente herramienta para manipular átomos. Es posible reducir su velocidad media, es decir enfriarlos hasta temperaturas próximas al cero absoluto, y confinarlos en el espacio con una alta precisión. Usar iones cargados introduce una repulsión electrostática que, combinada con pozos de potencial generados por la interferencia de varios haces láser, ha permitido aislar decenas de ellos en posiciones bien separadas entre sí dentro de cámaras de ultra alto vacío, comúnmente conocidas como trampas de iones [MK13]. La estructura electrónica de cada ion presenta un número de niveles electrónicos e hiperfinos que pueden utilizarse para codificar un qubit. Las rotaciones coherentes se inducen mediante pulsos ópticos o de micro-ondas, resonantes con la transición correspondiente del átomo elegido. Esta tecnología proporciona también un marco experimental adecuado para la primera propuesta de puertas condicionales, que constituyó un hito en pos de una arquitectura escalable [CZ95]. Esta propuesta, de marcado carácter español, introduce interacciones

efectivas entre iones medidas por su acoplo con los modos armónicos de la trampa, una idea que ha sido más tarde aprovechada en situaciones diversas. Estos dispositivos se han utilizado para llevar a cabo con éxito pruebas de códigos topológicos de corrección de errores [NMM+14]. Sin embargo, a pesar de la introducción de trampas iónicas integradas en chips y de contar con la ventaja de unos tiempos de coherencia muy competitivos, su escalado más allá de unas decenas de átomos supone todavía un reto considerable. Es posible trabajar con muchos átomos en una trampa pero a costa de perder resolución en el control y lectura de los estados atómicos así como velocidad en la implementación de puertas lógicas condicionales. Probablemente la aplicación más importante de estos sistemas sea en el ámbito de la simulación cuántica analógica, donde es posible obtener información relevante acerca del sistema problema a partir de medidas sobre el estado global del simulador [GB17].

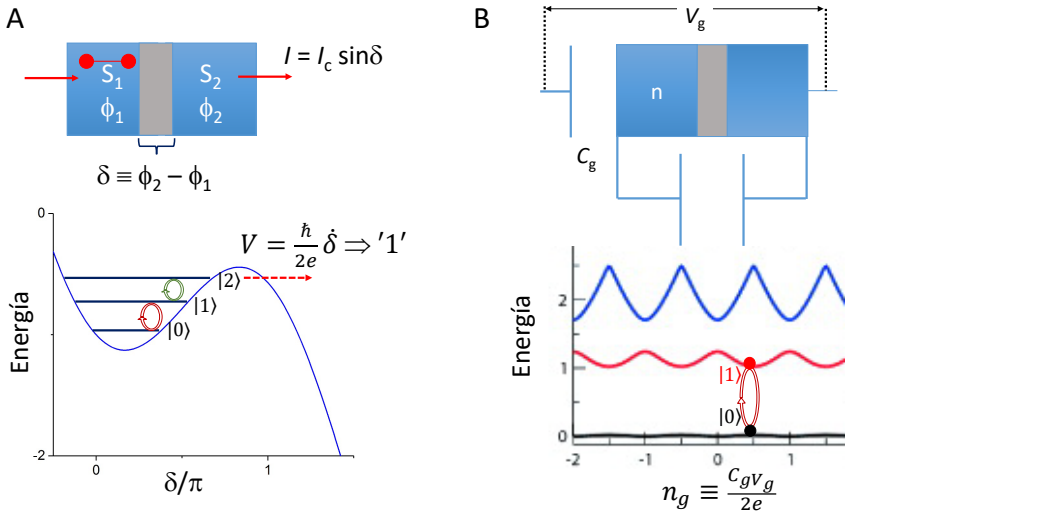

Figura 12: Ejemplos de qubits superconductores [CW08]. A) Qubit de fase. Sus estados se basan en la diferencia de fase δ entre las funciones de onda superconductoras a ambos lados de una unión Josephson. El carácter no lineal de dicha unión da lugar a un espectro anharmónico, que permite definir los estados del qubit y controlarlos mediante radiación de microondas. La lectura se lleva a cabo mediante la aplicación de un pulso resonante con la transición $|1\rangle \rightarrow |2\rangle$, que genera un cambio de fase y, por tanto, un voltaje, sólo si el estado del qubit es $|1\rangle$. B) Qubit de carga o trasmón. Los estados se asocian a dos superposiciones de estados caracterizados por el número de pares de Cooper n en una isla superconductora separada del resto del circuito por una unión Josephson. Un condensador externo permite sintonizar la frecuencia de túnel de los pares de Cooper que determina la frecuencia del qubit y hacerla más insensible a ruido eléctrico.

4.2. Circuitos cuánticos superconductores

Los dispositivos superconductores basados en uniones Josephson han jugado un papel central en la investigación de fenómenos cuánticos a escala macroscópica. Gracias a ellos, se ha logrado mostrar que el efecto túnel o el principio de superposición se aplican tam-

bién a estados asociados con magnitudes físicas tan cercanas a nuestra percepción como el voltaje o la corriente eléctrica, y todo ello en circuitos visibles para el ojo humano. Asimismo, constituyen la plataforma de futuras tecnologías cuánticas que probablemente se encuentra más avanzada en la actualidad [CW08, DS13]. Una unión Josephson es una barrera túnel que separa dos materiales superconductores. Su equivalente eléctrico es un circuito resonante formado por un condensador en paralelo con una inductancia que depende de manera no lineal de la diferencia de fase δ entre las funciones de onda de los pares de Cooper a ambos lados de la unión. La no linealidad da lugar a un espectro de energía anarmónico. Gracias a ello, dos niveles, usualmente el estado fundamental y el primer excitado, pueden codificar un qubit.

La naturaleza de estos estados depende de la relación entre dos escalas de energía, la energía de Josephson $E_J = I_c\Phi_0/2\pi$ y la de carga $E_C = e^2/C$ que parametrizan, respectivamente, la probabilidad de túnel a través de la unión y la energía acumulada en el condensador. Si la primera domina, los estados se pueden caracterizar por su diferencia de fase, lo que da lugar al qubit de fase o su pariente cercano, el qubit de flujo que está formado por un anillo con dos o tres uniones, es decir un SQUID. En caso contrario, los estados están caracterizados por su carga. En este límite se encuentran los qubits de carga, formados por una isla superconductora, o 'caja cuántica', separada del resto del circuito por una unión túnel y cuyos dos niveles de menor energía corresponden a la ausencia $|0\rangle$ o presencia $|1\rangle$ de un par de Cooper. Modificando la caida de voltaje en la unión es posible hacer que ambas situaciones tengan la misma energía clásica. Sin embargo, los autoestados cuánticos son superposiciones de $|0\rangle$ y de $|1\rangle$ con energías separadas por un desdoblamiento de efecto túnel que define la frecuencia del qubit.

Los tiempos de coherencia de estos dispositivos han aumentado de forma espectacular, desde fracciones de ns a principios de siglo hasta casi ms en la actualidad, gracias a mejoras en los materiales y las técnicas de fabricación, así como en sus condiciones de operación (temperatura y apantallamiento de ruido electrónico sobre todo) [DS13]. En paralelo, se han creado imaginativas soluciones gracias a las posibilidades que ofrece el diseño de los circuitos. Un ejemplo notable es el trasmón [KYG+07], que se basa en un qubit de carga al que se añade un condensador externo para reducir la capacitancia neta y aumentar el desdoblamiento por efecto túnel. La casi nula variación de la frecuencia del qubit característica del anticruzamiento entre niveles túnel reduce de manera muy significativa su sensibilidad a ruido eléctrico, el más nocivo en el caso de circuitos superconductores.

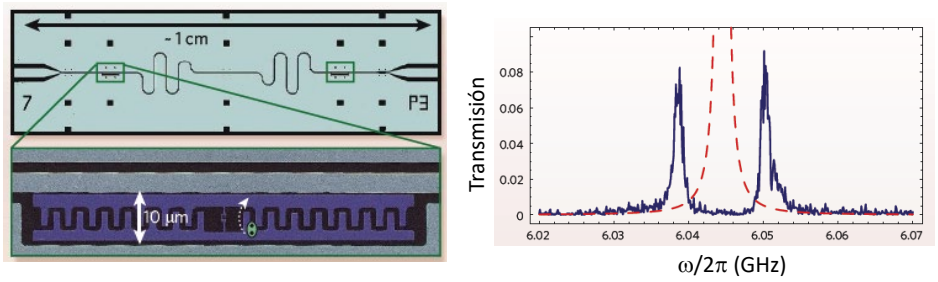

Figura 13: Izquierda: Imagen de un resonador superconductor 'en chip' (arriba) acoplado a un átomo artificial, en este caso un qubit superconductor de carga (abajo). Derecha: Cuando ambos sistemas están en resonancia, la interacción mutua genera superposiciones enlazantes y antienlazantes de excitaciones de luz (fotones de cavidad) y materia (el qubit) que pueden resolverse espectroscópicamente si dicha interacción es más fuerte que la decoherencia. En este límite, la transmisión a través del circuito permite leer el estado del qubit.

Pero probablemente la mayor ventaja de los circuitos superconductores para el desarrollo de ordenadores cuánticos radica en su notable capacidad de escalado. Los qubits son circuitos relativamente grandes y pueden conectarse entre sí en un chip usando componentes como condensadores o inductancias sintonizables. Una de las arquitecturas con mayor potencial es la basada en la denominada 'electrodinámica de circuitos', que consiste en traducir el problema de la interacción luz-materia a un circuito superconductor [SG08, BHW+04]. El esquema básico se compone de un 'átomo artificial', en este caso un qubit superconductor, que está acoplado a una cavidad resonante, usualmente otro circuito superconductor. Un ejemplo sencillo es un resonador coplanar, esencialmente un pedazo de hilo superconductor limitado por dos condensadores cuya longitud define modos resonantes estacionarios del campo electromagnético de manera análoga a la vibración de una cuerda. Cuando la frecuencia de Rabi $G/\hbar$ asociada a la interacción entre ambos componentes es mayor que las tasas de coherencia del qubit $1/T_2$ y de la cavidad κ, se generan estados híbridos de excitaciones de luz (los fotones de la cavidad) y de materia (los estados excitados del qubit) [WSB+04]. En este límite de acoplo fuerte, o coherente, la frecuencia de la cavidad depende del estado, $|0\rangle$ ó $|1\rangle$, del qubit, lo que proporciona un método para realizar una lectura dispersiva, no destructiva, de dicho estado [BHW+04]. Además, la interacción de dos qubits sintonizados entre sí con un mismo modo genera un acoplo efectivo y coherente entre ellos, que permite comunicarlos a distancia y llevar a cabo puertas condicionales [M+07]. Este esquema puede replicarse para crear la topología de un código de superficie, cuyo umbral de error para la operación resistente a fallos es compatible con el rendimiento de los circuitos superconductores.

4.3. *La era NISQ: supremacía cuántica*

Partiendo de sencillas pruebas de concepto, algunas implementaciones, en especial las basadas en iones atrapados y qubits superconductores, han progresado notablemente hasta crear plataformas capaces de llevar a cabo operaciones mucho más complejas. Estos 'ordenadores cuánticos' de pequeña escala no pueden todavía ejecutar códigos de corrección de errores, y no se espera que puedan en un corto o incluso medio plazo. Trabajar con ellos requiere, por tanto, aprender a convivir con el ruido inherente, que limita severamente las tareas a las que pueden enfrentarse. Aunque esto significa que el sueño de un ordenador cuántico programable queda aún lejos, los NISQS (de su abreviatura en inglés 'Noisy Intermediate Size Quantum Systems' [Pre18]) ofrecen la posibilidad única de controlar sistemas cuánticos formados por muchos elementos, que pueden codificar y procesar información en estados entrelazados, de manera radicalmente diferente a como lo hace un procesador digital clásico. La cuestión central de esta 'era NISQ' es, por tanto, qué hacer con ellos.

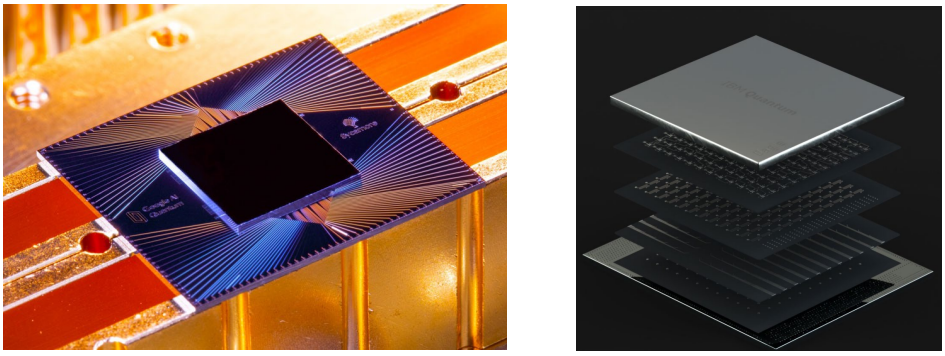

Figura 14: Izquierda: Imagen del procesador cuántico Sycamore, desarrollado por Google, que incluye 52 qubits superconductores y que logró por vez primera mostrar la ventaja cuántica en un problema computacional. Derecha: Imagen de las diferentes capas del procesador cuántico Eagle, desarrollado por IBM, que incluye más de 100 qubits superconductores.

Una ambición que ha sobrevolado el campo de las tecnologías cuánticas desde sus comienzos, y que ha servido de acicate para los desarrollos experimentales, es la demostración de la 'supremacía cuántica'. El objetivo es aprovechar la ventaja que ofrece utilizar el 'paralelismo cuántico' que introdujo David Deutsch [DP85] para llevar a cabo una tarea computacional que sea inaccesible a incluso los mejores supercomputadores. Encontrar una tarea adecuada, suficientemente bien definida y que permita comparar el rendimiento de máquinas clásicas y cuánticas se ha convertido en un campo de investigación en sí mismo. La que se ha impuesto es una especialmente bien adaptada a los procesadores cuánticos existentes: determinar la distribución de los resultados de medir los qubits tras

ejecutar una secuencia aleatoria de puertas lógicas de uno y dos qubits [LBR17], que resulta obviamente sencilla para ellos pero extremadamente compleja para las computadoras convencionales a medida que aumenta el tamaño del procesador. La carrera por alcanzar la supremacía cuántica ha atraído también el interés de gigantes de la informática, como Google, Intel e IBM, y generado la creación de numerosas empresas tecnológicas. Esta implicación industrial, que crece cada año, apoya la credibilidad de la segunda revolución cuántica como un área con un potencial para el avance de la tecnología y la sociedad, aunque también ha significado la aparición de un cierto componente comercial y de mercadotecnia en la forma de comunicar sus avances. En 2019, el laboratorio de computación cuántica de Google anunció que había demostrado la supremacía cuántica con su procesador Sycamore, que incluye 53 qubits superconductores [A$^+$19]. La discusión sobre la relevancia real de este resultado, y sobre si era o no inalcanzable para algoritmos clásicos funcionando sobre las mejores computadoras del planeta, ha quedado rápidamente obsoleta tras la publicación de pruebas experimentales similares sobre procesadores superconductores o redes ópticas que tienen una mayor complejidad [W$^+$21, Z$^+$21]. A finales de 2021 IBM-quantum presentó en sociedad el primer procesador cuántico, también basado en qubits superconductores, que supera la barrera de 100 qubits [Bal21] que amplió a más de 400 en la versión presentada en noviembre de 2022.

Una vez superado este hito, la cuestión de la posible utilidad de estos primeros NISQS permanece. He mencionado antes la posibilidad de aplicarlos en tareas de optimización, relacionadas con estudios de mercados financieros o de análisis de datos, en la resolución de problemas de álgebra lineal o en la simulación de nuevos estados de la materia, entre otros, en ocasiones apoyados por algoritmos ejecutados sobre ordenadores convencionales. Sin embargo, todo esto depende de una precisa evaluación realista de su capacidad de cálculo. Y ésta no sólo depende de su tamaño, medido en núhmero de qubits. La decoherencia limita también, y de manera muy severa, el número de operaciones que podemos llevar a cabo con cada grupo de qubits. Este número da idea de la profundidad de los algoritmos que pueden ejecutarse antes de que la función de onda decaiga. Multiplicado por el tamaño del procesador, define lo que se ha venido en llamar el 'volumen cuántico' [CBS$^+$19]. En un procesador que, como en el caso de circuitos superconductores, se basa en conexiones entre vecinos próximos, los errores inherentes a la aplicación de cada puerta lógica imponen que sólo podamos operar con grupos de qubits suficientemente próximos entre sí, lo que reduce su potencial práctico. Encontrar formas de aumentar el 'volumen cuántico', por

ejemplo creando topologías con una mayor conectividad o mitigando errores, constituye el reto más importante que separa la carrera hacia procesadores de mayor tamaño de su explotación práctica en aspectos útiles para la sociedad.

4.4. Aproximaciones híbridas

Combinar diversos materiales para conseguir una cierta funcionalidad no es algo exclusivo de las tecnologías cuánticas. La idea de aprovechar lo mejor de cada uno de ellos se manifiesta en prácticamente todos los dispositivos o máquinas que manejamos a diario, incluyendo ordenadores convencionales y coches. El objetivo de las tecnologías cuánticas híbridas [KBK+15] es explotar qubits de naturaleza microscópica, que son inherentemente cuánticos y cuyos tiempos de coherencia pueden ser muy elevados, con herramientas 'prestadas' del ámbito de circuitos que permitan resolver el reto de 'cablear' estos qubits.

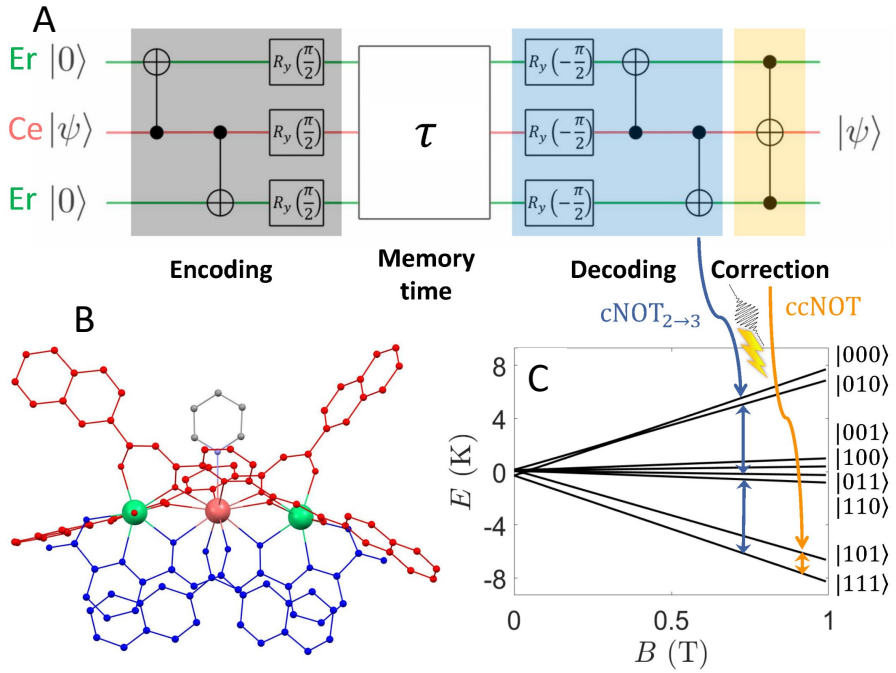

Figura 15: A) Circuito de un código de corrección de errores simplificado, pensado para ser implementado sobre tres qubits de espín diferentes. El qubit central (línea de evolución naranja) codifica la información, mientras los otros dos qubits auxiliares sirven para detectar y corregir errores. B) Molécula magnética que alberga tres iones de tierra rara en su 'core' magnético y que proporciona una posible realización experimental para este código. Los iones laterales (Er^{3+}) codifican los qubits auxiliares y el ion central (Ce^{3+}) codifica el qubit lógico en sus estados de espín electrónico. C) Esquema de niveles de energía magnética, que permite llevar a cabo cualquier operación con estos tres qubits y, por tanto, implementar el protocolo de corrección mediante la aplicación de secuencias de pulsos de microondas [MRA+20].

Existen propuestas para integrar átomos fríos [PBK+09] y espines [Ibu09] en arquitecturas de estado sólido, y usarlos como memorias cuánticas, es decir, como un soporte para almacenar estados cuánticos del procesador y protegerlos del ruido, o bien como elementos computacionales. En lo que sigue, me tomo la licencia de ilustrar el potencial de esta aproximación, así como sus retos, usando un ejemplo concreto, el de moléculas magnéticas, que me es cercano y que, al mismo tiempo, considero muy prometedor.

Un imán molecular consiste de un core magnético, formado por uno o varios iones de transición o tierras raras, que están rodeados por una cobertura de ligandos orgánicos [BLF14]. Estos sistemas guardan semejanzas con el caso de iones atrapados, con la diferencia de que la 'trampa' es aquí un material orgánico. Al igual que con los iones, los niveles de espín permiten codificar los estados de un qubit [AAL+12, GLHC19]. Pero el control sobre los ligandos ofrece un abanico muy superior de posibilidades de diseño. De hecho, una molécula es el objeto microscópico más pequeño que sigue siendo sintonizable. La estructura molecular y su composición permiten controlar las propiedades del qubit, como su frecuencia y los estados que definen la base computacional $|0\rangle$ y $|1\rangle$. Un objetivo obvio es reducir el efecto de la decoherencia, bien reduciendo las fuentes de ruido (como fluctuaciones de espines nucleares) o bien creando estados robustos frente a ellas. En el momento de escribir estas líneas, los tiempos de coherencia típicos de espines moleculares son del orden de $1 - 20\mu$s, mientras que en sistemas especialmente diseñados y 'limpios' se han alcanzado valores cercanos al ms [ZNPF15].

Sin embargo, el aspecto más interesante de este diseño químico es la posibilidad de escalar recursos al nivel de una sola molécula. Por ejemplo, el core magnético puede incluir varios iones débilmente acoplados entre sí, cada uno de los cuales puede codificar un qubit [LRM+11, ABV+14, MRA+20, LAR+20]. Otra opción es utilizar estados de espín internos de cada ion, como diferentes proyecciones de un espín $S > 1/2$ que pueden ser accesibles experimentalmente si la anisotropía magnética es suficientemente débil [JDD+17] o estados de espín nuclear en el caso de isótopos con $I \neq 0$ [GFB+17, GUR+21]. El último ejemplo supone una combinación de qubits de espín electrónico y nuclear en un único sistema físico, un átomo. Con respecto a espines nucleares en moléculas orgánicas, la interacción hiperfina aumenta la frecuencia de Rabi de las transiciones resonantes e introduce un desdoblamiento que hace posible inicializar el estado fundamental refrigerando a temperaturas del orden de 10 mK, accesibles a refrigeradores de dilución. Además, ofrece una vía para integrar espines nucleares en arquitecturas de estado sólido, por tanto contribuyendo a resolver las limitaciones más importantes de estos sistemas. Con un diseño

adecuado de las interacciones, que asegure que los niveles de espín no sean equidistantes, cada molécula codifica un qudit, generalización de un qubit a d dimensiones, o, en el caso en que $d = 2^n$, n qubits. Es decir, puede actuar como un procesador cuántico, o un NISQ, microscópico.

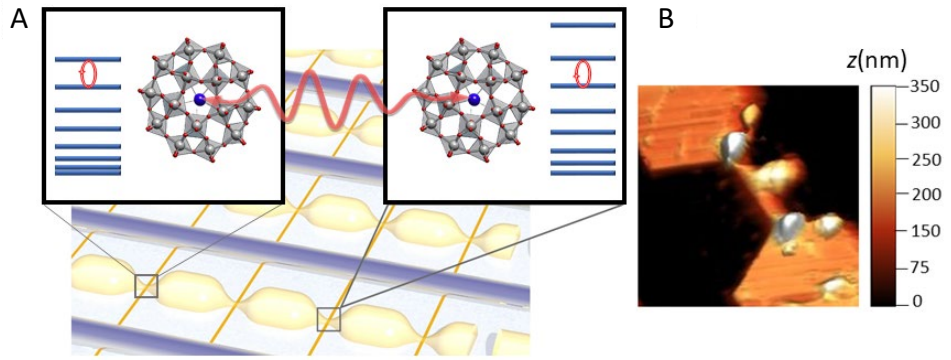

Figura 16: Izquierda: Imagen esquemática de un procesador cuántico híbrido basado en un resonador superconductor acoplado a moléculas magnéticas [JHM+13, JZR+16, CZC+21]. Cada molécula codifica un qudit (en la imagen de dimensión $d = 8$) equivalente a tres qubits y capaz de implementar corrección de errores. El circuito permite controlar los estados del qudit, leer el resultado y establecer interacciones efectivas que permiten llevar a cabo puertas lógicas condicionales. Derecha: Imagen de microscopía de fuerzas magnéticas de la línea central de un resonador superconductor en chip, sobre la que se han colocado nanodepósitos de radicales libres DPPH que actúan como qubits [GKP+20].

Utilizar qudits como unidades básicas puede tener importantes ventajas en computación cuántica. Los recursos extra que proporcionan los múltiples niveles permiten simplificar ciertas computaciones: la dimensión d del procesador aumenta más lentamente con el tamaño del problema a resolver que en el caso de operar con qubits. Además, puede facilitar la implementación práctica ya que, al operar con un único sistema físico, se reduce el número de operaciones no locales, por ejemplo puertas lógicas condicionales de dos qubits que son más costosas, en especial entre qubits distantes, y más proclives a error. Este aspecto permite aumentar la profundidad computacional y, por tanto, el volumen cuántico alcanzable con una dimensión dada. Una aplicación especialmente atractiva es la posibilidad de integrar la corrección de errores en cada unidad repetitiva. Es posible implementar un código de corrección de errores convencional en moléculas que alberguen al menos tres qubits [MRA+20] o, mejor aún, usar códigos diseñados específicamente para qudits [CMP+20]. Estos códigos aprovechan los niveles extra para conseguir la redundancia necesaria para proteger la información.

La perspectiva de construir un procesador cuántico usando 'ladrillos' microscópicos que codifiquen qubits resistentes al ruido puede suponer una ventaja notable para alcanzar el sueño de la computación cuántica a gran escala. La cuestión es cómo fabricarlo,

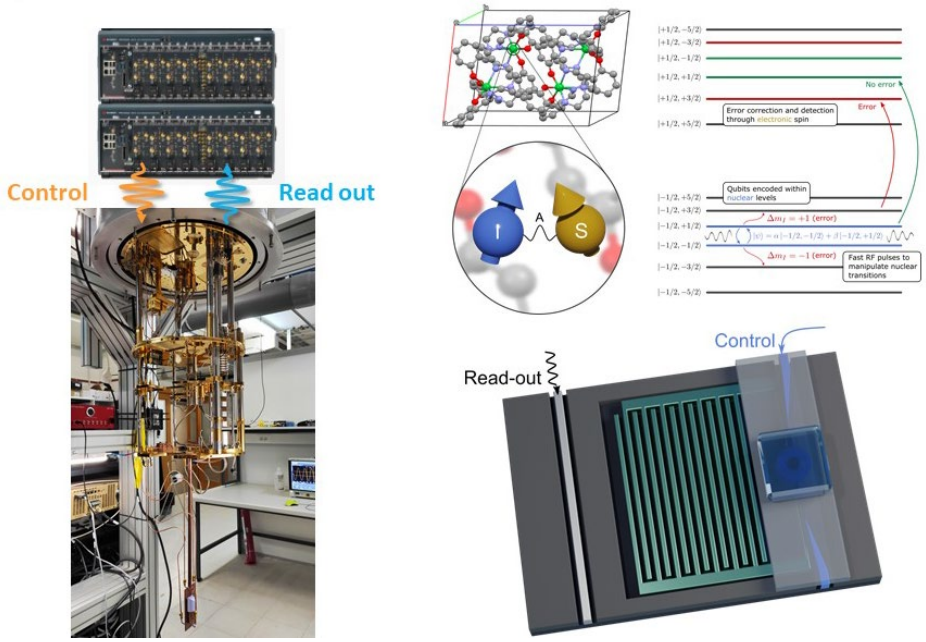

Figura 17: Procesador cuántico híbrido que se está desarrollando en el INMA. Izquierda: imagen del refrigerador de dilución que mantiene el chip a una temperatura de 8 mK sobre el cero absoluto y que alberga las líneas de control y lectura. Se muestra también la electrónica de microondas externa. Derecha, arriba: Estructura molecular y niveles de espín de la molécula Yb-trensal, que puede codificar un qudit de dimensión $d = 12$ con sus espines nuclear y electrónico. Cristales de estas moléculas, y de otras similares, permiten implementar diversos algoritmos cuánticos a pequeña escala (equivalente a 4 qubits) con la ventaja de evitar la necesidad de utilizar puertas no locales. Derecha, abajo: imagen artística de la unidad cuántica QPU de este procesador, que consiste de un cristal molecular acoplado a una línea de control y a un resonador superconductor, que a su vez se lee a través de una línea adicional.

es decir, encontrar la tecnología para controlar, leer y, sobre todo, cablear entre sí estas unidades básicas. El espíritu de una tecnología híbrida supone buscar soluciones desarrolladas en otros ámbitos y adaptarlas a esta situación. Una idea es combinar qudits de espín con circuitos superconductores [JHM+13, JZR+16, CZC+21]. Los momentos magnéticos asociados a los qubits de espín se acoplan al campo magnético de una cavidad. Es, por tanto, posible aplicar líneas y resonadores superconductores para controlar y leer los estados de espín de cada qudit, así como para introducir interacciones efectivas entre dos de ellos, con tal de que estén sintonizados entre sí. El reto es, sin embargo, considerable ya que la energía de acoplo de una molécula magnética a un fotón de micro-ondas es órdenes de magnitud inferior al de un trasmón, por ejemplo. Sin embargo, existen formas de intensificar el campo magnético generado por el circuito, usando resonadores con diseños específicos complementados con técnicas de nanofabricación para confinar este campo en regiones de tamaño comparable al de las moléculas [GKP+20]. Además, estos desarrollos prometen llevar la resonancia magnética a una nueva escala de sensibilidad, inalcanzable para los equipos comerciales. Para concluir este apartado, quiero mencionar que mi centro

de investigación, el INMA, y el CSIC están apostando por esta idea, que podría contribuir a que nuestro país tenga una tecnología propia en este ámbito. Aunque conseguir un procesador universal queda todavía lejos y requerirá solventar dificultades considerables, esperamos que sea posible llevar a cabo pruebas de concepto a pequeña escala en un plazo relativamente breve, de 1 a 2 años.

5. A modo de conclusión

Se puede discutir si el renovado interés por el estudio y control de fenómenos cuánticos en diversos sistemas físicos constituye una revolución comparable al propio desarrollo de la teoría cuántica hace más de un siglo. Para mí, resulta evidente que ha generado un campo de investigación apasionante, que seguramente traerá consigo oportunidades para desarrollar tecnologías disruptivas. Incluso si el objetivo final de construir un ordenador cuántico de propósito general toma más tiempo del prometido en algunos foros, algo que considero probable, sus consecuencias se harán sentir pronto en ámbitos como las comunicaciones y transacciones seguras y en novedosa instrumentación física, que siempre ha tenido un impacto notable en diversas áreas, especialmente la medicina. Además, nos ofrece una oportunidad única de explorar nuevos estados de la materia con un control exquisito. Al fin y al cabo, la mejor inversión es, y ha sido siempre, fomentar la curiosidad y la exploración de la naturaleza, sin necesariamente conocer los resultados. O, parafraseando de nuevo otra frase del artículo *There's plenty of room at the bottom*, mi favorita: aunque podamos citar motivaciones prácticas lo que realmente nos mueve es hacer algo intelectualmente interesante y divertido[2].

Agradecimientos

Quiero empezar agradeciendo el apoyo que siempre he recibido de mi familia. Mis padres pusieron la educación de sus hijos por encima de otras prioridades. Mi mujer, Josefina, es la mejor compañera que hubiera podido soñar y, además, ha compensado casi sin quejarse el tiempo de conciliación familiar que me ha robado la física. Y mis hijos, Isabel y Pablo, dan sentido a cada día. Gracias.

[2] Adaptación libre del original: *Why should we do it? Well I pointed out a few of the economic applications, but I know that the reason you would do it might be just for fun.*

La investigación que he desarrollado ha sido posible gracias al trabajo conjunto de muchos investigadores. Es un placer haber colaborado en estos temas, en ocasiones durante muchos años, con personas que han hecho que el trabajo sea, además de productivo, mucho más agradable. Muchas gracias, por ello, a Pablo Alonso, Ana Arauzo, Fernando Bartolomé, Nico Camón, Javier Campo, Chiara Carbonera, Jesús Chaboy, Marco Evangelisti, José Luis García Palacios, Luis Miguel García, Carlos Gómez-Moreno, Anabel Gracia Lostao, Jesús Martínez, Ángel Millán, Óscar Montero, Eva Natividad, Fernando Palacio, Mari Carmen Pallarés, Víctor Rollano, Juan Román, Olivier Roubeau, Javier Rubín, Carlos Sánchez Azqueta, Javier Sesé, Jolanta Stankiewicz, Ainhoa Urtizberea y David Zueco. También quiero acordarme de todos los miembros del grupo de investigación QMAD por crear un ambiente motivador, agradable y casi familiar, para el trabajo diario.

Por último, tampoco puedo olvidar las colaboraciones con investigadores como David Aguilà, Andreas Angerer, Guillem Aromí, Rafik Ballou, Bernard Barbara, Leoní Barrios, Lapo Bogani, Marina Calero, Salvador Cardona, Stefano Carretta, Alessandro Chiesa, Miguel Clemente, Andrea Cornia, George Christou, Eugenio Coronado, Enrique del Barco, Neus Domingo, Dietmar Drung, Alex Gaita, Juanjo García Ripoll, Dante Gatteschi, Rocco Gaudenzi, Alicia Gómez, Álvaro Gómez León, Violeta González, Joan Manel Hernández, Michael Kroll, Hannes Majer, Talal Mallah, Garry McIntyre, Satoru Maegawa, Andrea Morello, Peter Paulus, Fréderic Petroff, Daniel Ruiz Molina, Eliseo Ruiz, Thomas Schurig, Roberta Sessoli, Joris van Slageren, Tibi Sorop, Carlos Untiedt, Jaume Veciana, Richard Winpenny y Xixiang Zhang.

Bibliografía

[A+19] F. Arute et al., *Quantum supremacy using a programmable superconducting processor*, Nature **574** (2019), 505–510.

[AAL+12] G. Aromí, D. Aguilà, F. Luis, S. Hill, and E. Coronado, *Design of magnetic coordination complexes for quantum computing.*, Chem. Soc. Rev. **41** (2012), 537–546.

[ABB+18] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S.J. Glaser, F. Jelezko, S. Kuhr, M. Lewenstein, M.F. Riedel, P.O. Schmidt, R. Thew, A. Wallraff, I. Walmsley, and F.K. Wilhelm, *The quantum technologies roadmap: a european community view*, New Journal of Physics **20** (2018), no. 8, 080201.

[ABD+13] D.D. Awschalom, L.C. Bassett, A.S. Dzurak, E.L. Hu, and J.R. Petta, *Quantum spintronics: Engineering and manipulating atom-like spins in semiconductors*, Science **339** (2013), no. 6124, 1174–1179.

[ABV+14] D. Aguilà, D. Barrios, V. Velasco, O. Roubeau, A. Repollés, P.J. Alonso, J. Sesé, S.J. Teat, F. Luis, and G. Aromí, *Heterodimetallic [LnLn'] lanthanide complexes: Toward a chemical design of two-qubit molecular spin quantum gates*, J. Am. Chem. Soc. **136** (2014), 14215.

[AL18] T. Albash and D.A. Lidar, *Adiabatic quantum computation*, Rev. Mod. Phys. **90** (2018), 015002.

[APN+17] N. Aslam, M. Pfender, P. Neumann, R. Reuter, A. Zappe, F. Fávaro de Oliveira, A. Denisenko, H. Sumiya, S. Onoda, J. Isoya, and J. Wrachtrup, *Nanoscale nuclear magnetic resonance with chemical resolution*, Science **357** (2017), no. 6346, 67–71.

[Bal21] P. Ball, *First quantum computer to pack 100 qubits enters crowded race*, Nature **599** (2021), 542.

[BB84] C.H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **175** (1984), 8.

[BBB+92] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Entanglement-based secure quantum cryptography over 1120 kilometres*, J. Cryptol. **5** (1992), 3–28.

[BBC+95] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P.W. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, *Elementary gates for quantum computation*, Phys. Rev. A **52** (1995), 3457–3467.

[BHW+04] A. Blais, R.-S. Huang, A. Wallraff, S.M. Girvin, and R.J. Schoelkopf, *Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation*, Phys. Rev. A **69** (2004), 062320.

[BK98] S.B. Bravyi and A.Y. Kitaev, *Quantum codes on a lattice with boundary*, 1998.

[BLF14] J. Bartolomé, F. Luis, and J.F. Fernández (eds.), *Molecular magnets: Physics and applications*, Springer Verlag, 2014.

[BLM+20] S.L. Bayliss, D.W. Laorenza, P.J. Mintun, B.D. Kovos, D.E. Freedman, and D.D. Awschalom, *Optically addressable molecular spins for quantum information processing*, Science **370** (2020), no. 6522, 1309–1312.

[BM06] H. Bombin and M.A. Martín-Delgado, *Topological quantum distillation*, Phys. Rev. Lett. **97** (2006), 180501.

[BRI+14] S. Boixo, T.F. Rønnow, S.V. Isakov, Z. Wang, D. Wecker, D.A. Lidar, J.M. Martinis, and M. Troyer, *Evidence for quantum annealing with more than one hundred qubits*, Nature Phys. **10** (2014), 218–224.

[C+21] Y. Chen et al., *An integrated space-to-ground quantum communication network over 4600 kilometres*, Nature **589** (2021), 214–219.

[CBS+19] A.W. Cross, L.S. Bishop, S. Sheldon, P.D. Nation, and J.M. Gambetta, *Validating quantum computers using randomized model circuits*, Phys. Rev. A **100** (2019), 032328.

[CMP+20] A. Chiesa, E. Macaluso, F. Petiziol, S. Wimberger, P. Santini, and S. Carretta, *Molecular nanomagnets as qubits with embedded quantum-error correction*, The Journal of Physical Chemistry Letters **11** (2020), no. 20, 8610–8615.

[CVZ+98] I.L. Chuang, L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd, *Experimental realization of a quantum algorithm*, Nature **393** (1998), 143–146.

[CW08] J. Clarke and F.K. Wilhem, *Superconducting quantum bits*, Nature **453** (2008), 1031.

[CZ95] J.I. Cirac and P. Zoller, *Quantum computations with cold trapped ions*, Phys. Rev. Lett. **74** (1995), 4091–4094.

[CZ12] ———, *Goals and opportunities in quantum simulation*, Nature Phys. **8** (2012), 264–266.

[CZC+21] S. Carretta, D. Zueco, A. Chiesa, Á. Gómez-León, and F. Luis, *A perspective on scaling up quantum computation with molecular spins*, Applied Physics Letters **118** (2021), no. 24, 240501.

[DBI+16] V.S. Denchev, S. Boixo, S.V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. Martinis, and H. Neven, *What is the computational value of finite-range tunneling?*, Phys. Rev. X **6** (2016), 031015.

[Deu20] I.H. Deutsch, *Harnessing the power of the second quantum revolution*, PRX Quantum **1** (2020), 020101.

[DiV00] D.P. DiVincenzo, *The physical implementation of quantum computation*, Fortschritte der Physik **48** (2000), no. 9-11, 771–783.

[DMD+13] M.W. Doherty, N.B. Manson, P. Delanay, F. Jelezko, J. Wrachtrup, and L.C.L Hollenberg, *The nitrogen-vacancy colour centre in diamond*, Physics Reports **528** (2013), no. 1, 1–45, The nitrogen-vacancy colour centre in diamond.

[DP85] D.E. Deutsch and R. Penrose, *Quantum theory, the Church–Turing principle and the universal quantum computer*, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences **400** (1985), no. 1818, 97–117.

[DRC17] C.L. Degen, F. Reinhard, and P. Cappellaro, *Quantum sensing*, Rev. Mod. Phys. **89** (2017), 035002.

[DS13] M.H. Devoret and R.J. Schoelkopf, *Superconducting circuits for quantum information: An outlook*, Science **339** (2013), no. 6124, 1169–1174.

[Eke91] A.K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67** (1991), 661–663.

[Fey82] R. Feynman, *Simulating physics with computers*, Int. J. Theor. Phys. **21** (1982), 467–488.

[Fey92] ———, *There's plenty of room at the bottom*, J. Microelectromechanical Systems **1** (1992), 60.

[FGG14] E. Farhi, J. Goldstone, and S. Gutmann, *A quantum approximate optimization algorithm*, 2014.

[FMMC12] A.G. Fowler, M. Mariantoni, J.M. Martinis, and A.N. Cleland, *Surface codes: Towards practical large-scale quantum computation*, Phys. Rev. A **86** (2012), 032324.

[GB17] C. Gross and I. Bloch, *Quantum simulations with ultracold atoms in optical lattices*, Science **357** (2017), no. 6355, 995–1001.

[GDT+97] A. Gruber, A. Dräbenstedt, C. Tietz, L. Fleury, J. Wrachtrup, and C. von Borczyskowski, *Scanning confocal optical microscopy and magnetic resonance on single defect centers*, Science **276** (1997), no. 5321, 2012–2014.

[GFB+17] C. Godfrin, A. Ferhat, R. Ballou, S. Klyatskaya, M. Rubén, W. Wernsdorfer, and F. Balestro, *Operating quantum states in single magnetic molecules: Implementation of Grover's quantum algorithm*, Phys. Rev. Lett. **119** (2017), 187702.

[Gib14] E. Gibney, *Physics: Quantum computer quest*, Nature **516** (2014), 24–26.

[GKP+20] I. Gimeno, W. Kersten, M.C. Pallarés, P. Hermosilla, M.J. Martínez-Pérez, M.D. Jenkins, A. Angerer, C. Sánchez-Azqueta, D. Zueco, J. Majer, A.I. Lostao, and F. Luis, *Enhanced Molecular Spin-Photon Coupling at Superconducting Nanoconstrictions*, ACS Nano **14** (2020), 8707—-8715.

[GLHC19] A. Gaita-Ariño, F. Luis, S. Hill, and E. Coronado, *Molecular spins for quantum computation.*, Nature Chem. **11** (2019), 301–309.

[Gro97] L.K. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Phys. Rev. Lett. **79** (1997), 325–328.

[GUR+21] I. Gimeno, A. Urtizberea, J. Román-Roche, D. Zueco, A. Camón, P.J. Alonso, O. Roubeau, and F. Luis, *Broad-band spectroscopy of a vanadyl porphyrin: a model electronuclear spin qudit*, Chem. Sci. (2021), –.

[Hei27] W. Heisenberg, *Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik*, Z. Phys. **43** (1927), 172.

[HHL09] A.W. Harrow, A. Hassidim, and S. Lloyd, *Quantum algorithm for linear systems of equations*, Phys. Rev. Lett. **103** (2009), 150502.

[HLR+21] N.W. Hendrickx, W.I.L. Lawrie, M. Russ, F. van Riggelen, S.L. de Snoo, R.N. Schouten, A. Sammak, G. Scappucci, and M. Veldhorst, *A four-qubit germanium quantum processor*, Nature **591** (2021), 580—-585.

[Ibu09] A. Imamoğlu, *Cavity qed based on collective magnetic dipole coupling: Spin ensembles as hybrid two-level systems*, Phys. Rev. Lett. **102** (2009), 083602.

[JDD+17] M.D. Jenkins, Y. Duan, B. Diosdado, J.J. García-Ripoll, A. Gaita-Ariño, C. Giménez-Saiz, P.J. Alonso, E. Coronado, and F. Luis, *Coherent manipulation of three-qubit states in a molecular single-ion magnet*, Phys. Rev. B **95** (2017), 064423.

[JGP+04] F. Jelezko, T. Gaebel, I. Popa, A. Gruber, and J. Wrachtrup, *Observation of coherent oscillations in a single electron spin*, Phys. Rev. Lett. **92** (2004), 076401.

[JHM+13] M.D. Jenkins, T. Hümmer, M.J. Martínez-Pérez, J.J. García-Ripoll, D. Zueco, and F. Luis, *Coupling single-molecule magnets to quantum circuits*, New J. Phys. **15** (2013), 095007.

[JZR+16] M.D. Jenkins, D. Zueco, O. Roubeau, G. Aromí, J. Majer, and F. Luis, *A scalable architecture for quantum computation with molecular nanomagnets.*, Dalton Trans. **45** (2016), 16682.

[Kan98] B.E. Kane, *A silicon-based nuclear spin quantum computer*, Nature **393** (1998), 133–137.

[KBK+15] G. Kurizki, P. Bertet, Y. Kubo, K. Mølmer, D. Petrosyan, P. Rabl, and J. Schmiedmayer, *Quantum technologies with hybrid systems*, Proceedings of the National Academy of Sciences **112** (2015), no. 13, 3866–3873.

[KLZ98] E. Knill, R. Laflamme, and W.H. Zurek, *Resilient quantum computation*, Science **279** (1998), no. 5349, 342–345.

[KP16] I. Kerenidis and A. Prakash, *Quantum recommendation systems*, 2016.

[KYG+07] J. Koch, T.M. Yu, J. Gambetta, A.A. Houck, D.I. Schuster, J. Majer, A. Blais, M.H. Devoret, S.M. Girvin, and R.J. Schoelkopf, *Charge-insensitive qubit design derived from the cooper pair box*, Phys. Rev. A **76** (2007), 042319.

[LAR+20] F. Luis, P.J. Alonso, O. Roubeau, V. Velasco, D. Zueco, D. Aguilà, J.I. Martínez, L.A. Barrios, and G. Aromí, *A dissymmetric Gd_2 coordination molecular dimer hosting six addressable spin qubits*, Communications Chemistry **3** (2020), 176.

[LBR17] A.P. Lund, M.J. Bremner, and T.C. Ralph, *Quantum sampling problems, boson sampling and quantum supremacy*, npj Quantum Inf. **3** (2017), 15.

[LRM+11] F. Luis, A. Repollés, M.J. Martínez-Pérez, D. Aguilà, O. Roubeau, D. Zueco, P.J. Alonso, M. Evangelisti, A. Camón, J. Sesé, L.A. Barrios, and G. Aromí, *Molecular prototypes for spin-based cnot and swap quantum gates.*, Phys. Rev. Lett. **107** (2011), 117203.

[M+07] J. Majer et al., *Coupling superconducting qubits via a cavity bus*, Nature **449** (2007), 443–447.

[M+10] A. Morello et al., *Single-shot readout of an electron spin in silicon*, Nature **467** (2010), 687–691.

[M+22a] M.T. Madzik et al., *Precision tomography of a three-qubit donor quantum processor in silicon*, Nature **601** (2022), 348–353.

[M+22b] X. Mi et al., *Time-crystalline eigenstate order on a quantum processor*, Nature **601** (2022), 531–536.

[MDL+14] J.T. Muhonen, J.P. Dehollain, A. Laucht, F.E. Hudson, R. Kalra, T. Sekiguchi, K.M. Itoh, D.N. Jamieson, J.C. McCallum, A.S. Dzurak, and A. Morello, *Storing quantum information for 30 seconds in a nanoelectronic device*, Nature Nanotech. **9** (2014), 986–991.

[MK13] C. Monroe and J. Kim, *Scaling the ion trap quantum processor*, Science **339** (2013), no. 6124, 1164–1169.

[MRA+20] E. Macaluso, M. Rubín-Osanz, D. Aguilà, A. Chiesa, L.A. Barrios, J.I. Martínez, P.J. Alonso, O. Roubeau, F. Luis, G. Aromí, and S. Carretta, *A heterometallic [LnLn'Ln] lanthanide complex as a qubit with embedded quantum error correction*, Chem. Sci. **11** (2020), 10337.

[MRN+17] M. Mohseni, P. Read, H. Neven, S. Boixo, V. Denchev, R. Babbush, A.G. Fowler, V. Smelyanskiy, and J. Martinis, *Commercialize quantum technologies in five years*, Nature **543** (2017), 171–175.

[NMM+14] D. Nigg, M. Müller, E.A. Martínez, P. Schindler, M. Hennrich, T. Monz, M.A. Martín-Delgado, and R. Blatt, *Quantum computations on a topologically encoded qubit*, Science **345** (2014), no. 6194, 302–305.

[PBK+09] D. Petrosyan, G. Bensky, G. Kurizki, I. Mazets, J. Majer, and J. Schmiedmayer, *Reversible state transfer between superconducting qubits and atomic ensembles*, Phys. Rev. A **79** (2009), 040304.

[Pre18] J. Preskill, *Quantum computing in the nisq era and beyond*, Quantum **2** (2018), 79.

[PTD+12] J.J. Pla, K.Y. Tan, J.P. Dehollain, W.H. Lim, J.J.L. Morton, D.N. Jamieson, A.S. Dzurak, and A. Morello, *A single-atom electron spin qubit in silicon*, Nature **489** (2012), 541–545.

[PZY+07] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, *Experimental long-distance decoy-state quantum key distribution based on polarization encoding*, Phys. Rev. Lett. **98** (2007), 010505.

[Rab37] I.I. Rabi, *Space quantization in a gyrating magnetic field*, Phys. Rev. **51** (1937), 652–654.

[RHR+07] D. Rosenberg, J.W. Harrington, P.R. Rice, P.A. Hiskett, C.G. Peterson, R.J. Hughes, A.E. Lita, S.W. Nam, and J.E. Nordholt, *Long-distance decoy-state quantum key distribution in optical fiber*, Phys. Rev. Lett. **98** (2007), 010503.

[RLZ21] J. Román-Roche, F. Luis, and D. Zueco, *Photon condensation and enhanced magnetism in cavity qed*, Phys. Rev. Lett. **127** (2021), 167201.

[RSA78] R. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126.

[SG08] R.J. Schoelkopf and S.M. Girvin, *Wiring up quantum systems*, Nature **451** (2008), 664–669.

[Sho94] P.W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science (1994), 124–134.

[Sho95] ———, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A **52** (1995), R2493–R2496.

[Ste96] A.M. Steane, *Error correcting codes in quantum theory*, Phys. Rev. Lett. **77** (1996), 793–797.

[Ter15] B.M. Terhal, *Quantum error correction for quantum memories*, Rev. Mod. Phys. **87** (2015), 307–346.

[Tur37] A.M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society **s2-42** (1937), no. 1, 230–265.

[VC05] L.M.K. Vandersypen and I.L. Chuang, *NMR techniques for quantum control and computation*, Rev. Mod. Phys. **76** (2005), 1037–1069.

[VSB+01] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, *Experimental realization of a quantum algorithm*, Nature **414** (2001), 883–887.

[W+21] Y. Wu et al., *Strong quantum computational advantage using a superconducting quantum processor*, Phys. Rev. Lett. **127** (2021), 180501.

[WHW+15] D. Wecker, M.B. Hastings, N. Wiebe, B.K. Clark, C. Nayak, and M. Troyer, *Solving strongly correlated electron models on a quantum computer*, Phys. Rev. A **92** (2015), 062318.

[WSB+04] A. Wallraff, D.I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S.M. Girvin, and R.J. Schoelkopf, *Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics*, Nature **431** (2004), no. 7005, 162–167.

[WZ83] J.A. Wheeler and W.H. Zurek (eds.), *Quantum theory and measurement*, Princeton University Press, Princeton, New Jersey, 1983.

[WZ09] W.K. Wootters and W.H. Zurek, *The no-cloning theorem*, Physics Today **62** (2009), no. 2, 76–77.

[XMZ+20] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Secure quantum key distribution with realistic devices*, Rev. Mod. Phys. **92** (2020), 025002.

[Y+20] J. Yin et al., *Entanglement-based secure quantum cryptography over 1120 kilometres*, Nature **582** (2020), 501–505.

[YCY+16] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M.J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, *Measurement-device-independent quantum key distribution over a 404 km optical fiber*, Phys. Rev. Lett. **117** (2016), 190501.

[Z+21] H. Zhong et al., *Phase-programmable gaussian boson sampling using stimulated squeezed light*, Phys. Rev. Lett. **127** (2021), 180502.

[ZNPF15] J.M. Zadrozny, J. Niklas, O.G. Poluektov, and D.E. Freedman, *Millisecond coherence time in a tunable molecular electronic spin qubit.*, ACS Cent. Sci. **1** (2015), 488.

[Zur03] W.H. Zurek, *Decoherence, einselection, and the quantum origins of the classical*, Rev. Mod. Phys. **75** (2003), 715–775.