

COMPUTACIÓN CUÁNTICA:
PRINCIPIOS, AVANCES Y EXPECTATIVAS

RIANEIRO ERNESTO MIRON RECINOS



UNIVERSIDAD GALILEO

FACULTAD DE INGENIERIA DE SISTEMAS,
INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

2024

Esta tesis fue elaborada por el autor como requisito para obtener el grado de Ingeniero de Sistemas, Informática y Ciencias de la Computación.

Guatemala, abril de 2024

Guatemala, 29 de febrero de 2024.

Ingeniero Rodrigo Baessa lunge
Decano de FISICC
Universidad Galileo

Estimado Ingeniero Baessa,

Me dirijo a usted para informarle que he asesorado el trabajo de Tesis titulado "**Computación cuántica: Principios, avances y expectativas**" elaborado por el estudiante de la carrera de Ingeniería de Sistemas Rianeiro Ernesto Mirón Recinos.

El estudiante elaboró un excelente trabajo el cual será de beneficio para quienes lo consulten, ya que les proporcionará una clara comprensión del tema. Por ello me complace informarle que doy por **APROBADO** el contenido de este trabajo, el cual someto a su consideración.

Atentamente,



Ing. Ronald Israel López España

Ronald Israel López España
Ingeniero de Sistemas
Colegiado No. 5634

Ciudad de Guatemala, 03 de abril de 2024.

Ingeniero

Rodrigo Baessa

Decano FISICC

Universidad Galileo

Presente.

Señor Decano:

Le informo que la tesis: **"COMPUTACIÓN CUÁNTICA: PRINCIPIOS, AVANCES Y EXPECTATIVAS"**, del estudiante Rianeiro Ernesto Mirón Recinos, ha sido objeto de revisión gramatical y estilística, por lo que pueden continuar con el trámite de graduación.

Atentamente.



Lic. Edgar Lizardo Porres Velásquez

Asesor Lingüístico

Universidad Galileo



Galileo
UNIVERSIDAD
La Revolución en la Educación

Guatemala, 4 de abril de 2024

Ing. Rodrigo Baessa Iunge
Decano de FISICC
Universidad Galileo

Estimado Ingeniero,

Tengo el gusto de informarle que he tenido a la vista el trabajo de tesis elaborado por el estudiante **Rianeiro Ernesto Mirón Recinos** quién se identifica con carnet número I086060, titulado *“Computación cuántica: Principios, avances y expectativas”*, por tanto doy por *Aprobado* que se inicie el trámite final de Tesis de la carrera de Ingeniería de Sistemas, Informática y Ciencias de la Computación.

Atentamente,

**FACULTAD DE INGENIERIA DE SISTEMAS,
INFORMATICA Y CIENCIAS DE LA COMPUTACION**


Ing. Ronald López
Director de Ingeniería de Sistemas,
Informática y Ciencias de la Computación



Galileo
UNIVERSIDAD
La Revolución en la Educación

Guatemala, 5 de abril de 2024

Señor
Rianeiro Ernesto Mirón Recinos
Presente

Estimado señor Mirón:

Tengo mucho gusto en informarle que, después de tener a la vista la carta del Director de la Carrera quien indica haber revisado el trabajo de Tesis cuyo título es ***“Computación cuántica: Principios, avances y expectativas”*** y haber obtenido su dictamen como asesor específico, autorizo la publicación del mismo.

Aprovecho la oportunidad para felicitarlo por el magnífico trabajo realizado, el cual es de indiscutible beneficio para el desarrollo de las Ciencias de la Computación en Guatemala.

Atentamente,

**FACULTAD DE INGENIERIA DE SISTEMAS,
INFORMATICA Y CIENCIAS DE LA COMPUTACION**

Ing. Rodrigo Baessa
Decano

COMPUTACIÓN CUÁNTICA:
PRINCIPIOS, AVANCES Y EXPECTATIVAS

ÍNDICE

Capítulo	Página
I. INTRODUCCION.....	9
II. ANTECEDENTES.....	11
III. NECESIDAD ACTUAL.....	22
IV. MECANICA CUÁNTICA.....	25
V. ORIGEN Y DESARROLLO	32
VI. QUBITS.....	38
VII. COMPUERTAS CUÁNTICAS.....	48
VIII. ARQUITECTURA.....	52
IX. PROCESADORES CUÁNTICOS.....	57
X. COMPUTADORES CUÁNTICOS ACTUALES	62
XI. ALGORITMOS CUÁNTICOS	69
XII. LENGUAJES DE PROGRAMACIÓN CUÁNTICOS.....	79
XIII. EXPECTATIVAS FUTURAS.....	90
XIV. CONCLUSIONES.....	94

I. INTRODUCCION

Introducción:

A través de la historia de la humanidad, la necesidad de efectuar cálculos de diferentes tipos, llevó a esta a utilizar su ingenio y poder investigativo para satisfacer sus necesidades de cuantificación de la información. Primero, la necesidad de contar los activos, los granos, el ganado.

Luego, la necesidad de cálculo para la construcción, por ejemplo, de caminos, de puentes, casas, edificios.

Posteriormente para la construcción de máquinas simples, que a su vez se utilizaban para hacer máquinas más complejas.

Y todo se origina aquí.

Las diferentes áreas de la humanidad, como salud, comunicación, militar y cálculo han hecho que la computación provea los medios para los grandes cálculos que ellas requieren, y por lo mismo, se ha presionado a las empresas de tecnología para que provean mejores sistemas para efectuarlos. Eso es lo que da origen al presente estudio, en el que se presentan diferentes aspectos de la computación cuántica, como antecedentes, conceptos, elementos, relación con la mecánica cuántica, estado actual y expectativas de esta tecnología.

II. ANTECEDENTES

Antecedentes:

En los siglos tempranos de la historia de la humanidad por ejemplo, tenemos el ábaco (Mesopotamia, alrededor del siglo 24 AC)

A través de los siglos más recientes, se pudo observar la invención de máquinas más complejas, como la "Máquina Analítica" de Charles Babbage, que contenía una unidad de memoria, una unidad de control, una unidad aritmética y una unidad de salida.

Aunque esta no fue construida en su totalidad, por las limitaciones de la época, sin embargo, su importancia se vio aumentada pues sirvió de base para el desarrollo de las primeras computadoras electrónicas.

A través de los años se ha clasificado a las computadoras en generaciones

Primera generación (Aproximadamente, las construidas entre 1940 y 1950): Estas utilizaban tubos de vacío, lo que las hacía necesitar mucho espacio y electricidad, y producían mucho calor.

Segunda generación (Entre 1950 y 1960, aproximadamente): Utilizaban transistores, lo que ayudó a reducir su tamaño y eran más rápidas que las de tubos de vacío. Pudieron tener más memoria.

Tercera generación (Entre 1960 y 1970, aproximadamente): Utilizaban circuitos integrados, permitiendo que se combinaran muchos transistores en un solo chip.

Cuarta generación (Entre 1970 y 1980). Basada en microprocesadores, que son circuitos integrados que contienen todos los componentes necesarios para la ejecución de programas.

Quinta generación. De 1980 al presente (2023 o 2024). Esta es la generación con la que actualmente nos encontramos más familiarizados porque hemos sido testigos de los avances de las computadoras. La miniaturización de las tecnologías y el aumento del poder de cómputo, a través de la industria, han provisto a la humanidad de herramientas hasta hace unas décadas inalcanzables.

Escala de medida del poder de procesamiento:

FLOP es el acrónimo de Floating Point Operations per Second, es decir Operaciones de punto flotante por segundo. Es una unidad de medida del rendimiento de una computadora, especialmente en cálculos científicos que requieren un gran uso de operaciones de coma flotante.

Unidad	Abreviatura	Equivalencia	Decimal
Kiloflop	KFLOP	Mil FLOPS	10^3
Megaflop	MFLOP	Millón FLOPS	10^6
Gigaflop	GFLOP	Mil millones FLOPS	10^9
Teraflop	TFLOP	Billón FLOPS	10^{12}
Petaflop	PFLOP	Billón de billones FLOPS	10^{15}
Exaflop	EFLOP	Quintillón FLOPS	10^{18}
Zettaflop	ZFLOP	Mil Quintillones FLOPS	10^{21}
Yottaflop	YFLOP	Sextillón FLOPS	10^{24}

La tabla anterior nos muestra la escala del poder de procesamiento de las computadoras tradicionales. En la siguiente sección, veremos las características de algunas supercomputadoras que incluyen el uso de esta escala.

Veamos aquí algunos ejemplos de este poder de cómputo:

Cray-2: (1985)

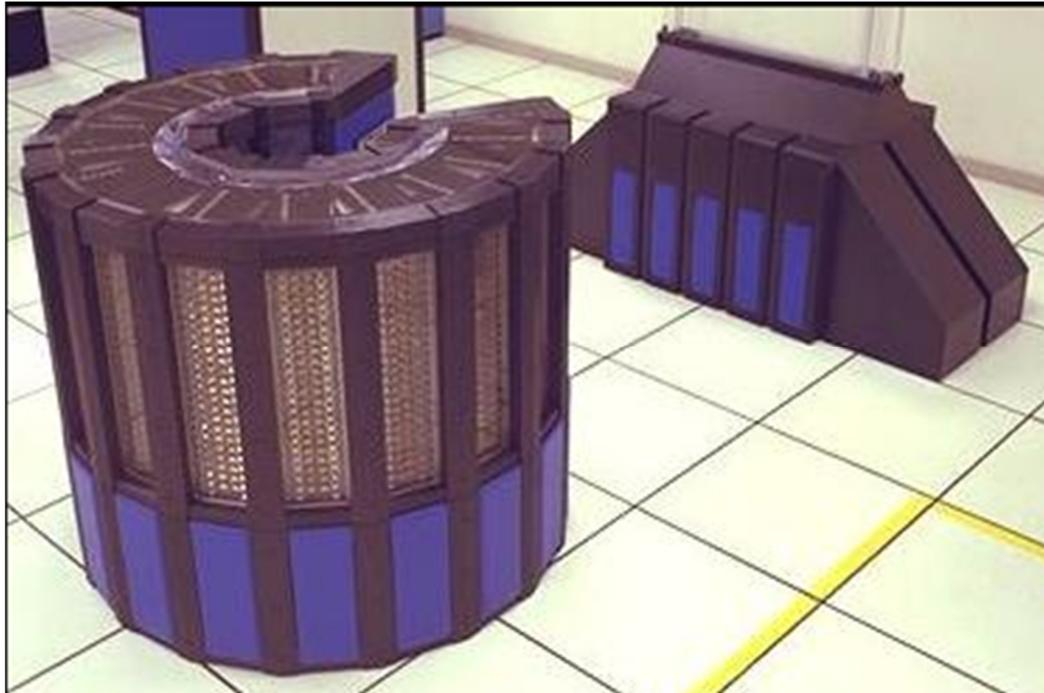


Foto: Wikipedia

Memoria de 256M palabras de 64 bits, o sea 2 gigabytes y una memoria secundaria de 2 gigabytes de estado sólido para almacenamiento de programas. (*Bard: "¿Qué cantidad de memoria tuvo la primera cray-2?", es.wikipedia.org*).

Velocidad de procesamiento: 1.9 GFLOPS.

Un smartphone promedio hoy en día puede superar los 100 GFLOPS

Reloj de 244 Mhz.

Enfriada por liquido

Fujitsu VP-200 (1990)



Memoria RAM de 2 GB

Velocidad : 1024 Gigaflops

Reloj de 312.5Mhz

Enfriada por agua

(Bard: "¿Cuáles son las características de la super computador Fujistus VP-200?")

IBM Blue Gene/L (2004)



Fue la primera super computadora en llegar a la escala de procesamiento en exaflops, o sea, 10^{18} flops

Memoria RAM a razón de 512 Mb de memoria DDR SDRAM por módulo de cómputo. Por ejemplo, el modelo que se instaló en el Lawrence Livermore National Laboratory, tenía 1024 nodos de cómputo, o sea 524 Gb.

Velocidad de procesamiento: Por lo menos un exaflop, aunque la arquitectura de esta computadora está basada en nodos paralelos, 65000 para ser exacto. Cada nodo contenía un microchip con un arreglo de procesador, motores matemáticos y sistemas de comunicación y memoria.

(dato comparativo curioso: Un Playstation 5 tiene 10.28 teraflops (10,280,000,000,000 flops) de capacidad de procesamiento)

Reloj de 700Mhz en cada nodo de cómputo.

Enfriada por refrigeración líquida.

(ChatGPT: "¿Cuáles son las características de la super computadora IBM Blue Gene/L?")

IBM Sequoia (2011)



En 2009, alcanzó 16.32 petaflops (16.32×10^{15}) de velocidad de procesamiento. Corre en su totalidad en Linux, con 98,000 nodos de cómputo.

Memoria RAM: Hay varias fuentes no oficiales, pero se supone que estaba en la escala de los petabytes (10^{15} bytes).

Reloj: 2.2 Ghz en cada nodo.

Enfriada por refrigeración líquida.

(ChatGPT, Bard: "¿Cuáles son las características de la IBM Sequoia", Wikipedia)

IBM Summit:



En 2019 alcanzó 148.6 PETAFLUPS

Memoria: > 600Gb de memoria coherente+800Gb de memoria volátil

Reloj: 3.8 Ghz por procesador

Enfriada por refrigeración líquida.

(ChatGPT, Bard: "¿Cuáles son las características de la super computadora IBM Summit?", Wikipedia)

Fugaku (2020)



Es la supercomputadora más rápida del mundo en la actualidad (2023-2024). Tiene un rendimiento de 442 petaflops.

Arquitectura basada en procesadores ARM (es decir, no Intel, no IBM).

Memoria: 5.5 PETABYTES (158976 nodos con 32 Gb cada uno)

Reloj: 3.45Ghz en cada procesador.

Enfriada por refrigeración líquida.

(ChatGPT, Bard: "¿Cuáles son las características de la super computadora Fugaku?", Wikipedia)

Uso de las super computadoras:

A través de su tiempo de funcionamiento, estas super computadoras tienen una variedad bastante amplia de aplicación y se utilizan en diferentes áreas para abordar problemas complejos que requieren de mucho poder de cómputo.

Ejemplos de uso:

En la investigación científica:

Climatología: Modelos climático para prever patrones climáticos, estudiar el cambio climático y simular eventos extremos.

Astrofísica: Simulaciones para entender la formación de galaxias, estrellas y otros fenómenos cósmicos.

Bilología: Simulación de estructuras biológicas y modelos de procesos biológicos

Genómica: Análisis de datos genómicos

Física de partículas: Procesamiento de datos de experimentos de alta energía, como los creados en los aceleradores de partículas.

Diseño de Fármacos y Simulación Molecular:

Investigación y diseño de nuevos medicamentos mediante simulaciones moleculares y modelado de interacciones a nivel atómico.

Dinámica de Fluidos y Simulación de Vuelo:

Simulaciones detalladas de la dinámica de fluidos para el diseño de aeronaves, vehículos espaciales y optimización de procesos industriales.

Investigación en Energía:

Modelado de procesos de fusión nuclear y simulaciones para el diseño y optimización de reactores nucleares.

Análisis y simulación de sistemas de energías renovables.

Investigación en Materiales:

Simulaciones para entender las propiedades de nuevos materiales, como superconductores o materiales avanzados para electrónica.

Análisis de Grandes Conjuntos de Datos:

Procesamiento masivo de datos en campos como la bioinformática, la astronomía, la inteligencia artificial y el aprendizaje automático.

Seguridad Nacional:

Simulaciones y análisis para la investigación en defensa y seguridad, incluyendo el modelado de explosiones, simulaciones de impacto, y análisis de inteligencia.

Simulaciones Financieras:

Modelado de riesgos financieros, simulaciones de carteras de inversión y análisis de datos económicos a gran escala.

Investigación en Inteligencia Artificial:

Entrenamiento de modelos de aprendizaje profundo en conjuntos de datos masivos para tareas como reconocimiento de imágenes, procesamiento del lenguaje natural y juegos estratégicos.

Diseño de Ingeniería:

Simulaciones avanzadas para el diseño y la optimización de productos en ingeniería, como automóviles, aviones, y estructuras.

III. NECESIDAD ACTUAL

Necesidad actual:

Criptografía Cuántica

La computación cuántica podría afectar la seguridad de los sistemas criptográficos actuales. Sin embargo, también se están desarrollando métodos de criptografía cuántica que aprovechan las propiedades únicas de la mecánica cuántica para proporcionar comunicaciones seguras.

Optimización

La computación cuántica puede ser especialmente eficiente para problemas de optimización, como la programación lineal y la optimización combinatoria, que son comunes en la logística, la planificación y la cadena de suministro.

Simulación Cuántica

La simulación de sistemas cuánticos es una aplicación natural de la computación cuántica. Esto podría tener aplicaciones en la simulación de materiales, reacciones químicas y procesos cuánticos complejos.

Aprendizaje Automático Cuántico

El aprendizaje automático cuántico aprovecha los principios de la mecánica cuántica para realizar cálculos más eficientes en tareas específicas de aprendizaje automático, como el análisis de grandes conjuntos de datos.

Química y diseño de Materiales

La simulación de moléculas y materiales a nivel cuántico es un desafío computacional significativo. Las computadoras cuánticas podrían acelerar el proceso de descubrimiento y diseño de nuevos materiales y compuestos químicos.

Finanzas Cuánticas

En el sector financiero, la computación cuántica podría utilizarse para realizar simulaciones más precisas de instrumentos financieros complejos y para optimizar carteras de inversión.

Biología y Medicina

La simulación cuántica puede ayudar en la comprensión de procesos biológicos a nivel molecular, lo que podría tener aplicaciones en el diseño de medicamentos y la comprensión de enfermedades.

Inteligencia Artificial Cuántica

La computación cuántica podría mejorar ciertos algoritmos de inteligencia artificial, como la optimización combinatoria y la búsqueda en grandes espacios de soluciones.

Logística y Distribución

Problemas de enrutamiento y planificación logística, que son esenciales en la cadena de suministro, podrían beneficiarse de algoritmos cuánticos para encontrar soluciones más eficientes.

Resolución de Problemas Cuánticos

La computación cuántica está diseñada específicamente para abordar problemas cuánticos, como la factorización de números grandes, lo que podría tener implicaciones para la seguridad de los sistemas criptográficos actuales.

IV. MECANICA CUÁNTICA

Mecánica cuántica:

“Creo que puedo decir con seguridad que nadie entiende la mecánica cuántica”

Richard Feynman.

El famoso físico estadounidense estaba en lo cierto. Es correcto que él era un provocador nato, es decir, le gustaba “molestar” a sus colegas de la época, pero, sus observaciones solían ser bastante acertadas. Lo que cabalmente pretendía era hacer notar con su comentario es la dificultad de la mente humana para aceptar la mecánica cuántica. Cuánto más se piensa en ella, más nos alejamos de entenderla, desafiando la intuición y tal vez hasta parece contradecir lo que se conoce a través de la física tradicional.

Y esto es así porque la física cuántica supone una ruptura radical con la física clásica, a la que estamos más acostumbrados debido a que se encuentra presente en nuestra actividad diaria.

Es fácil convencernos de la relación entre fuerzas y aceleraciones de la mecánica de Newton, porque nos hemos educado con ella.

Diferencias entre la física cuántica y la mecánica cuántica:

Estos términos a menudo son intercambiables y, para la mayoría de propósitos, se pueden considerar que son lo mismo. Sin embargo, hay algunos elementos conceptuales en los que difieren:

Física cuántica:

Término más amplio: Este involucra el campo total del estudio de tratar con el comportamiento de la materia y la energía en el nivel atómico y subatómico.

Incluye varias teorías: Esto incluye no solamente la mecánica cuántica misma sino también las teorías relacionadas, como la teoría de campos cuánticos, electrodinámica cuántica y cromodinámica cuántica.

Perspectiva más general: Se enfoca en los fenómenos y conceptos que provienen de la naturaleza cuántica del universo.

Mecánica cuántica:

Teoría específica: Se refiere al marco matemático específico usado para describir y predecir el comportamiento de sistemas cuánticos.

Principios básicos: Establece los principios fundamentales que rigen aspectos como la dualidad onda-partícula, la cuantificación, la superposición y el entrelazamiento.

Se enfoca en cálculos: Enfatiza las herramientas y técnicas matemáticas utilizadas para resolver problemas y hacer predicciones en el ámbito cuántico.

Podríamos pensar en la física cuántica como un gran país con diversos paisajes y ecosistemas.

La mecánica cuántica sería entonces un juego específico de leyes que gobiernan la física de ese país, explicando cómo las cosas como la gravedad, el electromagnetismo y la termodinámica trabajan ahí. (Bard "¿Cuál es la diferencia entre física cuántica y mecánica cuántica?")

Sin embargo, no es tan sencillo tener una idea intuitiva sobre el entrelazamiento cuántico, que usualmente solo conocemos a través de libros. *(Muy interesante, Avelino Vicente, "El gato de Schrödinger: más allá de las ecuaciones", 21-12-2023)*

Hablando más poéticamente, podríamos decir lo siguiente: En el vasto reino de la ciencia, anidado en el infinitesimal corazón del átomo, yace un dominio gobernado por leyes contraintuitivas y una belleza paradójica. Este es el enigmático dominio de la mecánica cuántica, una teoría que ha reescrito el guion de la realidad en su nivel más fundamental.

La mecánica cuántica surgió a principios del siglo XX, donde la física clásica comenzó a verse "en apuros", por decirlo así, bajo la presión de las observaciones experimentales, por ejemplo, la radiación del cuerpo negro, el efecto fotoeléctrico y la estabilidad de los átomos. Todos ellos representaban grandes enigmas que eran casi imposibles de explicar dentro del marco newtoniano.

La radiación del cuerpo negro es la radiación electromagnética térmica dentro o alrededor de un cuerpo en equilibrio termodinámico con su entorno, o emitida por un cuerpo negro. Un cuerpo negro es un objeto idealizado que absorbe toda la radiación electromagnética que incide sobre él y no refleja ni transmite ninguna.. (Bard: "¿Qué es la radiación del cuerpo negro?", Dic. 2023)

En 1900, Max Planck propuso la cuantización de la energía que indica que la energía no es continua sino que se emite en paquetes discretos llamados **cuantos**. *(Bing: "Qué es la cuantización de la energía?", Wikipedia en español)*

La cuantización de la energía es un procedimiento matemático para construir un modelo cuántico para un sistema físico a partir de su descripción clásica. Más formalmente, dada la descripción hamiltoniana de un sistema clásico mediante una variedad simpléctica, se puede

definir formalmente el proceso de cuantización como la construcción de un espacio de Hilbert tal que al conjunto de magnitudes físicas u observables medibles en el sistema clásico se le asigna un conjunto de observables cuánticos u operadores autoadjuntos.

Esta noción radical es la que sienta las bases para una revolución intelectual.

A partir de las propuestas de Planck, varias mentes brillantes empezaron a encender el panorama cuántico. Albert Einstein, Erwin Schrödinger, Werner Haisenberg, entre otros, crearon conjuntos de reglas matemáticas y abstracciones conceptuales para capturar la esencia del reino cuántico. La dualidad onda-partícula, la superposición y el entrelazamiento se convirtieron en los pilares fundamentales de una nueva física, donde el observador se convierte en una parte integral de lo observado.

La hipótesis de Planck fue confirmada por experimentos posteriores. En 1923, Albert Einstein recibió el Premio Nobel de Física por su explicación del efecto fotoeléctrico, que se basa en la naturaleza cuántica de la luz. Esta propuesta la hizo en 1905, indicando que la luz se propaga en paquetes discretos de energía, llamados fotones. Esta hipótesis fue necesaria para explicar el efecto fotoeléctrico, que es un fenómeno en el que la luz puede expulsar electrones de un metal. Este efecto fue una de las primeras pruebas experimentales de la naturaleza cuántica de la luz.

Einstein fue uno de los primeros en reconocer que la luz tiene una naturaleza dual, ya que se puede comportar como una onda o como una partícula. Esta dualidad se ha demostrado experimentalmente para otras partículas como los electrones.

La teoría de la relatividad especial de Einstein, publicada en 1905, también tuvo un impacto significativo en la mecánica cuántica. La relatividad especial establece que la velocidad de la luz es la misma para todos los observadores, independientemente de su movimiento. Esta restricción tiene implicaciones importantes para la mecánica cuántica, ya que limita la forma en que las partículas pueden interactuar entre si (*Bard: "Cuál fue el aporte de Albert Einstein a la mecánica cuántica", Dic. 2023*).

Niels Bohr hizo aportes fundamentales a la mecánica cuántica, ya que fue el primero en aplicar los principios de la mecánica cuántica al problema de la estructura atómica. Su modelo atómico, publicado en 1913, fue un éxito inmediato ya que explicaba de forma satisfactoria las líneas espectrales de los átomos. Los electrones pueden pasar de una órbita cuántica a otra, emitiendo o absorbiendo energía en forma de fotones.

Introdujo el concepto de órbitas cuánticas. Según Bohr, los electrones en un átomo no pueden ocupar cualquier órbita, sino sólo aquellas que cumplen con ciertas condiciones de energía.

Estableció el principio de la cuantificación de la energía: La energía de un electrón en una órbita cuántica es un múltiplo entero de una constante fundamental, la constante de Planck.

(Bard: "Cuál fue el aporte de Bohr a la mecánica cuántica?", Dic. 2023)

Por su parte, el aporte de Erwin Schrödinger a la mecánica cuántica fue su ecuación diferencial parcial, que se conoce como la ecuación de Schrödinger, la cual describe el comportamiento de las partículas cuánticas, tal como los electrones, en el espacio y tiempo. Esta es una ecuación no lineal, lo que significa que no tiene soluciones analíticas simples, pero se puede resolver numéricamente para obtener información sobre el comportamiento de las partículas cuánticas.

Otro de los aportes de Schrödinger fueron las contribuciones significativas para el desarrollo de la interpretación probabilística de la mecánica cuántica, las cuales sostienen que la función de onda de la partícula cuántica representa la probabilidad de que la partícula se encuentre en una ubicación determinada.

Schrödinger recibió el Premio Nobel de Física en 1933 por sus contribuciones a la mecánica cuántica *(Bard: "Cuál fue el aporte de Erwin Schroedinger a la mecánica cuántica", Dic. 2023)*.

También Werner Heisenberg fue un ente importante en la mecánica cuántica.

En 1927 formuló el principio de incertidumbre, que establece que es imposible medir simultáneamente la posición y el momento de una partícula con precisión arbitraria. Este principio es una consecuencia fundamental de la naturaleza cuántica del mundo y tienen implicaciones profundas para nuestra comprensión de la realidad.

Otro aporte de Heisenberg, aunque menos comentado, es la mecánica matricial. Heisenberg desarrolló una formulación matemática de la mecánica cuántica conocida como mecánica matricial, que es una forma equivalente de la mecánica cuántica a la ecuación de Schrödinger pero proporciona una perspectiva diferente sobre la teoría.

Interpretación probabilística de la mecánica cuántica: Heisenberg también apoyó la interpretación probabilística de la mecánica cuántica, que indica que la función de onda de una partícula cuántica representa la probabilidad que la partícula se encuentre en cierta ubicación. *(Bard: " Cuáles fueron las contribuciones de Werner Heisenberg a la mecánica cuántica?")*

Interpretaciones de la mecánica cuántica:

El inicio de la física cuántica, junto con los debates sobre su interpretación son algunos de los temas más centrales en la historia de la física del siglo XX y su desarrollo se marcó por una visión teórica totalmente nueva, la cual debía ser interpretada para dar cuenta de ciertas observaciones experimentales como la radiación de cuerpo negro, el efecto fotoeléctrico y los espectros atómicos.

Fue von Neumann quien fundamentalmente se encargó de crear los axiomas de la mecánica cuántica y crear lo que se llamaría la *interpretación ortodoxa* (la habitual, tal y como se

encuentra en los libros de texto) y que es confundida usualmente con la interpretación de Copenhague. La diferencia fundamental entre estas dos interpretaciones es precisamente la interpretación del estado cuántico. Ambas interpretaciones aceptan los conceptos fundamentales de la mecánica cuántica, como la dualidad onda-partícula, la función de onda y el principio de incertidumbre.

La interpretación de Copenhague: dice que la función de onda representa la probabilidad de que la partícula se encuentre en una ubicación determinada. El colapso de la función de onda es un evento fundamental que ocurre al medir la partícula.

La interpretación de von Neumann: dice que la función de onda es una descripción completa de la realidad. La medición no colapsa la función de onda, sino que simplemente revela la información que ya estaba presente en la función de onda.

La interpretación de Copenhague es una interpretación filosófica, mientras que la interpretación de von Neumann es una interpretación matemática. La interpretación de Copenhague es la más aceptada por los físicos. (*Bard: "Cuál es la diferencia principal entre la interpretación de Copenhague de la mecánica cuántica y la interpretación de von Neumann?". Dic. 2023*)

La interpretación de De Broglie-Bohm: Esta interpretación fue propuesta originalmente por Louis de Broglie en 1927 y redescubierta por David Bohm en 1952. También conocida como teoría de la onda piloto, es una interpretación de la mecánica cuántica que describe el comportamiento de las partículas cuánticas mediante la combinación de una función de onda y una trayectoria definida. La función de onda, como en la interpretación de Copenhague, describe la probabilidad de que la partícula se encuentre en una ubicación determinada. La trayectoria, por otro lado, describe el movimiento real de la partícula. (*Bard: "En qué consiste la interpretación de la mecánica cuántica de De Broglie-Bohm". Dic. 2023*)

La interpretación de muchos universos: Esta interpretación propone que todas las posibles historias y resultados cuánticos que podrían ocurrir en una situación dada realmente suceden, pero en diferentes "ramas" o "universos". Esta interpretación también se conoce como la "interpretación de la multitud de mundos" o "teoría de los muchos mundos". Esta fue propuesta inicialmente por Hugh Everett III en 1957. Según esta interpretación, cuando se realiza una medición cuántica y el sistema cuántico se encuentra en un estado de superposición, en lugar de colapsar en una de las dos posibles opciones, el universo se "divide" en dos ramas diferentes, cada una correspondiente a una de las posibles opciones (*ChatGPT 3.5: "En que consiste la interpretación de muchos universos de la mecánica cuántica?". Dic. 2023*).

La interpretación de Bell: Está relacionada con los experimentos propuestos por el físico John Bell para abordar la cuestión de la naturaleza de las correlaciones cuánticas y la aparente violación de ciertos principios de la física clásica. Estos experimentos y sus resultados llevaron a cuestionar las interpretaciones más convencionales de la mecánica cuántica, como la interpretación de Copenhague. La base de esta interpretación se encuentra en la desigualdad de Bell, que fue derivada por John Bell en 1967. Es una expresión matemática que establece ciertas restricciones

sobre las correlaciones que se pueden observar entre las propiedades cuánticas de partículas entrelazadas. La desigualdad de Bell mostró que si las correlaciones cuánticas se explicaran mediante variables ocultas locales, es decir, si hubieran propiedades locales preexistentes en las partículas que determinaran sus estados finales, entonces deberían cumplirse ciertas relaciones matemáticas específicas. Sin embargo, los experimentos realizados desde la propuesta de la desigualdad de Bell han demostrado que las correlaciones cuánticas violan las restricciones, lo que sugiere que la mecánica cuántica no puede ser explicada completamente por variables ocultas locales. (ChatGPT: "¿En qué consiste la interpretación de Bell de la mecánica cuántica?", Dic. 2023)

(Víctor Rivero Arranz, *Tesis de fin de grado, Universidad de Valladolid, Facultad de ciencias, 2016*, <https://uvadoc.uva.es/bitstream/handle/10324/19018/TFG-G1775.pdf;jsessionid=049AFC8F6A44BC264D705105CD7D9640?sequence=1>)

V. ORIGEN Y DESARROLLO

Origen y desarrollo de las computadoras cuánticas

Tratemos de definir una computadora cuántica:

Según Bard:

“Una computadora cuántica es un dispositivo de cálculo que utiliza los fenómenos específicos de la mecánica cuántica, como la superposición y el entrelazamiento, para ejecutar operaciones sobre datos.”

Según OpenIA:

“Una computadora cuántica es un tipo especial de computadora que utiliza principios de la mecánica cuántica para realizar operaciones y almacenar información. A diferencia de las computadoras clásicas, que usan bits clásicos para representar información como 0 o 1, las computadoras cuánticas necesitan qubits (bits cuánticos), que pueden existir en múltiples estados simultáneamente gracias al fenómeno conocido como superposición cuántica.”

Según Bing:

“Una computadora cuántica es una máquina que procesa información utilizando qubits en lugar de bits. Los qubits son unidades de información cuántica que pueden estar en una superposición de estados, lo que significa que pueden representar múltiples valores simultáneamente. Esto permite que las computadoras cuánticas realicen cálculos complejos a una velocidad increíblemente alta, mucho más rápido que las computadoras clásicas”

Según Wikipedia:

“Una computadora cuántica es una computadora que toma ventaja del fenómeno de la mecánica cuántica”

De acuerdo con Nihal Mehta, en su libro “Computación Cuántica” (Mehta, 2020) “Una computadora cuántica no es algo que se pueda descargar del internet o comprar en una tienda. Las computadoras cuánticas son grandes bestias que requieren una instalación cuidadosa y delicada. Tienen que ser enfriadas a temperaturas cercanas al cero absoluto –algo así como -

273 grados C, si queremos ser precisos. Su refrigerador, en comparación, es un sauna a donde una computadora cuántica iría después de un largo día de trabajo”

El mismo autor indica que el hardware de una computadora cuántica no está construido de puro material de silicio que puede ser manipulado por manos humanas o brazos robóticos. En vez de eso, está construida de átomos, que son millones de veces más delgados que el cabello humano. En el caso de una compuerta CNOT (controlled not (*not* no controlado)), que es un dispositivo utilizado en computadoras cuánticas, un solo átomo de Berilio es despojado de un electrón para formar un ion positivo. Este ion se enfría con un láser a temperaturas extremadamente bajas (mucho más frío de lo que uno estaría en la Antártida) para detener su movimiento oscilatorio natural. Entonces, un pulso de luz finamente sintonizado juega con los electrones restantes en el ion de Berilio para causar las operaciones CNOT. Esta maquinaria o aparato requiere ingeniería de precisión y está almacenado en instalaciones cuidadosamente monitoreadas.

Seiki Akama, en su libro “Elements of Quantum Computing” (Akama, 2015) nos presenta con una versión de la historia de la computación, la que considero apropiada para este estudio.

Benniof:

Paul Benniof (1930-1922) apuntó, en 1980, a una posibilidad de construir una computadora basada en la mecánica cuántica. El propuso un modelo de computadoras mecánico-cuánticas en el marco de una “Máquina de Turing”, que es un modelo standard de computación.

Una máquina de Turing es un modelo matemático de un dispositivo computacional que puede seguir un conjunto de instrucciones para realizar cálculos. Fue propuesto por el matemático británico Alan Turing en 1936.

El punto de partida de Benniof era hacer circuitos lógicos más pequeños. Él mostró que un circuito de escala atómica podría ser construido. El modelo de Benniof puede ser interpretado como un modelo computacional que satisface las leyes de la mecánica cuántica.

Sugirió el uso de diferentes espines de partículas elementales para representar 2 dígitos binarios y, prácticamente, en este modelo, la computación se lleva a cabo de acuerdo a las leyes de la mecánica cuántica sin consumir energía.

En física cuántica, el espín es una propiedad intrínseca de las partículas elementales que describe su momento angular intrínseco. El espín es una propiedad cuántica, lo que significa que no se puede relacionar directamente con una rotación en el espacio.

Feynman:

Richard Phillips Feynman (1918-1988) señaló en 1982 que algún tipo de fenómeno mecano-cuántico no puede ser simulado efectivamente por computadoras clásicas tradicionales y afirmó que la computación para simular fenómenos físicos puede ser ejecutada más efectivamente utilizando fenómenos mecano-cuánticos. Las computadoras deberían tener un mecanismo computacional que obedece las leyes de la mecánica cuántica.

Adicionalmente, Feynmann introdujo algunos ejemplos de fenómenos físicos que pueden ser interpretados como modelos computacionales de computadoras cuánticas.

Deutsch:

David Elieser Deutsch (1953-). En 1985 propuso un modelo computacional llamado "*quantum computer*" que reformula una máquina de Turing y tiene el poder computacional equivalente a Máquina de Turing cuántica.

La computadora cuántica de Turing es el primer modelo computacional de una computadora cuántica. Como esta teoría es más concreta que la de Feynman y es compatible con la tradición de las ciencias de la computación, debería ser considerada como otro origen de la investigación de computadores cuánticos.

Deutsch también mostró una teoría de *puerta cuántica*, que es otro modelo de computadoras cuánticas, en 1988. Una puerta cuántica es una puerta lógica para computadoras cuánticas y esto aumentó las posibilidades de crear computadoras cuánticas.

Bernstein y Vazirani.

Ethan Joseph Bernstein y Umesh Vazirani, en 1993 propusieron una Máquina de Turing universal cuántica, lo que generaliza la máquina cuántica de Turing.

También probaron que ambas máquinas de Turing, la clásica y la cuántica, tienen poder computacional equivalente. Su investigación se convirtió en un primer paso para clarificar los aspectos computacionales de las computadoras cuánticas, como computabilidad y complejidad

Shor:

Peter Shor Williston (1959-). En 1994 demostró un algoritmo cuántico de tiempo polinomial para factorización de números primos y logaritmos discretos.

Un algoritmo cuántico para factorización de números primos es llamado un *Algoritmo de Shor*. Se observa que el algoritmo justifica una fuerte posibilidad para utilizar computadores

cuánticos. Esto se debe a que la factorización de números primos se sabe que es algo muy difícil de resolver, que es la base del código RSA, que es un sistema de criptografía de clave pública que se utiliza para proteger la información confidencial, y desarrollado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977, siendo este uno de los algoritmos criptográficos más utilizados en la actualidad.

El resultado de Shor nos muestra que hay una posibilidad de romper la seguridad de la codificación RSA, si se implementa una computadora cuántica y esta factorización de números primos es ejecutada rápidamente por esta computadora.

Aquí, hago un paréntesis en la cronología histórica del autor del libro del cual se están tomando estos datos históricos, y hago el comentario que a pesar de que el algoritmo de Shor podría sonar como algo completamente ilegal e inadecuado, por razones morales, es decir la decodificación, es importante notar que este mismo poder computacional podría también ser utilizado para resolver problemas de carácter o comportamiento similar, y por lo tanto ayudando en el avance mundial hacia mejor utilización de estos recursos.

Grover:

Lov Kumar Grover (1961-). En 1996, propuso el Algoritmo Cuántico de búsqueda Grover, el cual puede buscar datos en una base de datos no estructurada en el orden de $O(\sqrt{n})$. El algoritmo es llamado *El Algoritmo de Grover*.

Wecker y su equipo

Davis Wecker, Christopher Monroe, Michael Nielsen y William Oliver, en 1998 implementaron el lenguaje QCL, que es un lenguaje procedural similar al lenguaje C y puede ser usado para la implementación y simulación de varios algoritmos cuánticos.

Gershenfeld y Chuang:

Neil Adam Gershenfeld y Isaac Chuang. En 1998, en el MIT, desarrollaron una computadora cuántica de 2 qubits, basado en NMR (Resonancia magnética nuclear). Y esta fue la primera implementación real de una computadora cuántica

En 2001, IBM tuvo éxito al desarrollar una computadora cuántica NMR de 7 qubits e implementó el algoritmo de Shor, y así, demostrando la efectividad de NMR para la implementación de computadores cuánticos.

También hay otros enfoques del hardware de computadores cuánticos. Ellos incluyen los iones atrapados, puntos cuánticos, y la intersección de Josephson. Actualmente, es posible

desarrollar computadoras cuánticas con más de 10 qubits y se espera que haya más investigación al respecto.

Nos damos cuenta que también se están estableciendo teorías fundamentales para aplicaciones de computación cuántica.

VI. QUBITS

Qubits:

Definición:

Un Qubit es una unidad básica de información cuántica. Los qubits son análogos a los bits clásicos, pero pueden existir en una superposición de estados, lo que significa que pueden estar en un estado 0 y 1 al mismo tiempo. Esta propiedad permite que las computadoras cuánticas ejecuten computaciones que son imposibles para las computadoras clásicas.

Los qubits se implementan típicamente utilizando sistemas físicos tales como circuitos superconductores, iones atrapados o fotones.

En cada uno de estos sistemas, el qubit se representa por un sistema de 2 niveles, tales como el spin de un electrón o la polarización de un fotón. El estado del qubit se determina por el valor de este sistema de dos niveles.

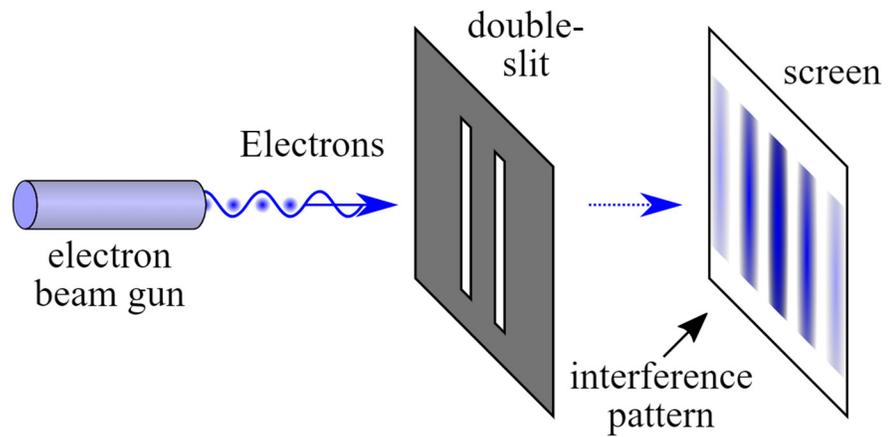
Las operaciones cuánticas son ejecutadas en los qubits, utilizando puertas cuánticas. Las puertas cuánticas son como puertas lógicas clásicas pero operan en qubits que pueden tomar ventaja de las propiedades de superposición de los qubits. Las compuertas cuánticas pueden utilizarse para entrelazar qubits, lo que significa que los qubits se encadenan juntos de tal manera que comparten el mismo destino, por así decirlo.

Propiedades principales de los qubits:

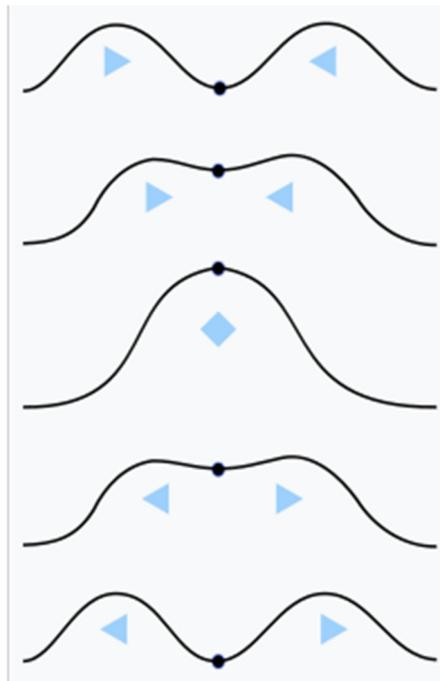
Superposición:

Los qubits pueden existir en una superposición de estados, lo que significa que pueden estar en dos estados completamente diferenciados (por ejemplo, 0 ó 1) o en ambos, con una cierta probabilidad de estar en uno o en otro de los estados. Esta propiedad permite que los ordenadores cuánticos puedan realizar cálculos mucho más complejos que los computadores convencionales.

Un ejemplo de superposición de qubits es el experimento de la doble rendija, que muestra cómo una partícula de luz, o fotón, puede pasar por dos rendijas al mismo tiempo y crear un patrón de interferencia en una pantalla detrás de las rendijas. *(tomado de ICHI.PRO, Dic. 2023)*



Otro ejemplo de uso de la propiedad de superposición son los experimentos de interferencia de ondas. Aquí, cuando 2 ondas se superponen, pueden interferir entre sí, creando patrones de interferencia.

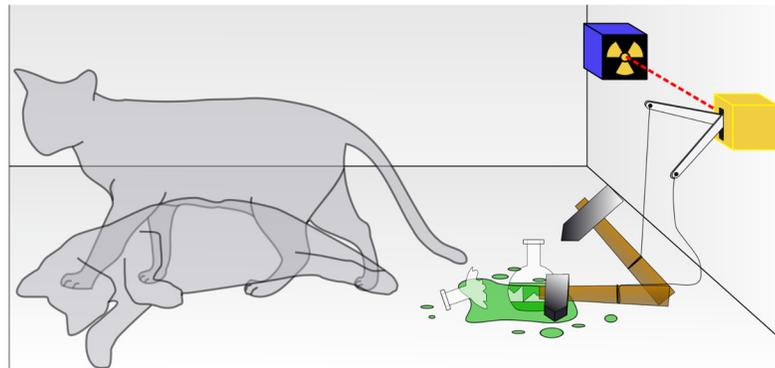


En esta gráfica podemos ver cómo 2 ondas que oscilan en diferentes direcciones llegan a "chocar" para formar una nueva onda, que a su vez obtiene nuevos parámetros de oscilación..

Otro ejemplo del uso de la propiedad de superposición son las cámaras de spin. Estos son dispositivos que se utilizan para detectar partículas subatómicas. Cuando una partícula subatómica pasa por una cámara de spin, queda en un estado de superposición cuántica, y la dirección del spin se puede determinar midiendo el estado de la superposición.

La superposición cuántica es un principio fundamental de la mecánica cuántica, y más formalmente, si dice, sostiene que un sistema físico como un electrón, existe en todos sus teóricamente posibles estados (o la configuración de sus propiedades) de forma simultánea, *hasta que es observado*. Al medirse (si es que esto es posible) el sistema colapsa aleatoriamente sobre uno de los posibles estados. Después de la medición el estado del sistema corresponde al resultado de la medición. (Wikipedia. Dic. 2023)

En 1935, Erwin Schrödinger ideó un experimento de naturaleza imaginaria llamado "el gato de Schrödinger". En este experimento, se pondría un gato adentro de una caja, con algún mecanismo mortal para el felino. En cualquier momento, el gato podría estar vivo o muerto, ya que no lo estamos observando, no hay certeza de su destino. Pero al abrir la caja, entonces sabremos si está vivo o muerto. Esto es, se sabe el estado del gato hasta que observamos (abrimos la caja).



La superposición de qubits tiene muchas aplicaciones potenciales en campos como la criptografía, inteligencia artificial, simulación molecular, optimización y aprendizaje automático. (your-physicists.com)

A pesar de ser un fenómeno complejo que aún no se entiende completamente, es un aspecto fundamental en la mecánica cuántica y está empezando a revolucionar la ciencia y la tecnología. (Bard: "¿Qué es la superposición en mecánica cuántica?", Dic. 2023)

Entrelazamiento:

El entrelazamiento cuántico es una propiedad predicha en 1935 por Einstein, Podolsky y Rosen (EPR) en su formulación de la llamada paradoja EPR, y básicamente se refiere a que uno o más qubits se pueden unir o enlazar de tal manera que tienen el mismo destino o suerte (en palabras).

Es un fenómeno fundamental de la mecánica cuántica en el cual dos o más partículas se relacionan de manera que el estado cuántico de una partícula no puede describirse de manera independiente del estado de las otras, incluso cuando están separadas por distancias significativas. (*Bard: "Qué es el entrelazamiento cuántico?". Dic. 2023*)

Cuando una o más partículas están entrelazadas, las propiedades cuánticas como el espín, la polarización o el momento angular de una partícula están correlacionadas de manera instantánea con las propiedades de otra partícula, independientemente de la distancia que las separe.

Entonces, si se hace una medición en una de las partículas y se determina su estado cuántico, el estado de la otra partícula se conoce instantáneamente, incluso si están lo suficientemente separadas para considerar esta distancia considerable.

Hay numerosos experimentos que han demostrado que el entrelazamiento cuántico existe.

A veces, se ha interpretado de manera errónea como una "comunicación más rápida que la luz", el entrelazamiento cuántico no permite la transmisión de información de manera instantánea, ya que las correlaciones cuánticas no se pueden utilizar para enviar señales a velocidades superiores a la velocidad de la luz.

Algunos ejemplos de experimentos que demuestran la existencia del entrelazamiento cuántico:

Experimento de Aspect:

En 1982, Alain Aspect llevó a cabo un experimento que confirmó las predicciones de la teoría cuántica sobre el entrelazamiento. El experimento de Aspect se basó en las desigualdades de Bell, propuestas por John Bell en la década de 1960. Estas desigualdades describen cómo deberían comportarse las correlaciones cuánticas en comparación con las correlaciones clásicas. En el experimento, se mostraron violaciones de las desigualdades de Bell, lo que indicaba que las correlaciones cuánticas eran inconsistentes con las teorías local realistas o de la física clásica.

Se generaron dos fotones entrelazados en una fuente. Los fotones se enviaron luego en direcciones opuestas a dos detectores, ubicados a una distancia de 12

metros. Cada detector tenía dos filtros, que podían girarse para permitir o bloquear el paso de los fotones.

Los investigadores midieron la polarización de los fotones a medida que pasaban por los filtros. La polarización es una propiedad de la luz que determina la dirección en la que se vibran las ondas electromagnéticas.

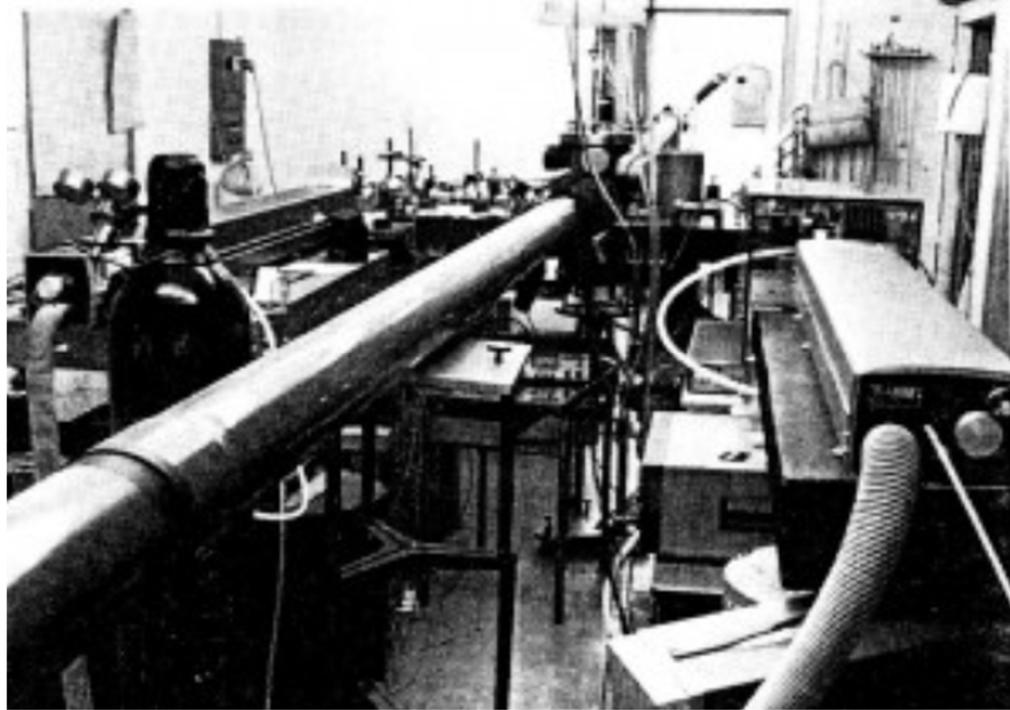
Si los fotones no estuvieran entrelazados, los investigadores esperarían que los resultados de las mediciones fueran aleatorios. Sin embargo, los resultados del experimento mostraron que los fotones entrelazados estaban correlacionados en su polarización.

Por ejemplo, si un fotón pasaba por un filtro que permitía el paso de fotones polarizados en una dirección, el otro fotón siempre pasaba por un filtro que permitía el paso de fotones polarizados en la dirección opuesta.

Estos resultados fueron inesperados, ya que desafiaban la intuición clásica. Según la física clásica, la polarización de un fotón debería ser independiente de la polarización del otro fotón. Sin embargo, los resultados del experimento de Aspect mostraron que los fotones entrelazados estaban correlacionados, incluso si estaban separados por una gran distancia.

Este experimento fue muy importante en la investigación del entrelazamiento cuántico. Sus resultados demostraron que el entrelazamiento cuántico es una propiedad real de la naturaleza y que desafiaba las leyes de la física clásica. (*Bard y ChatGPT: "Descripción del experimento de Aspect". Dic. 2023*)

En la siguiente fotografía, podemos ver el montaje del experimento de Aspect.



Experimento de Weihs:

En este experimento, realizado por Gerd Weihs, Anton Zeilinger, Thomas Jennewein, Christoph Simon y Harald Weinfurter en 1998; se utilizó el entrelazamiento de fotones para demostrar las correlaciones cuánticas. Utilizaron pares de fotones entrelazados y los separaron a distancias considerablemente grandes (3 metros). Luego, realizaron mediciones independientes en cada uno de los fotones. Los resultados de este experimento también mostraron violaciones de las desigualdades de Bell, respaldando la existencia del entrelazamiento cuántico. También mostraron que los fotones entrelazados estaban correlacionados en su polarización, incluso cuando los filtros se giraban de forma independientes.

Por ejemplo, si un fotón pasaba por un filtro que permitía el paso de fotones polarizados en una dirección, el otro fotón siempre paraba por un filtro que permitía el paso de fotones polarizados en dirección opuesta.

Este comportamiento de la polarización fue inesperado, ya que desafiaban la causalidad local, que indica que la polarización de un fotón no debe influir en la polarización de otro fotón, a menos que exista una conexión causal entre ambos. Sin

embargo, el experimento mostró que los fotones entrelazados estaban correlacionados, incluso cuando no existía ninguna conexión causal entre ellos.

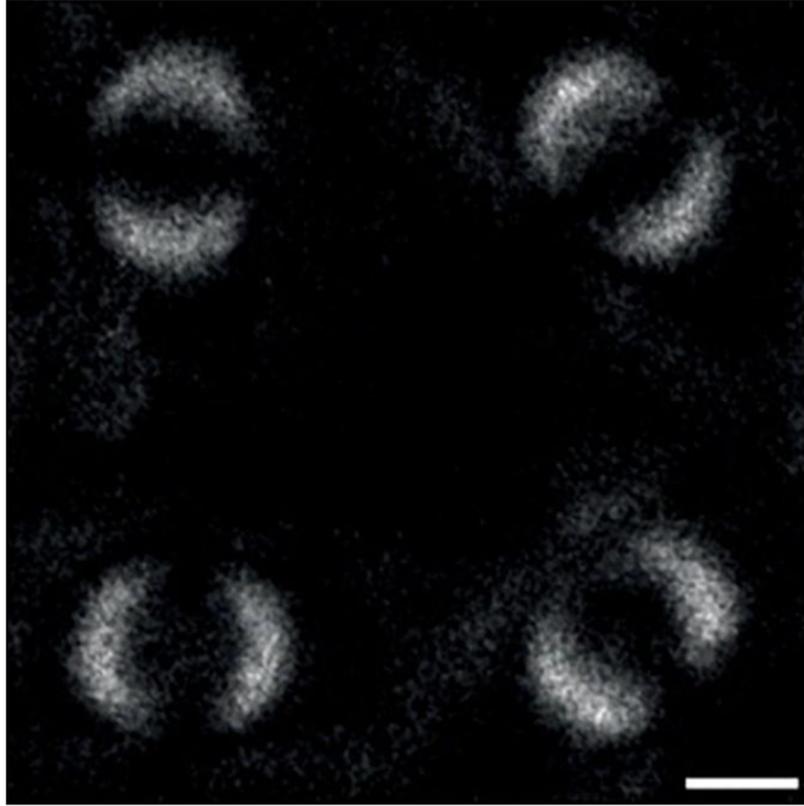
Los resultados de este experimento ayudaron a nuestra comprensión del universo, demostrando que el entrelazamiento cuántico es una propiedad real de la naturaleza y que no se puede explicar por las leyes de la física clásica.

El entrelazamiento cuántico tiene implicaciones importantes para la comunicación y computación cuánticas. La comunicación cuántica, utiliza el entrelazamiento cuántico para transmitir información de forma segura y eficiente. La computación cuántica lo utiliza para realizar cálculos que son imposibles de realizar en las computadoras clásicas.

Es importante notar, que en 2019, un equipo de físicos de la Universidad de Glasgow logró fotografiar por primera vez en la historia el preciso momento en el que se produce el entrelazamiento de dos partículas. Esto se logró gracias a un sistema desarrollado por los físicos, que origina una corriente de fotones en dirección a un punto de "*objetos no convencionales*" que son filtrados a través de un cristal líquido. El sistema, equipado con una cámara super sensible, capturó cuatro imágenes de los fotones pasando por diferentes etapas de transición. (Bing: "*¿Existen fotografías del experimento de entrelazamiento cuántico de Weihs?*").

(para una descripción completa y formal del experimento se puede consultar <https://www.science.org/doi/10.1126/sciadv.aaw2563>)

He aquí una de las 4 fotografías obtenidas por el equipo:



Experimento de Zeilinger:

En 1997, Anton Zeilinger y su equipo de la Universidad de Viena, Austria, logró el primer teletransporte cuántico.

Este experimento se realizó con fotones entrelazados cuánticamente. En el experimento, los investigadores generaron dos fotones entrelazados en una fuente. Luego, enviaron uno de los fotones a un detector en Viena, Austria, y el otro fotón a un detector en Innsbruck, Austria.

Luego, midieron el estado del fotón en Viena y esta información la utilizaron para reconstruir el estado del fotón en Innsbruck.

Los resultados del experimento mostraron que el estado del fotón en Innsbruck era idéntico al estado del fotón en Viena, incluso a pesar de que las dos partículas estaban separadas por una distancia de 144 kilómetros.

Este experimento y su resultado fueron un gran avance en la investigación del teletransporte cuántico y demostró que el teletransporte cuántico es posible, al menos a escalas pequeñas.

Luego, en 2001, el equipo de Zeilinger repitió el experimento con átomos de cesio. Este experimento demostró que el teletransporte cuántico también es posible con partículas más grandes.

En 2019, otro equipo de investigadores de la Universidad de Innsbruck, logró el primer teletransporte cuántico de un fotón a un átomo. De esta manera, se demostró que el teletransporte cuántico puede utilizarse para transferir información entre partículas de diferentes naturalezas. (*Bard: "Describe el experimento de Anton Zeilinger". Dic. 2023*)

VII. COMPUERTAS CUÁNTICAS

Compuertas cuánticas:

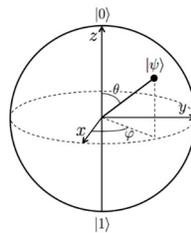
Son las operaciones que se realizan sobre los qubits para realizar cálculos. Las compuertas cuánticas pueden ser de un solo qubit, de 2 qubits, o de múltiples qubits.

Las compuertas cuánticas son análogas a las compuertas lógicas en las computadoras clásica, pero operan sobre *estados cuánticos*. Estas compuertas manipulan la amplitud de la probabilidad de los estados cuánticos, permitiendo la creación de superposiciones y entrelazamientos cuánticos, que como ya vimos, son fenómenos esenciales para la capacidad de procesamiento cuántico. (Bard: "Qué es una compuerta cuántica?". Dic. 2023)

Veamos a continuación algunos ejemplos de compuertas cuánticas:

Compuerta X (NOT cuántica): Realiza una rotación de 180 grados alrededor del eje X en la esfera de Bloch, equivalente a la compuerta NOT clásica. En otras palabras Si el qubit está en el estado base $|0\rangle$, la compuerta X lo cambiará al estado $|1\rangle$. (ChatGPT: "Dame ejemplos de compuertas cuánticas"). De manera similar, si el qubit está en el estado $|1\rangle$, la compuerta X lo cambiará al estado $|0\rangle$ (<https://medium.com/quantumhispano/amable-introducci%C3%B3n-a-las-compuertas-cu%C3%A1nticas-de-un-qubit-con-qiskit-6cb332c31663> "Introducción a las Compuertas cuánticas de un qubit con Qiskit")

"La esfera de Bloch es una representación geométrica del espacio de estados puros de un sistema cuántico de dos niveles, también conocido como qubit. Es una esfera de radio unitario, cuyo centro representa el estado del qubit cuando está en su estado fundamental, y la superficie representa todos los estados posibles del qubit."



Compuerta H (Hadamard)

Esta es una compuerta de un qubit que convierte un estado de qubit puro a uno de qubit superpuesto, es decir, el qubit resultante está en un estado de superposición de los estados $|0\rangle$ y $|1\rangle$ con una probabilidad del 50% de estar en cada uno. Se puede representar matemáticamente con la siguiente matriz unitaria:

$$H = 1/\sqrt{2}$$

$$|0\rangle\langle 0| + 1/\sqrt{2}$$

$$|1\rangle\langle 1|$$

que representa la transformación realizada por la compuerta sobre los estados de qubits puros. Por ejemplo, si el qubit de entrada está en el estado $|0\rangle$, la compuerta de Hadamard lo convertirá en el estado $(|0\rangle + |1\rangle)/\sqrt{2}$. Esto significa que el qubit resultante está en un estado superpuesto de los estados $|0\rangle$ y $|1\rangle$, con una probabilidad del 50% de estar en cada uno. (ChatGPT: "Dame ejemplos de compuertas cuánticas". Dic. 2023)

Compuerta CNOT (Controlled NOT)

También conocida como compuerta NOT controlada, es una compuerta cuántica de dos qubits que realiza la operación NOT en el segundo qubit, solo si el primer qubit está en el estado $|1\rangle$.

Matemáticamente, esta se puede representar por la siguiente matriz unitaria

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

que representa la transformación que realiza la puerta CNOT sobre los estados de dos qubits. Si por ejemplo, el primer qubit está en el estado $|0\rangle$ y el segundo qubit está en el estado $|0\rangle$, la puerta CNOT no cambiará el estado del segundo qubit. Sin embargo, si el primer qubit está en el estado $|1\rangle$, la puerta CNOT invertirá el estado del segundo qubit. (ChatGPT: "Dame ejemplos de compuertas cuánticas". Dic. 2023)

Compuerta SWAP

Esta es una compuerta intercambiadora, de dos qubits que intercambia los estados de los qubits.

Esta compuerta se puede representar matemáticamente por la siguiente matriz unitaria:

$$\text{SWAP} = |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|$$

Esta matriz representa la transformación que realiza la compuerta SWAP sobre los estados de 2 qubits. Por ejemplo, si el primer qubit está en el estado $|0\rangle$ y el segundo qubit está en el estado $|1\rangle$, la puerta SWAP intercambiará los estados

de los dos qubits, de modo que el primer qubit quedará en el estado $|1\rangle$ y el segundo qubit quedará en el estado $|0\rangle$. (*ChatGPT: "Dame ejemplos de compuertas cuánticas"*)

Como hemos visto a través de los ejemplos de compuertas cuánticas los estados de los qubits se pueden representar como

$|1\rangle$ y $|0\rangle$

VIII. ARQUITECTURA

Arquitectura de un computador cuántico:

La arquitectura de un computador cuántico se refiere a la forma en que se organizan los qubits y las compuertas cuánticas.

Hay diferentes arquitecturas de computadores cuánticos, cada uno con sus propias ventajas y desventajas.

Arquitectura de circuitos superconductores:

Esta arquitectura utiliza los estados cuánticos de los circuitos superconductores para representar los qubits. Los circuitos superconductores son circuitos eléctricos que se comportan como superconductores a temperaturas muy bajas. En un superconductor, la corriente eléctrica puede fluir sin resistencia. Esto permite que los circuitos superconductores se utilicen para crear qubits muy estables y precisos.

Arquitectura de iones atrapados:

En esta arquitectura, se utilizan iones atómicos atrapados en campos eléctricos y magnéticos para representar los qubits. Los iones atrapados son muy estables y precisos, pero pueden ser difíciles de fabricar y controlar.

Arquitectura de fotones:

Esta arquitectura utiliza los estados cuánticos de los fotones para representar los qubits. Los fotones son muy rápidos y eficientes, pero pueden ser difíciles de controlar y manipular.

Además de las arquitecturas comunes, hay muchas otras arquitecturas en desarrollo. Algunos ejemplos incluyen la arquitectura de defectos de diamante, la arquitectura de qubits topológicos, la arquitectura de qubits moleculares y la arquitectura de puntos cuánticos.

La elección de la arquitectura adecuada para un computador cuántico depende de una serie de factores, como la complejidad del algoritmo, la tecnología disponible y los recursos financieros.

Sistema de control:

Es el sistema que controla el funcionamiento del computador cuántico. El sistema de control se encarga de generar las señales que controlan los qubits y las compuertas cuánticas.

El sistema de control cuántico debe ser capaz de realizar las siguientes tareas:

Iniciar los qubits:

El sistema de control debe ser capaz de inicializar los qubits en un estado conocido y controlado.

Manipular los qubits:

El sistema de control debe ser capaz de manipular los qubits para realizar cálculos.

Leer los qubits:

El sistema de control debe ser capaz de leer los estados de los qubits.

Los sistemas de control de los computadores cuánticos usualmente están formados por los siguientes componentes:

Generadores de señales:

Los generadores de señales se utilizan para generar las señales que controlan los qubits y las computadoras cuánticas.

Amplificadores:

Estos se utilizan para amplificar las señales generadas por los generadores de señales.

Detectores:

Se utilizan para leer el estado de los qubits.

Los sistemas de control están en constante desarrollo y los científicos se mantienen en constante trabajo de desarrollo de sistemas más precisos, eficientes y escalables.

Aquí hay algunos ejemplos de sistemas de control de computadores cuánticos:

El sistema de control del computador cuántico superconductor de Google: Este sistema de control utiliza generadores de señales de microondas para controlar los qubits superconductores.

El sistema de control del computador cuántico de iones atrapados de IBM: Este sistema de control utiliza campos eléctricos y magnéticos para controlar los iones atrapados.

El sistema de control del computador cuántico de fotones de Intel: Este sistema de control utiliza circuitos ópticos para controlar los fotones.

El desarrollo de sistemas de control más avanzados es esencial para el desarrollo de computadores cuánticos más potentes y eficientes.

Sistema de enfriamiento:

Este componente de un computador cuántico es un sistema que mantiene los qubits a temperaturas extremadamente bajas, cercanas al cero absoluto. Esto es necesario para evitar que los qubits pierdan su estado cuántico.

El cero absoluto es la temperatura más baja posible. Se define como la temperatura a la que la energía térmica de un sistema es cero. En la escala Kelvin, el cero absoluto es 0 K, que equivale a $-273,15\text{ }^{\circ}\text{C}$ o $-459,67\text{ }^{\circ}\text{F}$.

Los qubits, que como ya sabemos son las unidades básicas de información en los computadores cuánticos, a diferencia de los bits de los computadores clásicos, estos pueden estar en un estado de superposición de 0 y 1 al mismo tiempo, lo que les permite realizar cálculos mucho más complejos que los computadores clásicos.

Sin embargo, estos son muy sensibles a las perturbaciones externas, como por ejemplo, el calor. Cuando estos están expuestos al calor, pierden su estado cuántico y se convierten en bits clásicos.

Existen a la fecha (2023) dos sistemas principales de enfriamiento para las computadoras cuánticas:

Refrigeración criogénica:

En este tipo de refrigeración se utiliza un refrigerante, por ejemplo el helio líquido, para enfriar los qubits hasta temperaturas cercanas al cero absoluto.

Refrigeración electrónica:

Este tipo de refrigeración utiliza dispositivos electrónicos, como los refrigeradores de efecto Peliter para enfriar los qubits hasta temperaturas bajas, pero no tanto como la refrigeración criogénica.

IX. PROCESADORES CUÁNTICOS

Procesadores cuánticos:

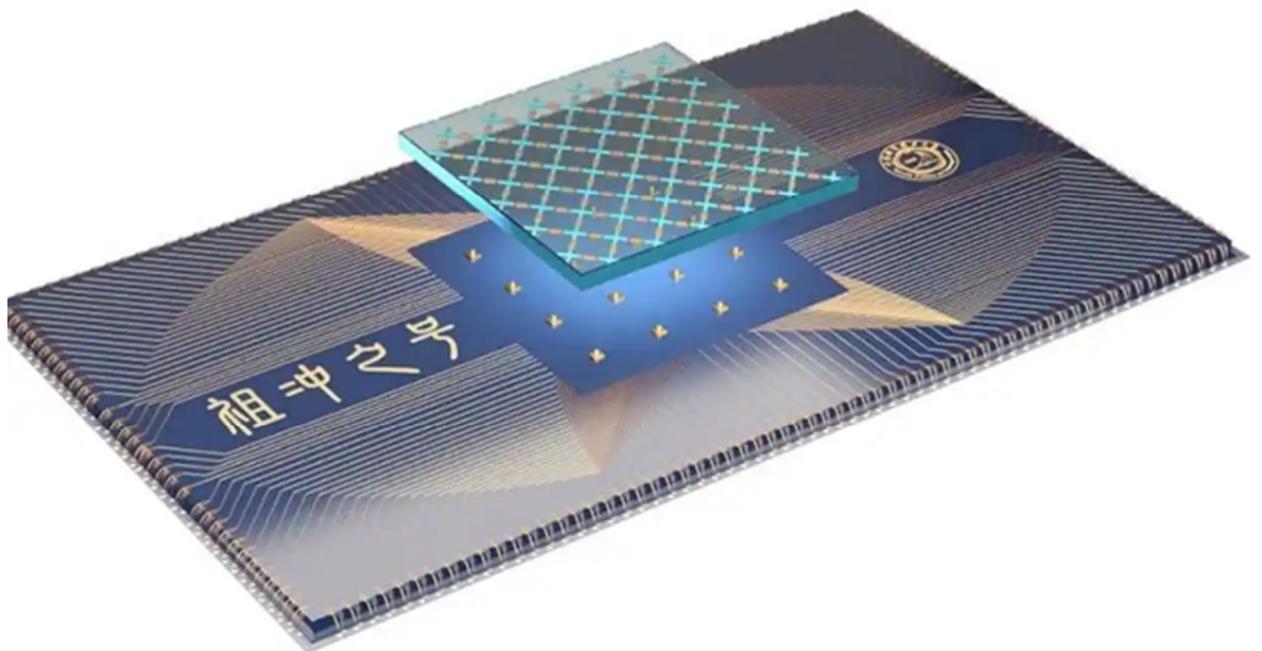
Zuchongzhi: procesador cuántico chino superconductor desarrollado por la Universidad de Ciencia y Tecnología de China, anunciado en 2021 y tiene 66 qubits. El procesador está refrigerado a 10 mK, que es una temperatura cercana al cero absoluto.

En su experimento de demostración, se utilizó para resolver un problema de optimización que requeriría unos 8 años de tiempo de cálculo de un ordenador clásico. Es un problema de optimización combinatoria llamado Ising de 56 qubits, que consiste en encontrar la configuración de 56 qubits que minimice la energía de un sistema de Ising.

Un sistema de Ising es un sistema físico formado por partículas que interactúan entre sí. La energía de un sistema de Ising depende de la configuración de las partículas.

El problema de Ising de 56 qubits es un problema NP-completo, lo que significa que es muy difícil resolverlo en un ordenador clásico.

El problema fue resuelto por Zuchongzhi en 200 milisegundos.



En la imagen anterior se muestra un esquema de diseño del procesador Zuchongzhi (https://www.abc.es/ciencia/abci-china-reclama-supremacia-cuantica-procesador-zuchongzhi-202107180046_noticia.html)

Eagle:

Este es un procesador cuántico superconductor desarrollado por IBM, anunciado en 2021, y tiene 127 qubits.

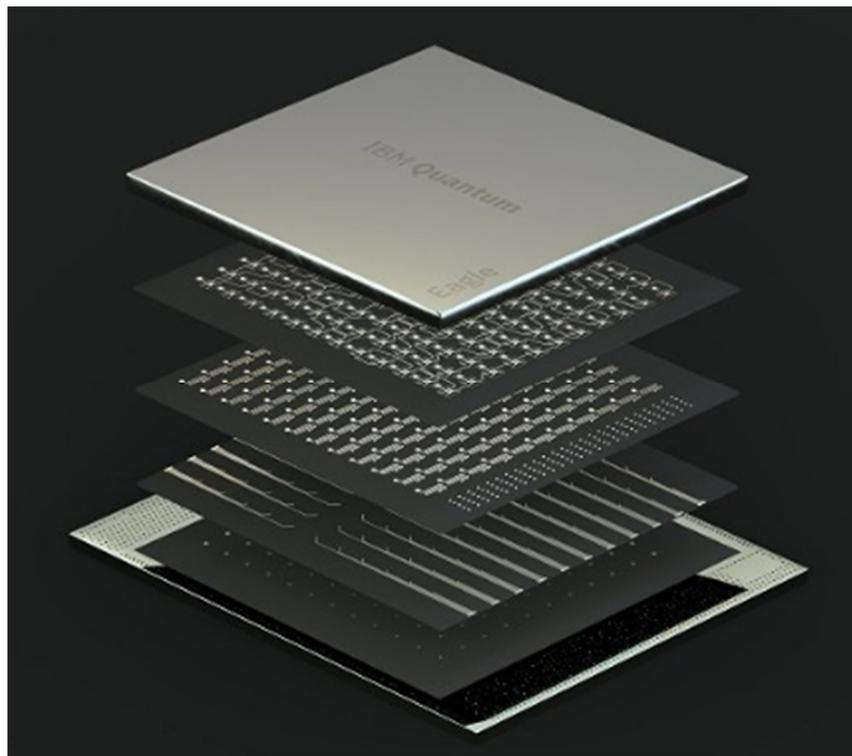
Estos qubits son del tipo de circuitos superconductores, también enfriado a 10 mK. En su experimento de demostración, se utilizó para resolver un problema de optimización que requeriría unos 2 días de tiempo de cálculo en un ordenador clásico.

El experimento realizado y resuelto por Eagle fue el mismo que realizó Zuchongzhi, pero con 127 qubits. El tiempo que tomó para resolverlo fue..... 20 microsegundos.

Es el primer computador cuántico en rebasar la barrera de los 100 qubits.

IBM afirmó que el número de bits clásicos para igualar la potencia de cálculo de este procesador, supera el número total de átomos de la población mundial ($56 \cdot 10^{37}$).

En su diseño, se colocan los componentes de control del procesador en múltiples niveles físicos, mientras que en las configuraciones tradicionales, qubits están ubicados en una sola capa. Esto permite un aumento significativo de la potencia computacional y la coherencia de los qubits.



Esquema del diseño del procesador Eagle. (<https://www.datacenterdynamics.com/es/noticias/ibm-presenta-un-procesador-cu%C3%A1ntico-innovador-de-127-qubits/>)

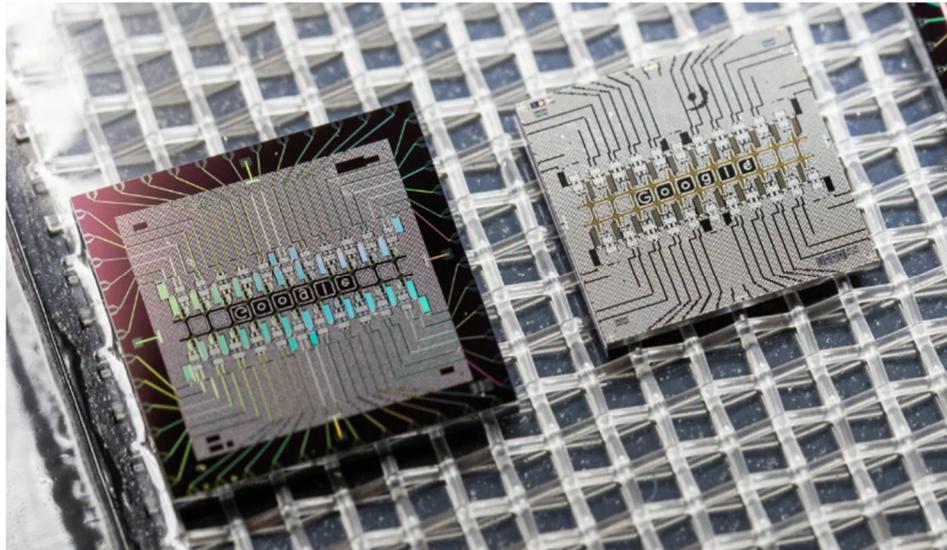
Sycamore:

Es un procesador de Google (en colaboración con IBM). En 2019 se anunció que había logrado una "supremacía cuántica", en la revista Nature.

El término "supremacía cuántica" se refiere al punto en el que una computadora cuántica puede realizar una tarea específica de manera más eficiente que las mejores supercomputadoras clásicas disponibles

Google afirmó que Sycamore completó una tarea en aproximadamente 200 segundos, y calculó que esta le llevaría a una supercomputadora clásica, más de 10,000 años.

La tarea llevada a cabo consistía en hacer un muestreo de circuitos cuánticos aleatorios. Básicamente, Sycamore ejecutó un algoritmo cuántico diseñado para generar secuencias de números aleatorios a partir de la evolución de un conjunto de qubits (53). La tarea por sí misma no tenía aplicaciones prácticas inmediatas, pero la demostración de la supremacía cuántica marcó un avance importante en la capacidad de las computadoras cuánticas para realizar ciertos tipos de cálculos de manera más rápida que las computadoras clásicas. (ChatGPT: "Describe la computadora cuántica Sycamore". Dic. 2023)



Procesador Sycamore. Construido con 2 elementos que se juntan para formar uno solo
(<https://www.cnet.com/pictures/take-a-look-at-googles-quantum-computing-technology/8/>)

IonQ-16:

Este procesador, fabricado por la empresa IonQ, tiene 16 qubits. Su arquitectura está basada en un diseño de iones atrapados, que son átomos cargados eléctricamente que se

mantienen suspendidos en el vacío mediante campos eléctricos y magnéticos. Estos qubits tienen una alta fidelidad y coherencia, lo que significa que las operaciones que se realizan sobre ellos son precisas y fiables.

La coherencia es la propiedad de los qubits de mantener su fase durante un cierto período de tiempo. La fase es un ángulo que determina el estado de un qubit.

Se controla mediante láseres, que se usan para cambiar el estado de los qubits, medir su estado y acoplarlos entre sí. Los láseres permiten implementar compuertas cuánticas universales, que son operaciones lógicas y aritméticas que pueden realizar cualquier cálculo cuántico posible. (Bing).

Los qubits de IonQ-16 son iones de berilio que están atrapados en un campo eléctrico. Los iones se controlan mediante los láseres mencionados en el párrafo anterior y con estos se puede manipular su estado cuántico.

El IonQ-16 tiene una tasa de errores de 0.001%, que es menor que la tasa de errores de otros procesadores cuánticos. Esto significa que el IonQ-16 es más preciso y puede realizar cálculos más complejos, y es menor a la de los otros procesadores cuánticos.

Uno de los avances significativos presentados por este procesador, son sus 16 qubits, lo que es más que cualquier otro procesador cuántico de iones atrapados desarrollados hasta el momento.

Este fabricante también presenta otros modelos de 9, 25, 29 y 35 (2024) y 64 (2025) qubits.

IBM Condor:

Este super procesador cuántico fue anunciado el 4 de diciembre de 2023. Tiene la asombrosa cantidad de 1121 qubits. Es el primer procesador cuántico en rebasar los 1000 qubits.

Utiliza una arquitectura de circuitos superconductores, por lo que requiere una refrigeración de 10mK, muy cercana al cero absoluto.

Es por supuesto, programable, o sea se puede utilizar para muchas tareas diferentes.

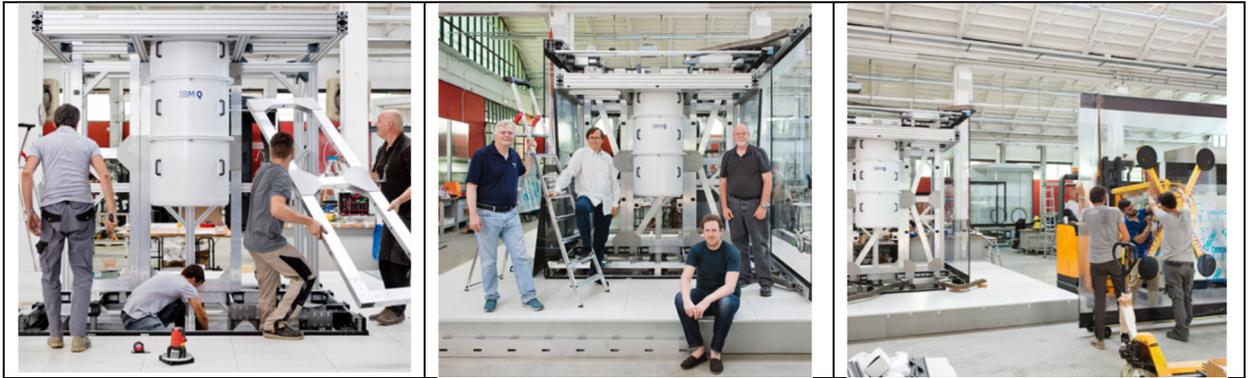
Está construido utilizando una nueva arquitectura tridimensional de IBM que puede respaldar el desarrollo de procesadores cuánticos futuros más avanzados. Esta se basa en un diseño de qubit hexagonal pesado que permite una alta conectividad y una baja tasa de error entre los qubits.

X. COMPUTADORES CUÁNTICOS ACTUALES

Si bien hablamos ya de procesadores cuánticos, es útil y razonable también hablar de sistemas cuánticos completos.

De IBM, la IBM Quantum System One. En su diseño final, incluye un case de 9' x 9' con un grosor de vidrio de borosilicato de media pulgada, presurizada. Marcos independientes de aluminio y acero mantienen la criostática del sistema, electrónica de control, encapsulamiento exterior, ayudando a aislar los componentes de los sistemas para un mejor desempeño. Esta tarea se llevó a cabo con la colaboración de las compañías Map y Goppion.

Tardaron 2 semanas en ensamblar el sistema. Aquí tenemos algunas fotografías



En el verano de 2018, el equipo ensambló el sistema para pruebas mecánicas en los cuarteles generales de Goppion, en Milan.

Y hoy día, se tienen sistemas IBM Quantum System One en lugares alrededor del mundo, empezando por Norte America y Alemania, y próximamente, Japón.

El hardware Quantum de IBM fue diseñado para estabilidad y autocalibración, para mantener desempeño predecible y repetible, con qubits de alta calidad.

Los sistemas criogénicos fueron diseñados con ingeniería para proporcionar temperaturas super frías con una consistencia remarcable, para aislar el ambiente cuántico.

La electrónica de alta precisión de estos sistemas se proporciona en factores de forma compactos para que gran cantidad de qubits pueden controlarse estrechamente con cada demanda.

Una característica muy importante de estos sistemas es que son los primeros sistemas cuánticos que están disponibles para venta al público (por decirlo así) y que puede ser instalado en cualquier lugar. No significa por ejemplo, que una persona pueda pedir un System One por internet. Estos requieren de instalaciones especiales para su mantenimiento e instalación.

Los servicios de estos computadores, también pueden ser utilizados en la nube. Tienen modalidades gratuitas, pagadas (a razón de 1.60\$ el segundo), y planes premium que dependen del uso para su precio.

Estos sistemas en principio poseen 20 qubits. Esto pues no se compara con el poder actual de otros computadores por ejemplo, Intel, con sus computadores de 49 qubits, o el propio IBM con 50 qubits y Google, con 72 qubits. Pero aun así, los 20 qubits serían útiles para la mayoría de los clientes.

Quantum System Two, de IBM:



Anunciada en diciembre de 2023, introduce el uso de 3 procesadores cuánticos Heron, de 133 qubits cada uno. A la fecha (diciembre de 2023) este computador se encuentra en el laboratorio Yorktown Heights, en el estado de New York, en Estados Unidos.

Mide 22 pies de ancho y 12 de alto. Combina infraestructura criogénica con electrónica de control de tercera generación y servidores clásicos.

Esta arquitectura modular presentada por el sistema será utilizada para llevar a cabo ejecuciones de circuitos paralelos para las supercomputadoras cuánticas y permitirá la escalabilidad de procesadores. Además, su arquitectura permitirá que varios sistemas System

Two se puedan unir o entrelazar para poder ejecutar hasta 100 millones de operaciones en un solo circuito cuántico.

IBM espera que para 2025, un solo circuito cuántico sea capaz de procesar 5000 operaciones simultaneas.

Para 2033 se espera que los sistemas sean capaces de ejecutar mil millones de operaciones simultaneas en un solo circuito cuántico.

Sycamore de Google:

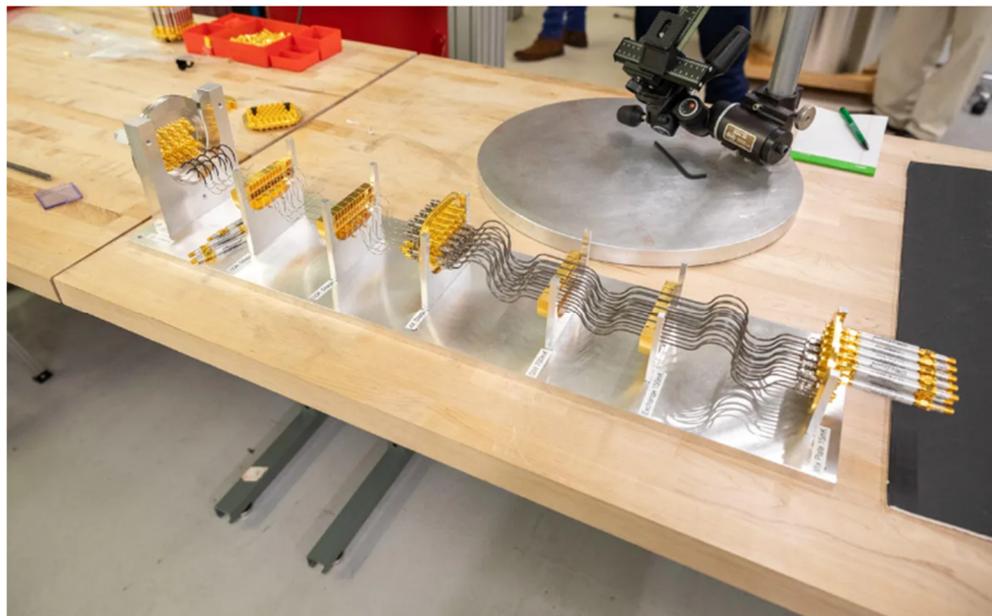
Este computador cuántico fue desarrollado por Google, anunciado en 2019 y logró la supremacía cuántica, es decir, realizó un cálculo que sería imposible para cualquier ordenador clásico.

Contiene 53 qubits, con arquitectura de superconductores que se enfrían a temperaturas cercanas al cero absoluto.

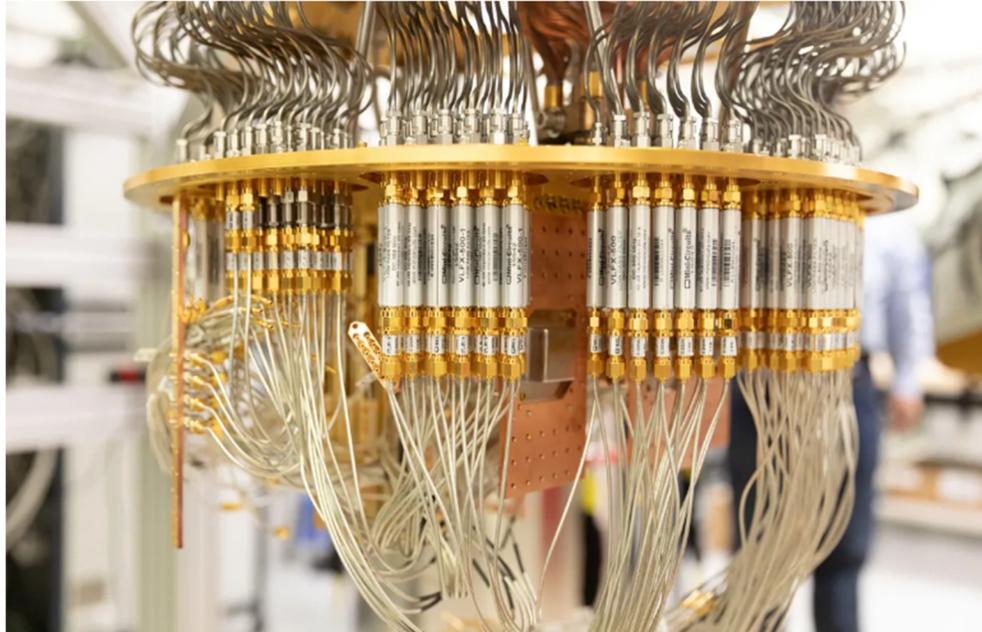
Tiene un sistema de refrigeración, un sistema de control, que envía señales a los qubits para realizar las operaciones.

Tiene un sistema de medición, que mide el estado de los qubits.

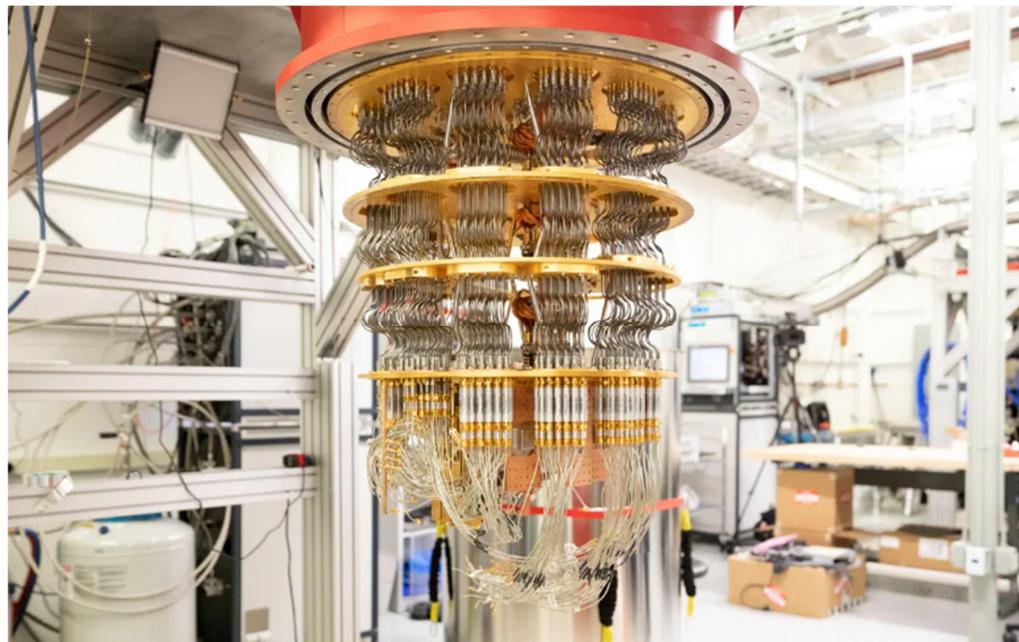
Utiliza 216 canales de cable coaxial para comunicarse con sus qubits. Las líneas de control, que son muy caras, costando alrededor de \$1,000 cada 2 pies de segmento.



En la siguiente fotografía apreciamos líneas que transmiten señales para controlar las computaciones y leer data de los qubits que la procesan.



Está instalado en un laboratorio de Google en Santa Cruz, California.



(Bard: "Describe el computador Sycamore. No solamente el procesador sino todos sus componentes". Dic. 2023)

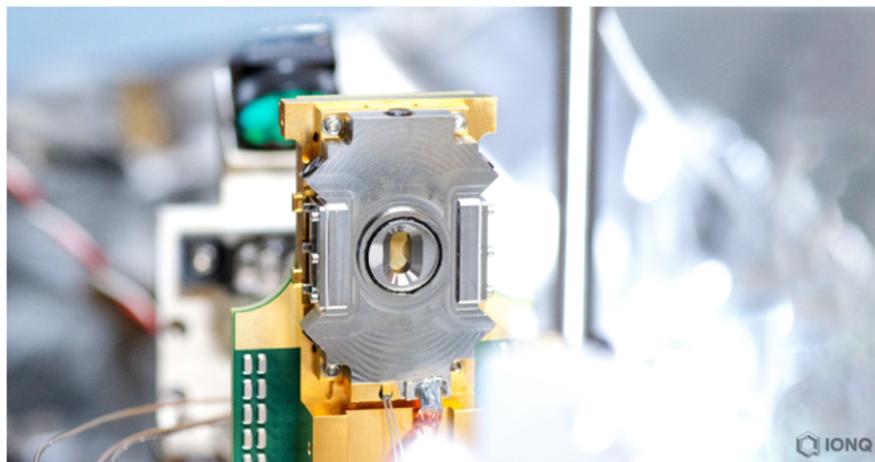
IonQ:

Esta compañía estadounidense, basada en Maryland, posee varios sistemas cuánticos de computo

Los principales sistemas son:

IonQ Harmony. Está disponible comercialmente, posee 11 qubits, con una fidelidad de 97.3%, es accesible a través de Google Cloud Marketplace, Azure Quantum y Amazon Braket. Admite programación en XACC, Pytket, ProjectQ, Pennylane, Cirq, Braket, Q# y Qiskit. Harmony utiliza una versión temprana de la arquitectura de iones atrapados, desarrollada entre 2018 y 2020. Posee mitigación de error y un sistema láser modulador acústico-óptico.

IonQ Aria. Disponible comercialmente, posee 25 qubits, con una fidelidad de 99.4% y mitigación de error y un sistema láser modulador acústico-óptico. Ha estado disponible desde 2022, disponible en la nube de IonQ. Sus 25 qubits implican menor ruido en el sistema cuántico, aún con los problemas más complejos a través de menos iteraciones. La compañía afirma que su arquitectura ha alcanzado el porcentaje más bajo de error de compuertas y mayores tiempos de coherencia de cualquier tecnología cuántica. También posee lo que le llaman "All-to-all connectivity", indicando que cualquier qubit del sistema puede estar entrelazado con cualquier otro qubit del sistema.



IonQ Forte: Posee 32 qubits, con una tasa de fidelidad del 99.6%. Posee un sistema láser de deflector acústico-óptico. Dado que indican que es su mejor sistema, indica la compañía que solo

unos pocos clientes tendrán acceso a ella a partir del 2023. Es la primera computadora cuántica configurable a través de software. Utiliza iones de ytterbio e integra deflectores óptico- acústicos para dirigir los rayos láser a los qubits individuales en la cadena de iones para aplicar las compuertas lógicas entre los qubits.



XI. ALGORITMOS CUÁNTICOS

Algoritmos cuánticos:

Un algoritmo es un conjunto de instrucciones o reglas organizadas de manera lógica y ordenada para resolver un problema. Se trata de una serie de pasos que permiten arribar a un resultado o solución.

En informática, un algoritmo es una secuencia de instrucciones secuenciales que permiten llevar a cabo ciertos procesos.

Otras descripciones de un algoritmo:

- Un procedimiento o fórmula para la resolución de problemas
- Una demostración paso a paso del procesamiento de datos o la resolución de problemas
- Un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema

Un algoritmo cuántico es un algoritmo que se ejecuta en un modelo realista de computación cuántica, como el modelo de circuito cuántico.

La teoría de la complejidad computacional le asigna la clase BQP a los algoritmos que pueden ser resueltos con un computador cuántico en tiempo polinómico con un margen de error promedio inferior a 0.25.

En teoría de la complejidad computacional, BQP (Bounded Error Quantum Polynomial Time) es la clase de problemas de decisión decidibles por un ordenador cuántico en tiempo polinomial con una probabilidad de error de como mucho 1/3 para todas las instancias. Un problema de decisión pertenece a BQP si existe un algoritmo cuántico que resuelve el problema de decisión con alta probabilidad y que se ejecuta en tiempo polinomial.

La teoría de la complejidad computacional es una rama de la teoría de la computación que se centra en la clasificación de los problemas computacionales de acuerdo con su dificultad inherente, y en la relación entre dichas clases de complejidad. Esta teoría se basa en el concepto de modelo de computación, siendo esta una abstracción de una computadora real.

Los modelos más comunes son la máquina de Turing y la máquina RAM.

La dificultad de un problema computacional está medido en función de la cantidad de recursos necesarios para resolverlo, siendo los más importantes el tiempo y la memoria.

Los problemas computacionales se dividen en clases de complejidad, y estos están divididos en dos grupos principales:

Problemas deterministas: Los que pueden ser resueltos por una máquina de Turing determinista.

Problemas probabilísticos: Los que pueden ser resueltos por una máquina de Turing Probabilística.

Las clases de complejidad más importantes son:

P: Los que pueden ser resueltos en tiempo polinomial. Es la clase de los problemas que son computacionalmente fáciles.

NP: Cualquier solución para un problema determinista puede ser verificada en tiempo polinomial. Para estos problemas, existe una verificación eficiente, pero no necesariamente una resolución eficiente.

NP-completos: La clase de problemas NP que son tan difíciles como cualquier otro problema NP. Es la clase de los problemas más difíciles de la clase NP.

Diferencias entre un algoritmo tradicional y uno cuántico:

La principal diferencia es que los algoritmos cuánticos aprovechan las propiedades de la mecánica cuántica para realizar los cálculos de la manera más eficiente.

Los algoritmos tradicionales, a la larga, funcionan con bits, que solo pueden estar en un valor u otro (de un conjunto de 2 valores, digamos, para ejemplificar, 0 y 1, y solo uno de los dos estados).

Los algoritmos cuánticos, por otro lado funcionan con qubits, que pueden estar en una superposición de 2 estados diferentes, digamos 0 y 1.

Otra diferencia entre los 2 tipos de algoritmos es que los algoritmos tradicionales están limitados por lo que se conoce como "la barrera de Landauer" que establece que la energía mínima necesaria para realizar un cálculo es proporcional a la cantidad de información que se está procesando. Esto sin embargo, para los algoritmos cuánticos es completamente superable, lo que les permite realizar cálculos más complejos.

La barrera de Landauer se refiere a un límite teórico en la cantidad mínima de energía requerida para borrar un bit de información en un sistema físico. Esta idea fue propuesta por Rolf Landauer, un físico estadounidense, en 1961. Landauer desarrolló su principio de borrado, que establece que cualquier operación irreversible que borre información debe disipar una cantidad mínima de energía proporcional a la temperatura del sistema y a la constante de Boltzmann.

Ejemplos de algoritmos cuánticos:

- Algoritmo de Shor: Este algoritmo puede factorizar un número primo en un tiempo exponencialmente menor que cualquier algoritmo clásico. Esto tiene implicaciones importantes para la seguridad de los sistemas de cifrado basados en números primos. Fue desarrollado en 1994 por el matemático estadounidense Peter Shor. (Bing: *"Describe el algoritmo de Shor"*). El algoritmo comienza preparando un sistema de qubits en una superposición de 0 y 1 y luego aplica una serie de operaciones cuánticas a los qubits. Estas operaciones cuánticas hacen que los qubits se comporten como si estuvieran representando los números primos que dividen el número N que se desea factorizar. Finalmente, el algoritmo de Shor mide los qubits. Los resultados de la medición revelan los números primos que dividen N. El algoritmo es probabilístico. Esto significa que no siempre da la respuesta correcta. Esta probabilidad, de obtener la respuesta correcta, aumenta con el número de qubits utilizados. Según Bard (*"Describe el algoritmo de Shor"*), el algoritmo de Shor es un algoritmo cuántico para factorizar números enteros en tiempo polinómico. Esto significa que, para un número entero N de L bits, el algoritmo puede encontrar sus factores en un tiempo que es proporcional a L^3 . El algoritmo se basa en la propiedad de que el orden de un número N en el anillo Z_N es igual al producto de todos los divisores primos de N. Por ejemplo, el orden de 5 en el anillo Z_{15} es 10, porque 5 es un divisor primo de 15.

Hay 2 partes principales en el algoritmo de Shor (Bing, *"Describe el algoritmo de Shor"*, *"Shor's Factorization Algorithm"*, [geeksforgeeks.org : https://www.geeksforgeeks.org/shors-factorization-algorithm/](https://www.geeksforgeeks.org/shors-factorization-algorithm/), Dic. 2023)

1. Conversión del problema de factorización al problema de encontrar el período. Esta parte se puede implementar con medios clásicos.
2. Encontrar el período utilizando la Transformada Cuántica de Fourier. Esta parte es responsable de la aceleración cuántica y utiliza el paralelismos cuánticos.

El algoritmo sugiere que la mecánica cuántica, a través de los computadores cuánticos permiten la factorización se realice en un tiempo polinomial, en vez de un tiempo exponencial utilizando computadoras clásicas.

El tiempo de ejecución de este algoritmo en una computadora a clásica es

$$O[\exp(L^{1/3}(\log L)^{2/3})]$$

Mientras que en una computadora cuántica es de

$$O(L^3)$$

La complejidad algorítmica es una medida abstracta de la eficiencia de un algoritmo. Se utiliza para comparar la eficiencia de diferentes algoritmos para el mismo problema.

La complejidad algorítmica se expresa en notación de O grande, que se utiliza para describir el crecimiento de una función en función de su argumento.

Por ejemplo, un algoritmo que tiene una complejidad de $O(n)$ significa que su tiempo de ejecución crece linealmente con el tamaño de la entrada. Un algoritmo que tiene una complejidad de $O(n^2)$ significa que su tiempo de ejecución crece cuadráticamente con el tamaño de la entrada. (Bard: "Cómo se mide la eficiencia de los algoritmos". Dic. 2023)

El algoritmo de Shor funciona de la siguiente manera:

1. Se selecciona el número aleatorio x que no sea divisor de N
2. Se prepara un sistema de qubits en un estado inicial uniforme.
3. Se aplica una serie de operaciones cuánticas al sistema de qubits, que tienen el efecto de preparar el sistema en un estado que representa el orden de x en el anillo Z_N .
4. Se mide el sistema de qubits.

Si el resultado de la medición es un número primo, entonces ese número es uno de los factores de N . Si el resultado de la medición es un número compuesto, entonces se repite el algoritmo con un nuevo valor de x .

Este algoritmo tiene importantes implicaciones para la criptografía. Muchos sistemas de cifrado, como RSA, se basan en la dificultad de factorizar números enteros grandes. Si el algoritmo de Shor se pudiera implementar de forma práctica, estos sistemas de cifrado se volverían vulnerables.

- Algoritmo de Grover: Este algoritmo puede realizar una búsqueda en una base de datos no estructurada. en un tiempo cuadrático, que es un factor de raíz cuadrada más rápido que cualquier algoritmo clásico, es decir $O(\sqrt{N})$, donde N es el número de componentes, y con una necesidad adicional de espacio de almacenamiento de $O(\log N)$. Fue inventado por Lov K. Grover en 1996 y también se le conoce como el "algoritmo de búsqueda cuántica". Esto tiene implicaciones importantes para la búsqueda de información en grandes bases de datos. También es un algoritmo probabilístico, por lo que produce la respuesta correcta con una determinada probabilidad de error, que, no obstante, puede obtenerse tan baja como se desee por medio de iteraciones.

Funciona de la siguiente manera:

1. Se prepara un sistema de qubits en un estado inicial uniforme. El algoritmo comienza en un estado que es una superposición de todos los elementos N . Este estado puede escribirse como:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

Donde

$$|x\rangle$$

Es el estado correspondiente al elemento x

2. Se aplica una operación cuántica llamada reflexión de Grover al sistema de qubits. Este es un operador de difusión que es una operación cuántica que amplifica las amplitudes de los estados que corresponden al elemento marcado. Puede escribirse como:

$$U_s = 2|s\rangle\langle s| - I$$

Donde I es el operador de identidad

3. Se mide el sistema de qubits. El algoritmo mide el estado del sistema. Esto colapsa la superposición y nos da el elemento marcado.

La operación "reflexión de Grover" tiene el efecto de reflejar el estado del sistema de qubits alrededor del estado que representa la entrada buscada. Por lo tanto, después de aplicar la operación, la probabilidad de que el sistema de qubits esté en el estado que representa la entrada buscada se ha duplicado. Iterando el proceso de aplicar la operación de reflexión de Grover y medir el sistema de qubits, la probabilidad de que el sistema de qubits esté en el estado que representa la entrada buscada se acerca a 1.

El algoritmo de Grover podría forzar una clave criptográfica simétrica de 128 bits en aproximadamente

$$2^{64}$$

iteraciones, o bien, una clave de 256 bits en

$$2^{128}$$

Iteraciones. Sin embargo, puede ser que el algoritmo de Grover no represente un riesgo significativamente mayor para la encriptación en comparación con los algoritmos clásicos existentes.

(Bard: "Define el algoritmo de Grover". Bing: "Define el algoritmo de Grover". Dic. 2023)

- Algoritmo de Deutsch-Jozsa: Este algoritmo puede determinar si una función booleana es constante o variable (balanceada) en un tiempo constante, que es imposible para cualquier algoritmo clásico. Fue propuesto por David Deutsch y Richard Jozsa en 1992.

La función binaria es constante si devuelve el mismo resultado para todas las entradas. Una función binaria es balanceada si devuelve 1 para la mitad de las entradas y 0 para la otra mitad.

El algoritmo funciona de la siguiente forma:

1. Se prepara un sistema de qubits en un estado inicial uniforme
2. Se aplica una compuerta cuántica llamada compuerta de Hadamard a cada qubit, formando todas las posibles entradas y un solo 1, que será el qubit de respuesta.
3. Se aplica una compuerta cuántica llamada compuerta de función f a cada qubit. Esta sería una operación XOR del resultado con el qubit de respuesta.
4. Se mide el sistema de qubits. Si el resultado de la medición es 0, entonces la función es constante. Si el resultado de la medición es 1, entonces la función es balanceada.

Este algoritmo es exponencialmente más eficiente que cualquier algoritmo clásico para resolver este problema. Un algoritmo clásico necesitaría evaluar la función para todas las posibles entradas, lo que requeriría un número exponencial de pasos.

Para un algoritmo determinista convencional, se requerirían

$$2^{n-1}$$

evaluaciones de la función en el peor de los casos.

El algoritmo cuántico de Deutsch-Jozsa produce una respuesta que siempre es correcta con solo una evaluación de la función. (Bard, Bing: "define el Algoritmo de Deutsch-Jozsa". Dic. 2023)

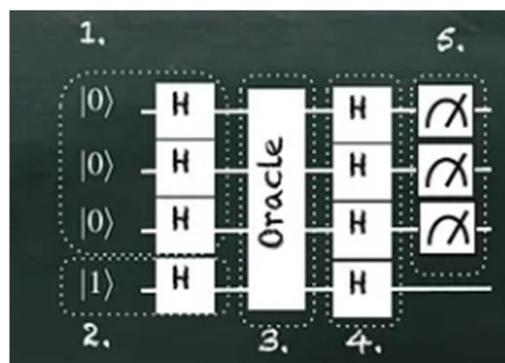
- Algoritmo de Bernstein-Vazirani: Este algoritmo puede determinar el valor de una función booleana que depende de una entrada secreta en un tiempo constante, que es imposible para cualquier algoritmo clásico. Dicho de otra forma, resuelve un problema de búsqueda de una cadena binaria oculta s , a partir de una función booleana $f(x) = s \cdot x$, con una única llamada a un oráculo que calcula la función f .

En computación cuántica, un oráculo es una función matemática que puede ser representada por una compuerta cuántica

El algoritmo funciona de la siguiente manera:

1. Se prepara un registro de n qubits en el estado $|0\rangle$
2. Se añade un qubit auxiliar en el estado $|1\rangle$
3. Se aplica la transformada de Hadamard a cada qubit del registro
4. Se aplica la función $f(x)$ como un oráculo a los qubits del registro, controlada por el qubit auxiliar
5. Se aplica nuevamente la transformada de Hadamard a cada qubit del registro.
6. Se mide el registro de qubits. El resultado de la medición será la cadena binaria s

Aquí tenemos una descripción gráfica de este algoritmo:



(Gráfica creada por Frank Zickert, Quantum Machine Learning en <https://pyqml.medium.com/how-to-implement-the-bernstein-vazirani-quantum-algorithm-with-qiskit-f7e545f99285>)

Encontramos una definición formal matemática en <https://www.mdpi.com/1099-4300/23/7/870> "QKD Based on Symmetric Entangled Bernstein-Vazirani"

- Algoritmo de Simon: Este algoritmo puede determinar si una función booleana es periódica en un tiempo constante, con dos períodos posibles., que es imposible para cualquier algoritmo clásico. Fue propuesto por Daniel R. Simon en 1994.

El problema de la función oculta periódica es el siguiente: Se tiene una función $f(x)$ que es periódica, pero se desconoce el período. La tarea es encontrar el período de la función.

El algoritmo funciona de la siguiente manera:

Se prepara un registro de n qubits en el estado $|0\rangle$

Se aplica una compuerta de Hadamard a cada qubit del registro.

Se aplica el oráculo $f(x)$ al registro, controlado por un qubit auxiliar.

Se aplica una compuerta de Hadamard a cada qubit del registro

Se mide el registro de qubits

El resultado de la medición es un vector de n bits, uno para cada qubit del registro. El período de la función es igual a la longitud del vector de bits que tiene un valor diferente de 0. La ventaja de este algoritmo es que puede resolver el problema de la función oculta periódica en un solo paso, mientras que un algoritmo clásico necesitaría al menos n pasos para resolver el problema, donde n es la longitud del período de la función.

La solución cuántica se puede proponer de la siguiente manera:

Se llevan a cabo $O(n)$ repeticiones de la Rutina Doble de Fourier.

- i. Realizar la transformación F en una cadena de n ceros, produciendo

$$2. \quad 2^{-n/2} \sum_x |x\rangle$$

- i. Calcular $f(x)$, concatenando la respuesta a x , esto produce

$$3. \quad 2^{-n/2} \sum_x |(x, f(x))\rangle$$

- i. Ejecutar F sobre x , produciendo

$$2^{-n} \sum_y \sum_x (-1)^{x \cdot y} |(y, f(x))\rangle$$

Esto finaliza la rutina doble de Fourier.

Luego de estas $O(n)$ repeticiones, se obtienen suficientes valores linealmente independientes de \mathbf{y} que permiten determinar el valor de la cadena \mathbf{s} al resolver el sistema de ecuaciones lineales definido por los valores de \mathbf{y} .

Por lo tanto, la complejidad de todo el algoritmo es

$$O(nT_f(n) + G(n)),$$

Donde

$$T_f(n)$$

Es el tiempo requerido para calcular \mathbf{f} en inputs de tamaño n , y $G(n)$ es el tiempo requerido para resolver el sistema lineal de ecuaciones $n \times n$

Se puede encontrar una definición formal y matemática del algoritmo en https://es.wikipedia.org/wiki/Problema_de_Simon.

(Bard: "Define el algoritmo de Simon", Simon, Daniel R. (1994). "On the Power of Quantum Computation". Dic. 2023)

XII. LENGUAJES DE PROGRAMACIÓN CUÁNTICOS

Lenguajes de programación cuánticos:

Se ejemplificará un programa para el entrelazamiento de 2 qubits

Q # (Microsoft)

Estas son las características principales de Q#

El modelo de datos de qubits y operaciones cuánticas de Q# es una de sus características más importantes. Este modelo proporciona una forma concisa y expresiva de representar los qubits y las operaciones cuánticas. Por ejemplo, un qubit se representa como un tipo de datos llamado Qubit y una operación cuántica se representa como una clase.

Q# también proporciona un ecosistema completo de herramientas de desarrollo que facilitan la creación y depuración de programas cuánticos. El compilador de Q# convierte el código fuente de Q# en un código máquina que se puede ejecutar en un dispositivo cuántico. El depurador de Q# permite a los desarrolladores rastrear el estado de un programa cuántico durante su ejecución. El IDE de Q# proporciona una interfaz gráfica de usuario para escribir, depurar y ejecutar programas cuánticos.

Por último, Q# proporciona una biblioteca de operaciones cuánticas predefinidas que se pueden utilizar para construir circuitos cuánticos. Estas operaciones incluyen puertas cuánticas básicas, como la puerta Hadamard y la puerta CNOT, así como operaciones más complejas, como la puerta de Grover y la puerta de Shor.

En conjunto, estas características hacen de Q# una herramienta poderosa y flexible para la programación cuántica. Q# es una buena opción para los programadores experimentados que quieren comenzar a desarrollar programas cuánticos.

```
// Allocate two qubits
let q1 = Qubit();
let q2 = Qubit();

// Apply Hadamard operation to the first qubit
H(q1);
```

```
// Apply CNOT operation to entangle the qubits
CNOT(q1, q2);

// Measure the qubits (optional)
let result1 = M(q1);
let result2 = M(q2);

// Print the measurement results
Message("Qubit 1: " + result1.ToString());
Message("Qubit 2: " + result2.ToString());
```

Qiskit (IBM)

Qiskit es un entorno (framework) de programación de código abierto de alto nivel diseñado específicamente para el desarrollo de algoritmos y aplicaciones cuánticas. Proporciona una interfaz amigable para interactuar con diversas plataformas de hardware cuántico, permitiendo a los programadores expresar sus algoritmos sin sumergirse en los detalles a nivel de hardware.

Estas son algunas de sus características:

Abstracción: Qiskit oculta las complejidades del hardware cuántico al proporcionar una abstracción de alto nivel para definir circuitos y operaciones cuánticas. Esto permite a los programadores concentrarse en la lógica de sus algoritmos sin preocuparse por los detalles subyacentes del hardware.

Sintaxis similar a Python: "Qiskit utiliza una sintaxis similar a Python, lo que lo hace familiar y fácil de aprender para programadores que ya están cómodos con Python. Esto permite una adopción rápida y reduce la curva de aprendizaje para nuevos usuarios."

Múltiples paradigmas de programación: Qiskit admite estilos de programación tanto imperativo como funcional, atendiendo a las diferentes preferencias de los programadores y permitiendo una mayor flexibilidad en la expresión de algoritmos cuánticos.

Ecosistema rico en herramientas y librerías: Qiskit ofrece un conjunto completo de herramientas y bibliotecas para diversas tareas, incluida la visualización de circuitos, simulación de ruido, corrección de errores y optimización. Esto la convierte en una plataforma potente y versátil para desarrollar y ejecutar aplicaciones cuánticas.

Una comunidad activa y desarrollo: Qiskit cuenta con una comunidad grande y activa de desarrolladores y usuarios que contribuyen al desarrollo continuo del marco y brindan soporte a los recién llegados. Esto garantiza que la plataforma se mantenga actualizada y relevante a medida que evoluciona el campo de la computación cuántica.

Código abierto y de uso libre: Qiskit es un proyecto de código abierto disponible para cualquiera de forma gratuita. Esto fomenta la colaboración y la innovación dentro de la comunidad de la computación cuántica, acelerando el desarrollo de nuevos algoritmos y aplicaciones.

A continuación, presentamos 2 ejemplos: El primero, el código para la implementación del algoritmo de Bernstein-Vazirani de la sección anterior, y el segundo, un programa para el entrelazamiento de 2 qubits.

Ejemplo 1:

```
from qiskit
import
QuantumRegister,
QuantumCircuit

DIGITS = 3

qr = QuantumRegister(DIGITS, "digits")
qc = QuantumCircuit(qr)
```

Ejemplo 2:

```
openqasm 3;
// Allocate two qubits
qreg q[2];

// Apply Hadamard gate to the first qubit
h q[0];

// Apply CNOT gate to entangle the qubits
cx q[0], q[1];

// Measure the qubits (optional)
// Measurement outputs are stored in classical bits c
// Note: Measuring destroys the entanglement
// Replace the following with desired measurements
// measure q[0] -> c[0];
// measure q[1] -> c[1];

// Circuit definition completed
```

Braket (Amazon/IonQ)

Desafortunadamente, por el momento, Braket no tiene un lenguaje de programación nativo como Qiskit y Q#. Sin embargo, se pueden utilizar librerías de Python para ejecutar las funciones.

Si bien Qiskit es un marco bien establecido, Braket es un participante relativamente nuevo en el campo del desarrollo de software cuántico. Comparado con Qiskit, el lenguaje de Braket tiene sus propias características y fortalezas únicas:

Agnóstico respecto al hardware: Significa que se centra en especificar la lógica de los algoritmos cuánticos sin depender de detalles específicos de la plataforma de hardware subyacente. Esto permite que los programas Braket se ejecuten sin problemas en varios backends de hardware cuántico, ofreciendo mayor flexibilidad y portabilidad.

Representación intermedia: En lugar de apuntar directamente a hardware específico, los programas Braket se traducen en una representación intermedia llamada "circuitos Cirq". Luego, los servicios backend de Braket compilan y optimizan estos circuitos para el hardware disponible. Esta separación de las preocupaciones de lógica y hardware simplifica la programación y mejora la compatibilidad.

Estilo funcional: A diferencia de la combinación de estilos imperativos y funcionales de Qiskit, el lenguaje Braket se basa predominantemente en un paradigma de programación funcional. Este énfasis en estructuras de datos inmutables y funciones puras conduce a un código más conciso y predecible, particularmente beneficioso para los algoritmos cuánticos, que pueden ser sensibles a los efectos secundarios.

Corrección de errores incorporada: Braket incorpora soporte nativo para protocolos de corrección de errores dentro de su lenguaje. Esto permite a los programadores integrar fácilmente técnicas de mitigación de errores directamente en sus algoritmos, lo que facilita el manejo del ruido inherente al hardware cuántico.

Enfoque en la seguridad y privacidad: Braket prioriza la seguridad y la privacidad para ejecutar cargas de trabajo cuánticas sensibles. Su lenguaje y servicios incorporan características como aislamiento de trabajos y enclaves seguros para proteger datos confidenciales durante la ejecución del programa.

Integración con AWS: Braket está estrechamente integrado con el servicio Amazon Braket, lo que brinda a los usuarios acceso a una variedad de hardware cuántico de diferentes proveedores a través de una única plataforma. Este enfoque basado en la nube facilita el acceso fácil y la escalabilidad para ejecutar cálculos cuánticos.

Etapa temprana de desarrollo: Es importante tener en cuenta que Braket todavía se encuentra en desarrollo activo y su lenguaje está evolucionando. Si bien ofrece ventajas únicas, es posible que el ecosistema de herramientas y bibliotecas no sea tan maduro como los marcos establecidos como Qiskit.

Este es el código en Python.

```
from braket.circuits import Circuit
```

```

# Create a Circuit with 2 qubits
circuit = Circuit(2)

# Add operations to the circuit
circuit.h(0) # Apply Hadamard gate to qubit 0
circuit.cnot(0, 1) # Apply CNOT gate with qubit 0 as control and
qubit 1 as target

# Print the circuit definition
print(circuit.draw())

```

Cirq (Google)

Cirq tampoco posee un lenguaje nativo, pero también pueden utilizarse librerías de Python para programar:

```

import cirq

# Define two qubits
q1, q2 = cirq.LineQubit.range(2)

# Create a circuit
circuit = cirq.Circuit(
    cirq.H(q1), # Apply Hadamard gate to first qubit
    cirq.CZPowGate(exponent=0.5).on(q1, q2) # Apply controlled-Z
gate (CNOT)
)

# Print the circuit diagram
print(cirq.draw(circuit, show_braces=True))

# Optionally, add measurements for qubit states
# cirq.measure(q1), cirq.measure(q2) would add measurements to the
circuit

```

PennyLane

PennyLane es otro actor intrigante en el ámbito del desarrollo de software cuántico, que ofrece una perspectiva y funcionalidades únicas en comparación con Qiskit y Braket. Estas son algunas de las características clave que distinguen a PennyLane:

Optimización basada en gradientes: PennyLane se destaca por integrarse perfectamente con marcos de diferenciación automática como TensorFlow y PyTorch. Esto permite a los programadores aprovechar potentes técnicas de optimización basadas en gradientes para entrenar y mejorar algoritmos cuánticos, en particular los circuitos cuánticos variacionales (VQC).

VQC significa Circuito Cuántico Variacional, que es un tipo de algoritmo cuántico utilizado en la computación cuántica. La idea básica detrás de VQC es utilizar un

circuito cuántico parametrizado para codificar información sobre un problema y luego optimizar los parámetros del circuito para encontrar la solución al problema.

Diferenciación automática (Autodiff): A través de la integración autodiff, PennyLane calcula automáticamente los gradientes de la función de costo con respecto a los parámetros del circuito. Esto simplifica la optimización de hiperparámetros y facilita el aprendizaje eficiente para los VQC.

Programación híbrida clásica-cuántica: PennyLane fomenta un paradigma de programación híbrido, donde la lógica de control clásica interactúa con operaciones cuánticas dentro del mismo código. Esto permite a los programadores integrar perfectamente algoritmos clásicos y la toma de decisiones dentro de sus algoritmos cuánticos para mejorar la funcionalidad.

Enfoque en aplicaciones de aprendizaje automático: PennyLane ha sido diseñado específicamente teniendo en cuenta las aplicaciones de aprendizaje automático. Proporciona soporte integrado para tareas populares de aprendizaje automático, como clasificación de datos, regresión y aprendizaje por refuerzo, lo que permite a los programadores aplicar fácilmente algoritmos cuánticos a estos dominios.

Interfaz de Python y modular: PennyLane utiliza una sintaxis familiar basada en Python, lo que la hace accesible para programadores que ya se sienten cómodos con Python. Además, su estructura de código modular promueve la reutilización de código y facilita la gestión de circuitos cuánticos complejos.

Código abierto e impulsado por la comunidad: Al igual que Qiskit, PennyLane es un proyecto de código abierto impulsado por una vibrante comunidad de desarrolladores e investigadores. Esto fomenta la colaboración y la innovación, garantizando que el marco siga siendo relevante y evolucione junto con el campo de la computación cuántica.

Enfoque en plataformas de hardware específicas: Mientras obtiene soporte para un acceso más amplio al hardware, PennyLane actualmente se enfoca en integrarse con plataformas de hardware cuánticas específicas como Google Sycamore y Rigetti Aspen. Esta integración profunda puede ofrecer un control y una optimización más detallados para estos dispositivos específicos.

PennyLane también utiliza librerías externas, de Python, por ejemplo.

```
import pennylane as q1

# Define two qubits
q1, q2 = q1.wires(2)

# Create a quantum circuit
with q1.tape() as tape:
    q1.Hadamard(q1) # Apply Hadamard gate to the first qubit
```

```

    ql.CNOT(q1, q2) # Apply CNOT gate to entangle the qubits
# Get the circuit as a function
circuit = tape.compile()
# Simulate the circuit and get statevector
simulator = ql.MPSolver()
probs = simulator.sample(circuit, shots=1000)
# Print the most frequent probabilities
print(f"Probabilities after entanglement:")
for i, prob in enumerate(probs.most_frequent()):
    binary_string = f"{q1}{q2} = {i:b}"
    print(f"{binary_string}: {prob * 100:.2f}%")

```

ProjectQ (ETH Zurich)

ProjectQ es un lenguaje de programación cuántica menos conocido pero fascinante con características y principios de diseño únicos. Aquí hay un desglose de sus características clave:

Estilo declarativo: A diferencia de la mayoría de los lenguajes cuánticos que utilizan programación imperativa (instrucciones paso a paso), ProjectQ adopta un estilo declarativo. En lugar de especificar explícitamente las operaciones de puerta, los usuarios definen las propiedades y relaciones deseadas entre los qubits, y ProjectQ sintetiza automáticamente las operaciones de circuito necesarias. Esto puede generar un código más conciso e intuitivo, especialmente para algoritmos complejos.

Abstracción de alto nivel: ProjectQ proporciona abstracciones de alto nivel para conceptos cuánticos comunes como estados, mediciones y operaciones. Esto simplifica la programación al ocultar los detalles de bajo nivel de la manipulación de qubits y permitir a los usuarios centrarse en la lógica de sus algoritmos.

Optimización automática de circuitos: ProjectQ optimiza automáticamente los circuitos generados para lograr eficiencia y rendimiento. Esto reduce la sobrecarga de la optimización manual y garantiza una ejecución eficiente en el hardware disponible.

Componibilidad y reutilización: ProjectQ fomenta la modularidad y la reutilización del código a través de bloques cuánticos componibles. Estos bloques encapsulan operaciones cuánticas comunes y pueden combinarse para construir circuitos más grandes y complejos. Este enfoque simplifica la organización del código y promueve el desarrollo eficiente de algoritmos.

Extensible y de Código Abierto: ProjectQ es un framework de código abierto con una arquitectura modular. Esto permite a los usuarios ampliar el lenguaje con puertas, algoritmos y backends personalizados para la integración con plataformas de hardware específicas. Esta flexibilidad permite a los desarrolladores adaptar el marco a sus necesidades específicas y mejorar las capacidades del lenguaje.

Enfocado en la investigación y desarrollo: ProjectQ se desarrolló inicialmente con un fuerte enfoque en la investigación y la educación. Ofrece documentación intuitiva, tutoriales y herramientas educativas, lo que lo hace accesible para estudiantes e investigadores cuánticos.

ProjectQ, como los anteriores frameworks que hemos visto, no tiene un lenguaje nativo dedicado. Este ofrece una interfase basada en Python, para construir y manipular los circuitos, utilizando compuertas y operaciones.

```
from projectq import *

# Initialize the ProjectQ engine
engine = LocalSimulator()

# Define two qubits
q1 = allocate(engine)
q2 = allocate(engine)

# Build the quantum circuit
with EngineMode(engine):
    H(q1)
    CNOT(q1, q2)

# Run the circuit and get the statevector
all_measurements = get_shots(engine, [q1, q2], num_shots=1000)

# Analyze the measurement results
counts = defaultdict(int)
for i in range(len(all_measurements)):
    counts[tuple(all_measurements[i])] += 1

# Calculate and print the probabilities
for bitstring, count in counts.items():
    probability = count / len(all_measurements)
    print(f"Qubit states {bitstring}: {probability:.4f}")

# Release the qubits
```

```
del q1, q2  
  
# Stop the engine  
engine.stop()
```

Pytket (Cambridge Quantum Computing)

Pytket adopta un enfoque único para la programación cuántica, centrándose en la construcción y optimización de circuitos a un nivel alto en lugar de la manipulación a un nivel bajo de compuertas. Aunque no cuenta con un lenguaje "nativo" dedicado como Qiskit o Q#, su interfaz en Python ofrece una forma potente y concisa de construir y manipular circuitos cuánticos.

Estas son algunas de sus características:

Abstracción de alto nivel: Pytket proporciona un alto nivel de abstracción en comparación con otros lenguajes de programación cuántica, lo que permite a los programadores centrarse en la lógica de sus algoritmos cuánticos sin atascarse en los detalles de bajo nivel de cómo se implementan en hardware específico. Esto hace que sea más fácil escribir y razonar sobre programas cuánticos.

Modelo basado en circuitos: Pytket utiliza un modelo basado en circuitos para representar programas cuánticos. Esto significa que los algoritmos cuánticos se expresan como una serie de puertas que se aplican a los qubits, las unidades básicas de información cuántica. Este modelo se utiliza ampliamente en el campo de la computación cuántica y resulta familiar para muchos programadores cuánticos.

Estilo declarativo: los programas Pytket están escritos en un estilo declarativo, lo que significa que especifican lo que debe hacer el programa sin especificar explícitamente cómo debe hacerse. Esto hace que los programas Pytket sean más concisos y fáciles de leer que los programas escritos en lenguajes imperativos.

Elementos de programación funcional: Pytket incorpora algunos elementos de programación funcional, como la inmutabilidad y funciones de orden superior. Esto puede hacer que los programas Pytket sean más modulares y más fáciles de probar.

Admite múltiples backends de qubits: Pytket se puede utilizar para apuntar a una variedad de backends de qubits diferentes, incluidos simuladores, computadoras cuánticas basadas en la nube y computadoras cuánticas locales. Esto lo convierte en una herramienta versátil para desarrollar y ejecutar algoritmos cuánticos.

Diferenciación automática: Pytket puede diferenciar automáticamente circuitos cuánticos, lo que significa que puede calcular el gradiente de una función con respecto a los parámetros del circuito. Esto es útil para optimizar algoritmos cuánticos.

Corrección de errores: Pytket admite una variedad de técnicas de corrección de errores que pueden ayudar a mitigar los efectos del ruido y los errores en las computadoras cuánticas.

Herramientas de visualización: Pytket proporciona una serie de herramientas para visualizar circuitos cuánticos, que pueden ayudar a que sean más fáciles de entender y depurar.

Veamos cómo crear dos qubits entrelazados en Pytket:

```
from pytket import Circuit, Op, Qubit
# Define two qubits
q1 = Qubit(0)
q2 = Qubit(1)
# Create a Hadamard operation on the first qubit
h = Op.H(q1)
# Create a CNOT operation with q1 as control and q2 as target
cnot = Op.CNOT(q1, q2)
# Build the circuit
circuit = Circuit(h, cnot)
# Print the circuit diagram
print(circuit.draw())
# Optionally, simulate the circuit and analyze the state
# Pytket integrates with various simulators and backends for this
purpose
```

XIII. EXPECTATIVAS FUTURAS

Expectativas futuras:

IBM planea para el 2025 lanzar al mercado un computador cuántico con más de 4000 qubits, con un procesador Heron, con arquitectura mejorada de acoplamiento ajustable, y diseño modular.

También en 2024, IBM planea lanzar Crossbill. Este es un procesador cuántico de 408 qubits basado en tecnología superconductora. Tiene 3 microchips, cada uno formado por 136 qubits. Estos están fabricados con un nuevo diseño que mejora la fidelidad y la fiabilidad con tasas de 99.9% y 99.999% respectivamente.

La fidelidad es una medida de la probabilidad de que un qubit se encuentre en el estado correcto. La fiabilidad es una medida de la probabilidad de que un qubit no se vea afectado por errores.

Flamingo, que se espera que sea lanzado en 2024 es un procesador cuántico con 462 qubits, basado también en tecnología superconductora y utiliza un nuevo diseño de qubit que mejora la fidelidad. Una característica importante de este procesador es que posee un enlace de comunicación cuántico integrado. Se planea hacer una demostración de esta arquitectura con tres procesadores Flamingo para formar un sistema de 1386 qubits.

Para 2025, también planea lanzar Kookaburra, un procesador cuántico de por lo menos 4158 qubits que utiliza un nuevo diseño de interconexión que permite escalar el número de qubits.

Crossbill será un procesador de 408 qubits, diseminados en tres microchips, y Flamingo serán un módulo de 462 qubits que planea unirlos entre sí mediante una comunicación cuántica de un metro de extensión.

En mayo de 2023, IBM lanzó la noticia de que comenzaría a proveer de mayor velocidad y calidad a sus computadoras cuánticas, mediante una capa de *orquestración de software inteligente*, que pudiese superar los retos de infraestructura y distribuir las cargas de trabajo. Por lo tanto, se centra un hardware cuántico robusto y escalable.

Lo que pretende IBM es crear supercomputadoras cuánticas. Estas supercomputadoras incorporarán procesadores cuánticos, procesadores clásicos, redes de comunicación cuántica y redes clásicas, todas trabajando juntas para completar la transformación y seguir con el avance de la computación.

Parte de este reto, indica IBM es resolver los retos de escalabilidad de los procesadores cuánticos, así como desarrollar un ambiente de tiempo real para proveer cálculos cuánticos con velocidad y calidad agrandada, aparte de introducir un modelo de programación que no utilice

servidores y permitir que procesadores cuánticos y tradicionales puedan trabajar juntos sin ningún tipo de fricción.

Google Sycamore:

Escalabilidad: El camino de Google apunta al dramático incremento del número de qubits en sus procesadores. Su objetivo ambicioso es alcanzar el procesador con 1 millón de qubits para el año 2029.

Coherencia y corrección de errores: Mantener la coherencia y fidelidad de los qubits en largos períodos de tiempo es crucial para la exactitud de los cálculos computacionales. Google está activamente desarrollando importantes técnicas de corrección para afrontar este reto.

Ecosistema de software cuántico: Google reconoce la necesidad de un ecosistema de software robusto para soportar la adopción más amplia de la computación cuántica. Esto incluye el desarrollo de herramientas para programación, debugging y optimización de algoritmos cuánticos.

El futuro de Google en los procesadores cuánticos es brillante, guiado por una combinación de investigación innovadora, objetivos ambiciosos y enfoque en aplicaciones prácticas. A medida que la tecnología madure y los retos puedan ser resueltos, podríamos esperar ser testigos de avances revolucionarios en varios campos, transformando todo el paisaje de la computación y la tecnología.

IonQ-32:

Este procesador continúa con la línea de iones atrapados y tiene 32 qubits. Fue anunciado en agosto de 2023, y al momento, es el procesador cuántico de iones atrapados más potente del mundo.

Estos son iones de berilio atrapados en un campo eléctrico, controlados por rayos láser.

Posee una tasa de errores de 0.001%, que es menor a la tasa de errores de otros procesadores cuánticos, con una tasa de fidelidad de las compuertas mayor a 99%.

Su tiempo de coherencia es mayor a 10 milisegundos.

Es escalable por medio de la adición de más iones.

Este procesador está disponible a través de la plataforma de nube de la compañía IonQ.

La compañía está trabajando en el desarrollo de la nueva generación de procesadores cuánticos de iones atrapados llamados IonQ-1000. Este tendrá 1000 qubits y será capaz de resolver problemas que para una computadora clásica es prácticamente imposible.

XIV. CONCLUSIONES

Es innegable que las necesidades mundiales cada día requieren más y más participación de los elementos electrónicos de pequeña y gran escala para la fabricación de dispositivos.

Estos dispositivos son tan simples como un transistor y tan complejos como supercomputadoras.

Y dentro de estas supercomputadoras se encuentran las computadoras cuánticas. Estas computadoras serán capaces de realizar tareas que aun para las supercomputadoras convencionales sería casi imposible en términos de unidades de tiempo. Hablamos de cientos o miles de años que le tomaría a una computadora convencional para realizar ciertas tareas, contra las horas o minutos que una computadora cuántica utilizaría.

Cabe mencionar también que la supremacía de los computadores cuánticos, no es absoluta. Se ha demostrado recientemente que algunas supercomputadoras convencionales han sido capaces de llevar a cabo las mismas tareas que un computador cuántico en tiempos razonablemente comparables. Sin embargo, a pesar que el poder de cómputo de ambos tipos de computadores podría ser similar, la cantidad de potencia (eléctrica) que necesitan los computadores convencionales es muchísimas veces más grande que un computador cuántico, en el que la mayoría de la potencia requerida, se utiliza en el enfriamiento de los componentes cuánticos, mientras que las supercomputadoras requieren esta potencia para manejar los componentes (procesadores) y los sistemas en enfriamiento, a gran escala física. (ver fotografías de las secciones de antecedentes y computadores cuánticos).

Actualmente Estados Unidos, China, Alemania, Japón, Países Bajos, Reino Unido, Francia, Canadá, Australia, India, Rusia y Corea del Sur tienen computadores cuánticos o tienen proyectos de fabricación de los mismo, tanto en proyectos gubernamentales como privados, y algunos en colaboración de ambos.

A medida que pasa el tiempo y las necesidades aumentan, el desarrollo de estos proyectos avanza y la disponibilidad de los equipos cuánticos ya no es exclusiva para sus desarrolladores o fabricantes, sino que está disponible para el público por medio de servicios en la nube, lo que seguramente agilizará la oferta y el abaratamiento de estos servicios.

Se espera que el estudio aquí presentado pueda ser tomado como base para estudios avanzados en el área de la computación cuántica.