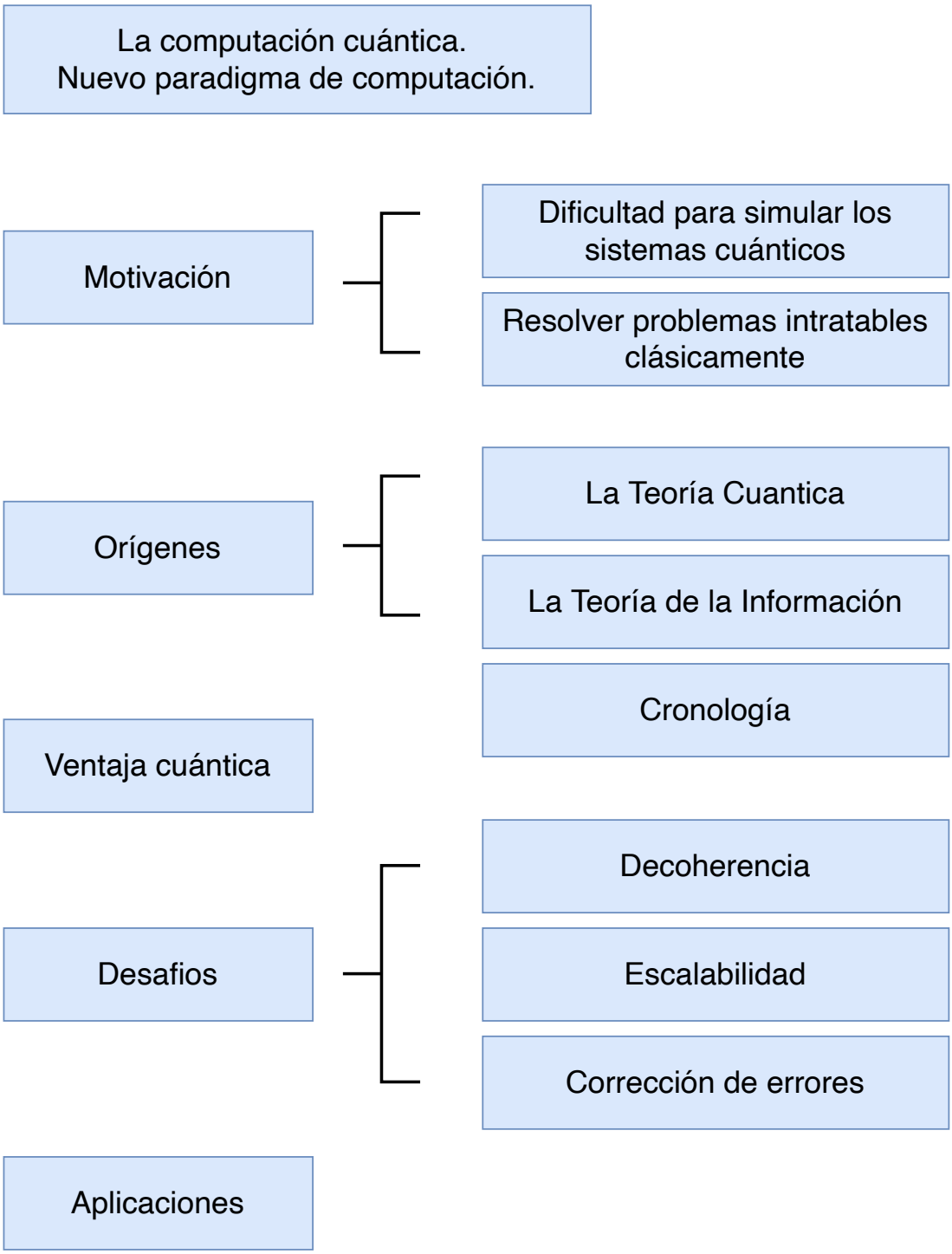
Computación Cuántica

Introducción a la Computación Cuántica

Índice

Esquema


La computación cuántica.
Nuevo paradigma de computación.
Motivación
Dificultad para simular los sistemas cuánticos
Resolver problemas intratables clásicamente
Orígenes
La Teoría Cuantica
La Teoría de la Información
Cronología
Ventaja cuántica
Desafios
Decoherencia
Escalabilidad
Corrección de errores
Aplicaciones

Ideas clave

1.1 Introducción y objetivos

A principios de los ochenta el físico Richard Feynman publicó un artículo científico en la Revista Internacional de Física Teórica titulado *Simulando la Física con computadores.*

Este artículo, lo presento en 1982 en lo que podría definirse hoy como la primera conferencia sobre Computación Cuántica de la historia. El título de la conferencia fue *La Física de la Computación*, ya que, en aquel momento, el término *Computación Cuántica* todavía no había sido acuñado.

En su artículo, Feynman proponía un dispositivo cuántico para la simulación de los fenómenos naturales. Su repercusión ha sido de tal importancia que el número de veces que este artículo es referenciado es mayor que el de su trabajo sobre electrodinámica cuántica (QED), por el cual recibió el Premio Nobel de Física. La razón de ello es que esa publicación se considera fundacional para el campo de la Computación Cuántica y en ella se describe como un sistema cuántico controlable puede utilizarse para simular otro sistema cuántico proporcionando una ventaja sobre la computación clásica. De forma simplificada, Feynman tuvo la intuición de entender que dado un sistema cuántico que se desea simular, como por ejemplo una molécula, se puede utilizar otro sistema cuántico distinto pero controlable y que sigue la misma dinámica que el primero, de tal forma que los observables de uno y otro son equivalentes. Es decir, proponía construir un sistema cuántico artificial y controlable para simular la Naturaleza.

Si bien es posible simular un sistema de n partículas utilizando un procesador clásico, Feynman observó que el problema crecía exponencialmente en tiempo y recursos, era muy ineficiente. Puesto que las partículas podían «simularse» a sí mismas de forma eficiente, con un cambio de perspectiva, pensó, que podría considerarse que las propias partículas eran el procesador, computando bajo las leyes de la física pero de forma exponencialmente más eficiente que la de un procesador clásico. Extendiendo

este razonamiento, propuso construir sistemas de múltiples partículas de forma que su comportamiento natural pudiera realizar otros cómputos interesantes para nosotros de forma eficiente. El concepto de un computador cuántico estaba en marcha, había nacido un nuevo paradigma de computación y una nueva rama de la Ciencia: La Computación Cuántica.

La computación clásica o computación binaria es una herramienta extraordinaria que ha transformado nuestro mundo y acelerado el progreso de forma incuestionable, sin embargo no puede resolver todos los problemas a los que nos enfrentamos, de hecho puede resolver muy pocos. Cuando abordamos problemas exponenciales las maquinas binarias de computación exacta que tanta ayuda nos proporcionan y tan bien hacen su trabajo, dejan de ser útiles pues exigen una enorme demanda computacional y necesitamos un paradigma diferente de computación, necesitamos un modelo de computación exponencial, ese otro paradigma de computación es la computación cuántica, basada, no en el bit, sino en otra unidad de información, el cúbit, que utiliza el estado de un sistema cuántico para almacenar información y las leyes de la Mecánica Cuántica para procesarla.

Para conseguir ese extraordinario potencial que promete, la computación cuántica hace uso de la superposición de estados que permite manipular múltiples estados del registro cuántico de forma simultánea, a diferencia del tratamiento secuencial impuesto por el modelo de la computación clásica.

Así, si una máquina clásica de dos bits puede estar en uno de las cuatro posibles estados en cada momento, una máquina cuántica, maneja los cuatro estados simultáneamente, ese paralelismo cuántico lo aprovechamos para computar. Pero la superposición no es la única herramienta que ofrece el nuevo modelo, otro efecto cuántico, el entrelazamiento, es igualmente importante pues nos permite relacionar el estado de los cubits o la interferencia con la que conseguimos cancelar las soluciones incorrectas y así obtener la solución al problema que queremos resolver.

El objetivo de esta asignatura es presentar este nuevo paradigma de computación, sus fundamentos y sus aplicaciones.

Los objetivos de este primer tema de la asignatura son los siguientes:

- La motivación que ha llevado al desarrollo de esta disciplina.
- Los orígenes de la computación cuántica.
- La ventaja que proporciona la computación cuántica frente a la computación clásica.
- Cuales son las principales aplicaciones de la computación cuántica.
- Los desafíos a los que se enfrenta el desarrollo de la computación cuántica.

1.2 Motivación

El origen de toda motivación es siempre una necesidad, en el caso de la computación cuántica, esa necesidad fue la de abordar uno de los aspectos más complicados a los que se ha enfrentado la Física, la Teoría Cuántica mostraba un mundo de tal complejidad que incluso modelar los sistemas más simples, formados por un pequeño número de partículas, quedaba fuera de nuestro alcance, y ello debido a que es necesaria una capacidad de computación que crece exponencialmente tanto en tiempo como en recursos a medida que el problema aumenta.

Para entender la magnitud del problema, una sistema cuántico formado por apenas 25 partículas requiere tal volumen de información para describir su estado que es mayor que el numero de átomos de La Tierra, lo cual, evidentemente, es imposible de almacenar en ningún ordenador. Además, añadir una partícula al sistema supone duplicar la memoria necesaria.

Para describir el estado de un sistema de 300 partículas sería necesaria toda la materia del Universo. Es, por consiguiente, evidente, que la computación clásica nunca podrá simular un sistema cuántico no trivial. Pero sin embargo, la Naturaleza resuelve el problema con extraordinaria eficiencia en tiempo real pues todo lo que nos rodea está gobernado por las leyes de la Mecánica Cuántica.

La dificultad de este problema de la simulación de los sistemas cuánticos en contraste

con el comportamiento natural hizo pensar a los pioneros de la computación cuántica sobre la oportunidad que nos ofrece la naturaleza de aprovechar sus propias reglas para crear un dispositivo que utilice la mecánica cuántica como base de los operadores para el procesamiento de la información, es decir, la computación. Si esto fuera posible, no solo podríamos simular los sistemas naturales sino, extendiendo sus capacidades, aplicarlo a resolver otros problemas de cualquier tipo. Este enfoque terminó finalmente en el nacimiento de la computación cuántica.

1.3 Orígenes

A finales del siglo XIX la idea general en el mundo de la Física era que se conocían las leyes que gobiernan la Naturaleza y que tan solo quedaba mejorar la precisión de los resultados. Sin embargo, algunos fenómenos físicos relativos a la interacción entre la materia y la radiación electromagnética no podían ser explicados aplicando las ecuaciones de las teorías existentes. Uno de estos fenómenos era la radiación del cuerpo negro. El físico Max Plank trabajaba en este problema pues el modelo matemático no permitía predecir el color, es decir la longitud de onda, de la emisión de un cuerpo en función de su temperatura. Solo cuando Plank introduce un concepto revolucionario, las predicciones funcionan: la energía emitida no es continua sino que está formada por paquetes de energía indivisibles, los cuantos. Había nacido una nueva rama de la Física, la Mecánica Cuántica.

Durante los años 70, Paul Benioff, investigó sobre la factibilidad teórica de la computación cuántica y en 1980 publicó un artículo ("The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines", Paul Benioff, Journal of Statistical Physics, 22, 563, 1980), donde describía una versión cuántica del modelo de la Maquina de Turing. La base de este trabajo de investigación, a su vez, fueron los estudios que otro físico, Charles Bennet, hizo en 1973 sobre las máquinas de Turing reversibles pues el modelo de computador cuántico de Benioff era reversible y no disipaba energía. Fue, por tanto, Benioff, el primero en mostrar que la computación cuántica reversible era, teóricamente posible

despejando así el camino hacia la posibilidad de una computación cuántica general. Este trabajo, seguido por el de otros como Richard Feynman, que propuso un simulador cuántico universal, David Deutsch, que demuestra como la Mecánica Cuántica permite un nuevo paradigma de computación que puede ser utilizada para resolver problemas de forma más rápida a la que puede hacerlo un computador clásicos y describe la primera Máquina Universal de Turing Cuántica, una extensión del principio de Church-Turing.

En la década de los 80, dos de las teorías mas revolucionarias e influyentes del siglo, la Mecánica Cuántica y la Teoría de la Información se combinaron para dar lugar a un nuevo paradigma de la computación y de la información. Esta visión proporcionó una perspectiva completamente nueva de la forma en la que la Física, la Información y la Computación se relacionan, inspirando novedosas aplicaciones en comunicaciones y computación.

A mediados de los años 80 el físico David Deutsch observo que la Maquina Universal de Turing no era en realidad universal pues ciertos problemas, ciertos fenómenos cuánticos asociados al entrelazamiento de partículas, que presentan un crecimiento exponencial en tiempo y recursos necesarios para ser computados no podría, en la práctica, simularlos. Faynman, Manin y otros propusieron aprovechar esos fenómenos cuánticos para acelerar la computación en un sentido general lo cual implicaba una redefinición del modelo teórico de computación y desplazarlo fuera del dominio de la Mecánica Clásica. Deutsch propuso entonces un nuevo modelo de computación, la Maquina de Turing Cuántica, que sí era realmente universal pues podía simular, no solo todos aquellos procesos realizables en una Maquinad de Turing sino además, aquellos otros que quedaban fuera de su alcance.

El algoritmo de Deutsch, en 1985 demostró como es posible realizar una tarea de forma más eficiente que su versión clásica utilizando la superposición de estados y Peter Shor, en 1994 describió un algoritmo de factorización que se considera exponencialmente más rápido que su versión clásica, lo cual hizo que la idea de un computador cuántico cobrara impulso y distintas industrias y gobiernos comenzaran a estar interesados. Hoy es uno de los sectores más competitivos y de más rápido crecimiento con aplicaciones en ciberseguridad, criptografía, optimización, simulación y muchas otras.

La Computación, la Informática y las Telecomunicaciones están todas ellas presentes en nuestro entorno de forma ubicua y su comportamiento se puede describir con las leyes de la Física Clásica. Si bien la aplicación de ciertas leyes de la Mecánica Cuántica permitió el desarrollo de tecnologías tan disruptivas y transformadoras como el transistor, el láser, los LEDs o el GPS, los dispositivos que las utilizan están gobernados por las leyes de la Física Clásica. El modelo de computación tal y como lo conocemos, el que hace funcionar nuestros teléfonos o nuestros ordenadores está basado en la Máquina de Turing, que es, de nuevo, un modelo clásico. Solo recientemente, esas otras leyes de la Mecánica Cuántica que no se utilizaban, como el entrelazamiento o la superposición, han empezado a aplicarse a las comunicaciones y la computación.

La Ley de Moore predijo que el número de transistores por unidad de superficie en circuitos integrados se duplicaría cada año y que la tendencia se mantendría durante décadas. Así ha sido hasta el momento, sin embargo, no es posible miniaturizarlo de forma indefinida pues el transistor es un dispositivo clásico y al alcanzar determinadas dimensiones las leyes que lo gobiernan dejan de ser clásica ay pasa al reino de la Mecánica Cuántica afectando a su correcto funcionamiento. Es por ello que el límite de miniaturización se está acercando.

La Computación Cuántica no busca reemplazar el transistor por otro dispositivo que pueda operar bajo las leyes de la Mecánica Cuántica sino proporcionar un paradigma de computación distinto. Ese nuevo paradigma no utiliza el bit como unidad de información sino el bit cuántico o cúbit. La aplicación de la Mecánica Cuántica en Computación conduce al desarrollo de nuevos algoritmos más rápidos, nuevas formas de criptografía y protocolos de comunicaciones mejorados.

Los computadores clásicos, los que utilizamos cada día o los super computadores o los procesadores presentes en los electrodomésticos o los vehículos se basan en transistores que son una tecnología que aprovecha el comportamiento de un semiconductor, un fenómeno derivado de la Teoría Cuántica, sin embargo, el modelo de computación está basado en el bit y por tanto no se consideran procesadores cuánticos. Un procesador es clásico o cuántico si la forma en la que la información es representada y procesada es clásica o cuántica.

La Computación Cuántica tiene cierto parecido con la Computación Analógica ya que en esta última, a diferencia de la Computación Binaria, se permiten valores continuos además de los discretos. Sin embargo, los modelos son radicalmente diferentes, pues la Computación Analógica no implementa el entrelazamiento, un recurso fundamental en Computación Cuántica, y a su vez, en la Computación Cuántica, el proceso de medida del registro cuántico proporciona únicamente valores discretos, de esta forma el proceso de medida permite solamente extraer un bit de información del cúbit.

La Computación Cuántica fue inicialmente desarrollada en las dos últimas décadas del siglo XX por un grupo de investigadores que elaboraron una teoría de la información cuántica y el procesamiento de la información cuántica o computación cuántica. David Deutsch elaboró el concepto de la Maquina de Turing Cuántica, Daniel Bernstein, Vijay Vazirani and Andrew Yao mejoraron el modelo y demostraron como una Máquina de Turing Cuántica podría simular una Máquina de Turing Clásica y por consiguiente, su universalidad. A continuación se desarrollo el modelo de circuito cuántico lo cual condujo al entendimiento de la complejidad cuántica en términos de un repertorio básico de transformaciones denominadas puertas cuánticas, las cuales podían o no tener su equivalente con los componentes físicos de los ordenadores clásicos.

Los primeros algoritmos realmente cuánticos que mostraron, al menos teóricamente, que la computación cuántica, para cierto tipo de problemas, era superior a la computación clásica, fueron desarrollados en los primeros años de la década de los 90. Estos algoritmos permitían resolver con certeza y en tiempo polinómico problemas que solo era posible resolver por un computador clásico en tiempo polinómico con alta probabilidad pero no con certeza. Tales resultados, si bien carecían todavía de aplicación práctica al no existir una implementación física de un procesador cuántico, fueron del suficiente interés teórico como para despertar el interés de varios investigadores, entre ellos, Peter Shor, que en 1994 sorprendió a la comunidad científica con el algoritmo que lleva su nombre y que permite factorizar un numero entero en tiempo polinómico. Este algoritmo proporcionaba una solución a un problema muy estudiado ya que estaba reconocido por la comunidad científica su dificultad computacional y que no existía una solución, hasta el punto de que dicho problema se utilizaba como la base, para los protocolos de seguridad, incluido el algoritmo ampliamente utilizado en

multitud de aplicaciones RSA.

Se desconoce si existe una solución clásica eficiente de forma que el algoritmo de Shor no prueba que un computador cuántico pueda resolver un problema de forma más eficiente que un procesador clásico pero en cualquier caso, respaldaba y mostraba la efectividad y elegancia de la computación cuántica, a pesar de todos los aspectos no intuitivos de la mecánica cuántica.

A pesar del éxito que supuso el algoritmo de Shor, las dudas sobre el interés práctico de la computación cuántica continuaban. Los sistemas cuánticos son extremadamente frágiles, efectos cuánticos fundamentales como la superposición o el entrelazamiento se ven fácilmente afectado por la influencia del entorno que causan la decoherencia y el desfase. Además, imposiciones de la mecánica cuántica como la derivada del teorema de no clonado que impide realizar una copia del estado de un sistema cuántico desconocido, hacían improbable que pudiera desarrollarse un mecanismo efectivo de corrección de errores para la computación cuántica y por todo ello existían fuertes dudas de que pudiera construirse un computador cuántico fiable. Afortunadamente, y a pesar de las dudas sobre el valor que puede aportar la computación cuántica, la comunidad científica continuó investigando y finalmente, desarrollando técnicas que hacían posible la corrección de errores. Hoy en días es uno de los campos más activos y el más desarrollado de la computación cuántica.

Cronología de la Computación Cuántica

1980 Paul Benioff describe un modelo cuántico de la Máquina de Turing, siendo el primero en demostrar la posibilidad de la computación cuántica.

1981 En la conferencia sobre La Física de la Computación, Richard Feynman (IMT) habla sobre la simulación de la física con computadoras y propone que una computadora cuántica podría simular fenómenos físicos intratables por una computadora clásica.

1985 David Deutsch (Universidad de Oxford) describe la Máquina de Turing Cuántica Universal.

1992 David Deutsch y Richard Jozsa presentan el algoritmo de Deutsch-Jozsa, uno de los primeros ejemplos de un algoritmo cuántico determinista que es exponencialmen-

te más rápido que cualquier posible algoritmo clásico determinista.

1993 Charles Bennet (IBM) publica un artículo donde se describe la idea de la teleportación cuántica

1994 Peter Shor (Bell Laboratories) desarrolla un algoritmo cuántico para factorizar enteros exponencialmente más rápido que ningún algoritmo clásico conocido.

1996 Lov Grover (Bell Laboratories) desarrolla el algoritmo de Grover para búsqueda en bases de datos no estructuradas con una ventaja cuadrática sobre cualquier algoritmo clásico.

1998 David Cory realiza la primera demostración experimental de la corrección de errores cuánticos confirmando la esperada estabilización del estado cuántico.

1999 Yasunobu Nakamura (Universidad de Tokio) y Jaw-Shen Tsai (Universidad de Ciencias de Tokio) demuestran que un circuito superconductor puede usarse como un cúbit.

2004 Jian-Wei Pan (Universidad de Ciencia y Tecnología de China) demuestra el primer entrelazamiento de cinco fotones.

2011 D-Wave Systems ofrece la primera computadora cuántica disponible comercialmente

2014 Físicos del Instituto Kavli de Nanociencia (Universidad Tecnológica de Delft) demuestran la teleportación del estado entre dos qubits separados 3 metros con una tasa de error del cero por ciento.

2017 Un equipo de investigadores chinos de diferentes instituciones demuestran la primera teleportación cuántica entre un observatorio terrestre y un satélite en órbita baja a una distancia de 1400 km.

2017 IBM despliega Quantum Experience, el primer procesador cuántico en la nube accesible para que cualquiera pueda ejecutar sus propios experimentos de computación cuántica.

2019 Google afirma haber alcanzado la supremacía cuántica al realizar una tarea en

200 segundos y que requeriría 10,000 años para un super-computador clásico.

1.4 Ventaja cuántica

Todavía no está claro hasta donde podrá llegar la computación cuántica pero no existen principios físicos fundamentales que impidan el desarrollo de procesadores cuánticos fiables y a gran escala. Actualmente es uno de los campos de investigación más activos, con infinidad de investigadores teóricos y experimentales explorando nuevos enfoques que permitan alcanzar esa meta.

La computación cuántica no proporciona soluciones eficientes para todos los problemas ni permite eludir los limites a la escalabilidad del procesador clásico. Se conocen importantes limitaciones de la computación cuántica, para determinados problemas no proporciona ninguna ventaja, para otros, como el algoritmo de Grover, que permite realizar búsquedas en una base no estructurada, la ventaja es solo cuadrática. La simulación de la naturaleza, de sistemas cuánticos cada vez más grandes, podría finalmente ser la aplicación que justifique la construcción de un procesador cuántico escalable.

Encontrar una ventaja demostrable para un problema práctico es un área activa de investigación en computación cuántica, incluso si no es posible demostrar que no existe un algoritmo clásico más eficiente, la computación cuántica puede ser un recurso para resolver un determinado problema

A principios de la década de 2000, se descubrieron varios algoritmos nuevos y se desarrollaron nuevas ideas para el desarrollo de algoritmos cuánticos. La Computación Cuántica y la simulación de los sistemas cuánticos, también han promovido el desarrollo de nuevos algoritmos clásicos de inspiración cuántica. Además, todo este esfuerzo de investigación ha desencadenado en formas de computar alternativas al modelo de circuito generando a su vez nuevos algoritmos, importantes avances en la tecnología de construcción de procesadores cuánticos así como una mejora en el entendimiento de los elementos fundamentales de la computación cuántica. Por mucho que se tar-

de en construir una computadora cuántica escalable y cualquiera que finalmente sea el alcance de sus aplicaciones, la computación cuántica ha cambiado para siempre la forma en que se entiende la propia Mecánica Cuántica contribuyendo a su comprensión en aspectos como el proceso de medida o el entrelazamiento. Estos avances han generado a su vez aplicaciones fuera del ámbito de la información y el procesamiento de la información cuánticas como en el campo de la sensórica. Las consecuencias de esta convergencia entre las dos teorías más importantes y transformadoras del siglo pasado, la Teoría de la Información y la Teoría Cuántica, que desencadenaron la revolución informática, la nanotecnología y muchas otras, con toda seguridad dejarán una profunda huella en el desarrollo científico y tecnológico del presente siglo.

A pesar de los extraordinarios avances en la capacidad de computación disponible actualmente y cuya evolución hemos visto en las últimas décadas, todavía son muchos los problemas a los que nos enfrentamos, que no pueden ser tratados por la computación clásica. De hecho, la mayoría de los problemas son intratables, solo un reducido subconjunto de los problemas computacionales podemos resolverlos. Y no solo no podemos tratarlos actualmente sino que con la computación clásica no podrán ser nunca resueltos pues los problemas exponenciales requieren un paradigma computacional distinto para poder ser tratados, requieren de computación exponencial, de la computación cuántica.

La computación cuántica no solo puede resolver ciertos problemas exponenciales gracias al paralelismo inherente que proporciona, también permite una mayor densidad de información y un ahorro en el consumo energético. Problemas tan variados como la gestión del tráfico, la optimización de una fábrica o el comportamiento esperado de un nuevo fármaco son ejemplos de problemas exponenciales. Un procesador cuántico no es más rápido que un procesador clásico, de hecho es más lentos, nuestros sistemas clásicos de computación binaria, de computación exacta, los hemos ido mejorando hasta alcanzar una eficiencia extraordinaria. La clave está en que el computador cuántico, aun siendo más lento, aborda el problema de forma diferente y finalmente puede resolver en muy poco tiempo un problema exponencial intratable para la computación clásica. Sin embargo, el procesador cuántico no podrá resolver todos los problemas de forma eficiente, al menos con el entendimiento que disponemos actualmente.

Investigar qué problemas pueden resolverse y desarrollar algoritmos para ello es el foco de la investigación en computación cuántica tanto en el mundo académico como el industrial. No solo es importante la construcción del procesador físico, las distintas capas necesarias para ofrecer capacidad de computación cuántica a los usuarios finales son igualmente vitales. El software es fundamental, el desarrollo de librerías que permitan abstraer los detalles de la implementación física y acelerar el desarrollo de aplicaciones es de extraordinaria importancia, prácticamente todo los fabricantes de hardware de esta naciente industria proporcionan entornos de desarrollo con interfaces gráficas y programáticas de acceso a los procesadores.

Hoy, es todavía difícil determinar que problema puede beneficiarse de la computación cuántica o hasta donde podrá llegar esta, hasta el momento se han identificado ciertas soluciones a problemas que ofrecen ventajas significativas sobre las soluciones clásicas, en todas ellas, un entendimiento de la estructura del problema y el aprovechamiento de los efectos cuánticos han logrado la ventaja. Los algoritmos de Simon, Deutsh-Jozsa, Shor o Grover son claros ejemplos de aplicación que demuestran cómo el entrelazamiento y la interferencia permite que el algoritmo descarte las soluciones incorrectas y proporcione la solución.

La computación cuántica es el fin, pero aspectos derivados de ella como la sensórica, la metrología, la criptografía o las comunicaciones, se ven también impulsados ya que con el esfuerzo en mejorar el control, la medición o la coherencia del cúbit, con el fin de almacenar y procesar la información, también se ha mejorado la comprensión en otras áreas de aplicación de la ciencia cuántica.

1.5 Aplicaciones

Las aplicaciones más importantes de la computación cuántica están probablemente todavía por descubrir, nos encontramos en los albores de esta tecnología, hacer una lista de las aplicaciones sería como haber predicho la aplicación de *Whatsup* como una aplicación de la computación clásica en los años 40, en los años de Alan Turing.

Sin embargo, los avances hasta el momento, y las actuales aplicaciones sí permiten, al menos, identificar las grandes áreas que podrán beneficiarse.

Es probable que el área que primero se beneficie de la computación cuántica sea la de la simulación de la Naturaleza, la simulación de sistemas cuánticos. Simular una molécula es un problema extremadamente costoso computacionalmente pues el calculo de la energía de una molécula depende de los electrones y los núcleos, las interacciones de repulsión entre electrones y la de atracción entre electrones y núcleos. Se tiene que calcular la interacción de cada elemento con todos los demás y si uno de ellos cambia se debe calcular todo nuevamente. De forma que la dinámica molecular es un problema de n cuerpos que crece exponencialmente con n y solo moléculas muy pequeñas pueden simularse clásicamente.

La Química, la simulación de la naturaleza como nunca antes ha sido posible, el modelado de los sistemas físicos con resolución cuántica es un problema intratable incluso para los super-computadores. La simulación de moléculas e incluso de materiales sería posible. Esto, en si mismo, es suficiente para justificar toda la inversión realizada, tanto intelectual como económica. Tiene el potencial de transformar industrias enteras, como la de los materiales, la industria farmacéutica, la industria química, la genética y muchas otras, donde la capacidad de simular el comportamiento de la materia a escala molecular dará lugar a una nueva era de descubrimientos. La simulación eficiente con computación cuántica permitiría el desarrollo de nuevos medicamentos para la industria farmacéutica, nuevos materiales, catalizadores, baterías eléctricas más eficientes, etc.

La segunda área en aprovechar la ventaja de la computación cuántica será la Inteligencia Artificial, si bien la IA es una tecnología, su potencial esta muy limitado por la insuficiente capacidad de computación de los procesadores clásicos. Ya existen pruebas de este potencial, el modelo matemático de la computación cuántica se base en espacios vectoriales de muy grandes dimensiones sobre el cuerpo de los números complejos, el aprendizaje automático, la base de la IA Aprendizaje automático utiliza igualmente un modelo de espacios vectoriales de dimensiones muy grandes, además, las sub-rutinas utilizadas en aprendizaje automático se pueden ver muy beneficiadas en sus implementaciones cuánticas por la facilidad natural que tiene la computación cuántica para

manejar matrices, algo muy costoso en computación clásica pero fácil en computación cuántica, especialmente cuando hablamos de dimensiones muy grandes. La computación cuántica podría acelerar los procesos necesarios subyacentes a la la IA, incluso permitiendo el procesamiento en tiempo real. Aplicado en robótica, por ejemplo, permitiría mejorar la percepción, la comprensión y el tiempo de respuesta. También el procesamiento del lenguaje natural, otra disciplina dentro de la IA, exige una enorme potencia de cálculo y tiene un modelo matemático próximo a la computación cuántica que podría beneficiarse. Podría ser la tecnología que permita impulsar el desarrollo de una verdadera IA.

La optimización es otra de la aplicaciones más prometedoras, se han desarrollado algunos algoritmos de optimización muy prometedores y que se adaptan bien a esta primera etapa del desarrollo de la computación cuántica en la que los procesadores son de una escala intermedia y sometidos al ruido (NISQ, Noisy Intermediate Scale Quantum) como el algoritmo QAOA (Quantum Approximate Optimization Algorithm). La optimización es un campo de las matemáticas que se ocupa de encontrar la solución óptima a un determinado problema y tiene aplicación en multitud de campos, desde la distribución a la fabricación o las finanzas, son problemas exponenciales, como el problema del viajero, donde encontrar la solución optima entre un numero cada vez mayor de posibilidades, a medida que crece la magnitud del problema, requiere enormes recursos computacionales. La computación cuántica permite abordar ciertos problemas de optimización de forma eficiente frente a la computación clásica para la que resultan intratables.

El campo de los sistemas financieros se enfrenta a enormes necesidades computacionales, existen numerosos problemas computacionalmente intensivos, como la optimización de carteras financieras, optimización de la trayectoria, la detección del fraude, el análisis de riesgos, la predicción de las crisis financieras, la lista es interminable porque el modelado del sistema financiero es extraordinariamente complejo. Para ciertos problemas en este sector, la computación cuántica puede proporcionar una ventaja significativa en comparación con la computación clásica, podría permitir simulaciones mas eficientes, rápidas y complejas que las actualmente disponibles con computación clásica.

1.6 Desafios

El desarrollo de esta tecnología se enfrenta a grandes desafíos técnicos. El sistema cuántico que permite la computación es extremadamente frágil y cualquier perturbación del entorno puede afectarlo, ya sea radiación electromagnética no deseada, vibraciones, cambios en la temperatura, etc. Durante la computación, el sistema debe enfrentarse a la decoherencia, es decir mantener el estado cuántico necesario para los cómputos sin alteraciones indeseadas pues de lo contrario los resultados no serán correctos. Técnicamente el desafío es enorme ya que por un lado necesitamos controlar el procesador cuántico con precisión y rapidez lo cual exige un fuerte acoplamiento con él, así como con el mecanismo de medida pero por otro queremos que el sistema permanezca aislado del entorno, totalmente desacoplado de este para evitar su influencia, esta contradicción entre los requerimientos hace muy difícil alcanzar ese equilibrio.

Una vez que se ha producido un error en el proceso de cómputo, este puede corregirse mediante un adecuado tratamiento, esta disciplina se conoce como la corrección del error cuántico y es de vital importancia, dado que un único error en un cálculo puede invalidar la totalidad de la computación.

Error en la medida, una vez que la computación ha finalizado, el estado cuántico no puede extraerse pero si se pueden medir ciertos observables, la fiabilidad de este proceso de medida es fundamental ya que proporciona los resultados, la solución al problema y cualquier defecto en su lectura igualmente invalida los resultados.

Existen numerosas tecnologías que permiten la realización de un cúbit, todas ellas con ventajas y desventajas de forma que todavía no existe una tecnología definitiva que permita escalar y a la vez garantizar la fiabilidad, nos encontramos todavía en una etapa de exploración en este aspecto, investigando para encontrar la optima. Varias de las tecnologías requieren unas condiciones de refrigeración del chip cuántico extremas lo que dificulta su desarrollo, la capacidad para construir chips cuánticas con características identicas es otro de los problemas asociados a las técnicas de fabricación.

A fondo

1.7 Referencias bibliográficas

Richard Feynman. Simulating physics with computers. International Journal of Theoretical Physics, 1981.

Nielsen and Chuang (2011) Quantum Computation and Quantum Information

Eric R. Johnston, Nic Harrigan y Mercedes Gimeno-Segovia (2019), Programming Quantum Computers

Eleanor Rieffel and Wolfgang Polak (2011), Quantum Computing

Robert Sutor (2019), Dancing with Qubits