Computación clásica y cuántica (JM Barandiaran 2025)

Hoy día no podemos imaginar la vida sin la ayuda de un ordenador o computador, sea en el trabajo, en casa o en cualquier situación. Nuestro teléfono móvil es un computador de potencia inimaginable para cualquier persona (incluidos científicos punteros) hace 50 años. Podemos imaginar la vida sin gasolina (todo o casi todo eléctrico), sin aviones y hasta sin Amazon, pero no sin teléfono móvil o sin ordenador. Sin embargo, la capacidad de los ordenadores se acerca a un límite que no vamos a poder superar si continuamos utilizando la misma tecnología y los mismos fundamentos que rigen para los computadores actuales, basados en la física clásica o "macroscópica". La Física Cuántica, que comenzó ya hace más de 100 años, puede ser una alternativa para superar las actuales barreras de cálculo, con lo que sería la Computación Cuántica (QC de sus siglas en inglés)

1.- Computación clásica

Los ordenadores actuales son máquinas que utilizan elementos clásicos, es decir obedecen las leyes de la mecánica, termodinámica y electromagnetismo de cuerpos compuestos de muchos átomos (macroscópicos). Aún cuando puede parecer que hay muchos tipos distintos de ordenadores o computadoras, todos ellos se basan en principios comunes, establecidos hace mucho por los científicos de la Información y, en concreto, por Alan Turing, que describió lo que llamamos la Máquina Universal de Turing, capaz de realizar cualquier tarea que realiza ahora una computadora.

1.1.- La Máquina Universal de Turing

Una máquina de Turing es un modelo conceptual de ordenador, que se puede reducir a un dispositivo mecánico (figura 1) compuesto por:

- **Una cinta**, potencialmente infinita, dividida en celdas, o "bit"s, que contienen un carácter (0 o 1) cada una, y **un cabezal** que se puede mover sobre la cinta y puede leer, borrar y escribir en ella.
- Un manual de instrucciones o "**programa**" para operar el cabezal.

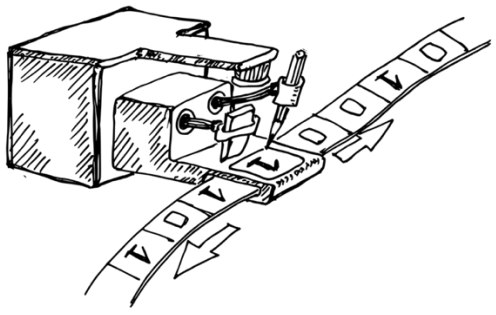


Figura 1.- *Máquina de Turing. El cabezal es el equivalente a la CPU (Unidad de Control de Procesos) de los ordenadores. La cinta sería la memoria de trabajo*

En principio la cinta podría contener muchos más símbolos que el 0 y el 1, pero todos ellos se podrían codificar en sistema binario, por lo que lo más simple es usar solamente esos dos. Igualmente, el "programa" puede ser codificado en binario y constar solamente de 0's y 1's escritos en otra cinta.

Situación inicial: La lista inicial de símbolos de la cinta constituye la "entrada" de la máquina

Al principio, el cabezal de lectura/escritura está situado sobre la celda más a la izquierda de la cinta y se encuentra en un estado $\mathbf{q_0}$

¿Cómo funciona una Máquina de Turing?: Estando en un estado **q**, sobre una celda cualquiera de la cinta, la cabeza de lectura/escritura realiza las siguientes operaciones en la celda.
a) Lee el símbolo que está escrito en la celda.
b) Pasa al nuevo estado **q'**, que indica el "programa" (que dependerá del estado anterior y del símbolo leído),
c) Borra el símbolo que hay en la celda y escribe el nuevo símbolo que corresponde a **p'** (aunque puede ser el mismo que había antes en la celda).
c) Mueve la cabeza de lectura/escritura (o la cinta) a izquierda o derecha, según indique el estado **p'**, o bien se para y da por terminado el proceso.
Cuando se para, el contenido de símbolos de la cinta constituye la "salida" de la máquina. Existen muchas variantes de la Máquina de Turing, pero todas ellas son equivalentes a la que hemos descrito. **Una máquina de Turing puede resolver cualquier problema que pueda ser descrito por un algoritmo (el programa),** por eso se llama máquina universal.

Una posible máquina de Turing sería una persona con una cinta escrita con ceros y unos, una goma de borrar y un lápiz, y un manual que indica qué hacer en cada situación. Este dispositivo, sin embargo, es muy lento. Una mecanización de las tareas de la máquina de Turing se llevó a cabo, primero, con interruptores electromecánicos, luego con válvulas de vacío, más tarde con transistores y otros componentes electrónicos discretos, montados sobre un circuito impreso, y finalmente, con los componentes electrónicos integrados en un solo circuito o "chip" de silicio. El primer circuito integrado fue construido en 1958 por Jack S. Kilby, que recibió el Premio Nobel de Física en el año 2000.
Todos los ordenadores actuales constan de circuitos integrados que trabajan sobre los dígitos binarios 0 y 1 (bits), a su vez materializados por componentes electrónicos, algunos de cuyos principios básicos se muestran en la figura 2. Sea cual sea su origen , los bits se trasladan o "circulan" por un ordenador como estados de voltaje en sus circuitos: 0*Volt*= bit 0, 1*Volt* (u otro valor) = bit 1

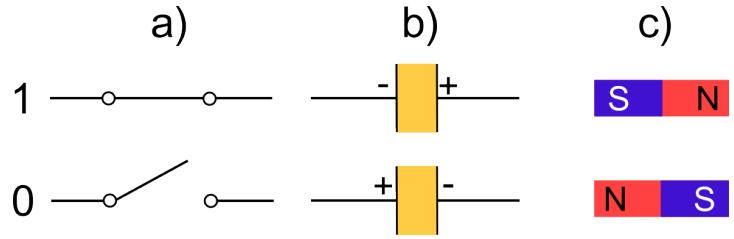


Figura 2.- *Posibles realizaciones físicas de los "bits" de una máquina de Turing, en un ordenador electrónico a) un interruptor abierto (no pasa corriente= 0) o cerrado (deja pasar la corriente =1). Estos interruptores son ahora transistores; b) un condensador cargado con polaridad +,– (0) o –,+ (1) un pequeño imán (un sector de un disco duro, por ejemplo) imanado en dirección Norte-Sur (0) o Sur-Norte (1). En los dos últimos casos, la elección de los estados 0 y 1 es arbitraria*

Puertas lógicas: Las operaciones lógicas y aritméticas sobre los bits se realizan mediante complicados circuitos electrónicos. A pesar de su complejidad, todos estos circuitos pueden construirse como combinaciones de unos pocos circuitos llamados "puertas" lógicas. Las puertas reciben entradas binarias (0,1) y producen una salida, también binaria, dada por unas tablas lógicas, o "tablas de verdad" y se representan por símbolos estándar, figura 3.

Puerta SI	
Entrada	Salida
0	0
1	1

Puerta NO	
Entrada	Salida
0	1
1	0

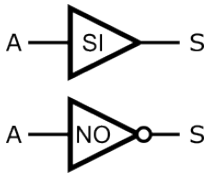
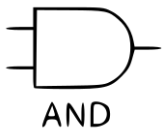
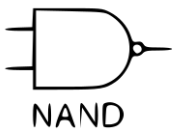


Figura 3a.- *"Tablas de verdad" y símbolos de puertas lógicas de una sola entrada, cuyos valores figuran en las celdas azules. Las correspondientes salidas figuran en las celdas blancas. La puerta SI, deja la entrada igual y la puerta NO (NOT) la invierte*

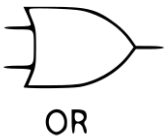
Puerta AND (Y)		
A / B	0	1
0	0	0
1	0	1



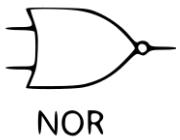
Puerta NAND		
A / B	0	1
0	1	1
1	1	0



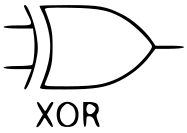
Puerta OR (O)		
A / B	0	1
0	0	1
1	1	1



Puerta NOR		
A / B	0	1
0	1	0
1	0	0



Puerta XOR		
A / B	0	1
0	0	1
1	1	0



Puerta XNOR		
A / B	0	1
0	1	0
1	0	1

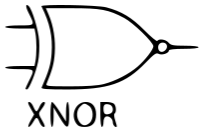


Figura 3b.- *"Tablas de verdad" y símbolos de puertas lógicas con dos entradas (A y B) cuyos valores figuran en las celdas azules. Las salidas figuran en las celdas blancas. La puerta AND(Y), por ejemplo, solamente saca un 1 cuando ambas entradas son un 1. La puerta OR(O) saca un 1 cuando cualquiera de las entradas, o las dos, es un 1. La puerta NOR es la negación de la OR y su salida es un 1 solo cuando ninguna de las entradas es 1.*

Todas las operaciones aritméticas y lógicas pueden llevarse a cabo combinado solo tres de las puertas descritas, lo que se llama un "conjunto de puertas universal". Cada una de las puertas lógicas están, a su vez, formadas por componentes electrónicos elementales, tales como resistencias, diodos y transistores, integrados sobre silicio, en un "chip". Algunos de estos circuitos, que pueden ser muy sencillos, o no tanto, se representan en la figura 4.

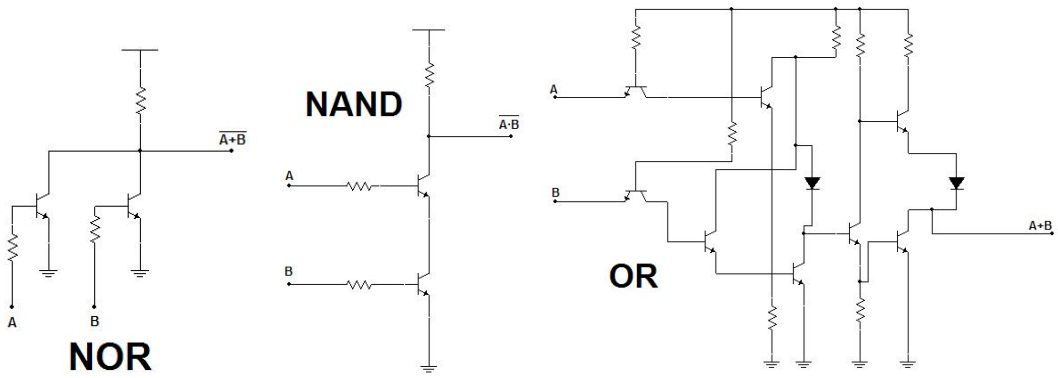


Figura 4.- *Circuitos de puertas lógicas formadas por componentes elementales: resistencias, diodos y transistores.*

1.2.- Ley de Moore

La tecnología microelectrónica se ha desarrollado de manera exponencial desde la aparición de los circuitos integrados (chips) a finales de los años 60 del s XX. El número de transistores por "chip" (o por mm^2, como se muestra en la figura 5) ha crecido de manera exponencial hasta hoy en día, doblándose cada aproximadamente dos años, y pasando de unos 100 transistores/mm^2 en 1970 a 100 millones en 2020. Este crecimiento rápido y sostenido durante más de 50 años es lo que se denomina la Ley de Moore, pues fue Gordon Moore, cofundador de *Fairchild Semiconductors* e *Intel* y luego director de *Intel*, quien la formuló allá por 1965, al comienzo de la Era electrónica. El rapidísimo aumento de densidad de los chips es posible gracias a las técnicas de miniaturización que han permitido disminuir el tamaño de los componentes electrónicos (en concreto los transistores) hasta dimensiones infinitesimales.

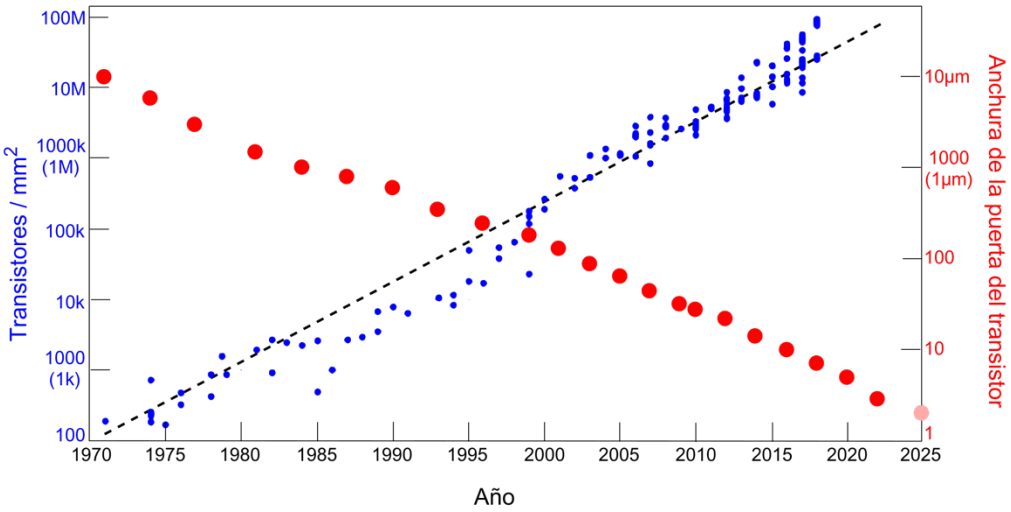


Figura 5.- La Ley de Moore. *En la escala izquierda se muestra el aumento del número de transistores por milímetro cuadrado a lo largo del tiempo (puntos azules). Obsérvese la escala logarítmica, en la que cada división supone multiplicar por 10 la anterior. La escala derecha y los puntos rojos indican cómo ha ido disminuyendo las dimensiones de la "puerta" de un transistor en esos mismos años, medida en nanómetros, es decir en millonésimas de milímetro. La reducción del tamaño de los componentes es la que ha permitido, hasta ahora, el aumento de la densidad de componentes en los chips. (datos de la Wikipedia)*

Los primeros chips de ordenadores, allá por el año 1968, tenían transistores cuya "puerta" (la parte más pequeña y precisa del mismo, que permite o no el paso de corriente) era ya de solo unas 20 micras (µm) de anchura (menor que el grosor de un cabello humano). El año que viene (2025) la puerta de un transistor de silicio será de solo 2 nanómetros (nm), es decir, 10.000 veces más pequeña, y apenas tendrá 9 átomos de espesor. Está claro que este tamaño no puede seguir disminuyendo indefinidamente pues llegaremos rápidamente a dimensiones inferiores a la de los átomos. Podríamos aumentar la densidad de transistores, sin disminuir su tamaño, apilándolos en varias capas, aunque se complica muchísimo su procedimiento de construcción y la refrigeración de los circuitos, por lo que también llegaríamos en poco tiempo, a un límite físico infranqueable. Por lo tanto, la potencia de cálculo de los ordenadores tiene un límite cercano que no ya no podrá superar. De hecho, los superordenadores actuales ya ocupan tanto, y consumen tanta energía, como los primeros ordenadores, que funcionaban con válvulas de vacío, antes de aparecer los transistores y los circuitos integrados.

¿Podremos limitarnos a la potencia de cálculo actual para siempre?: La respuesta es que no, claro. Siempre aparecen necesidades mayores. No me refiero a nuestro ordenador portátil o a nuestro teléfono móvil, que tienen ya capacidades más que suficientes para

cualquier necesidad personal privada. Lo que nos reta ya hoy mismo son cosas mayores: los cálculos meteorológicos, la Inteligencia Artificial, la medicina personalizada, la encriptación y seguridad de nuestros datos, etc., requieren cada vez de más potencia de cálculo. Incluso problemas que parecen sencillos en principio, como los que veremos ahora, resultan imposibles de resolver en los ordenadores actuales y futuros, si seguimos utilizando la misma tecnología.

1.3.- Problemas "intratables"

El problema del viajante es un problema clásico de optimización, muy importante en ciencias de la computación. Se plantea de la siguiente forma, al parecer muy sencilla:
Dada una lista de ciudades y las distancias entre cada par de ellas, ¿cuál es la ruta más corta posible que visita únicamente una vez cada ciudad y regresa al final a la ciudad de partida?
Pero es claramente un problema de combinatoria que crece exponencialmente con el número de ciudades a visitar. Si hay N ciudades, habrá N! rutas para recorrer entre ellas (siendo N! = Nfactorial = N x (N-1) x (N-2)... x 2 x 1). Se puede simplificar un poco el problema, ya que nos da igual el punto de partida y la dirección en que se recorra la ruta. Así todo, con 5 ciudades habría 12 rutas diferentes. Aún no hace falta un computador para analizarlas. Con 10 ciudades el número de rutas diferentes es ya: 181.440. Ahora ya si que vamos a necesitar el ordenador. Para 30 ciudades hay más de $4 \cdot 10^{30}$ rutas posibles, y ya no hay ningún ordenador que pueda resolver el problema. En efecto, un ordenador que calcule un millón (10^6) de rutas por segundo, necesitaría 10^{17} años para resolverlo, por lo que, si hubiera comenzado a calcular en el Big Bang, hace unos 14.000 millones de años ($1{,}4 \cdot 10^{10}$) todavía no habría calculado ni una millonésima parte de las rutas entre las 30 ciudades. Este problema es, por tanto, intratable incluso por un supercomputador que utiliza algoritmos clásicos.
Otro problema similar es el de ***los granos de trigo en el tablero de ajedrez***, que fue el premio solicitado por el inventor del juego, y consistía en pedir: *un grano por la primera casilla, dos por la segunda, cuatro por la tercera y así sucesivamente, doblando la cantidad de granos en cada casilla*. Este pareció un premio pequeño al rey que recibió el ajedrez, pero los granos de trigo crecen como 2^N, siendo N el número de casillas del tablero (64 en un tablero de ajedrez actual), y al final, la cantidad de trigo que habría que colocar en el tablero superan con mucho (más de 1.000 veces) la producción mundial de trigo en 2017 (dato de la Wikipedia). Como en el caso anterior, el número de granos de trigo crece exponencialmente con N y resulta inabordable cuando N va aumentando.
Los algoritmos normalmente utilizados en las computadoras para resolver problemas son algoritmos polinomiales, es decir, aquellos en que el tiempo de cálculo crece como N^n, siendo n un número entero determinado y N el número de elementos de cálculo (como las ciudades o casillas en los ejemplos anteriores). Los algoritmos de tiempo exponencial son aquellos en que el tiempo de cálculo crece como 10^N, como en los problemas que acabamos de mencionar. La mayoría de los algoritmos exponenciales se limitan simplemente a realizar una búsqueda exhaustiva, y muchas veces un análisis profundo del problema podría encontrar un algoritmo polinomial capaz de resolverlo sin necesidad de utilizar el algoritmo exponencial. En teoría de la computación, se dice que un problema no está "bien resuelto" hasta que se encuentra un algoritmo polinomial que lo resuelva.
Sin embargo, hay problemas tan difíciles que no existe algoritmo polinomial capaz de resolverlos. Estos problemas se llaman **"intratables"**. Es evidente que cualquier ordenador clásico (Máquina de Turing) se ve sobrepasado rápidamente con los problemas de tipo exponencial o "intratables", y, como hemos visto, no podemos esperar que la

potencia de cálculo de los ordenadores clásicos siga creciendo hasta el infinito. La solución, como veremos, puede ser la Computación Cuántica (QC en inglés).
Un problema exponencial muy importante es la **factorización de números enteros**, es decir, descomponer un número compuesto (que no es primo) en divisores que sean números primos, tales que cuando se multiplican entre sí dan el número original. Cuando los números son muy grandes este problema también crece exponencialmente. Los casos más duros son aquellos en que los factores que hay que encontrar son solo dos números primos, y aproximadamente del mismo tamaño. El problema de factorizar enteros en tiempo polinómico no ha sido aún resuelto en computación clásica. Si se consiguiera, tendría gran interés en criptografía, ya que muchos sistemas de encriptación dependen precisamente de encontrar esos factores primos, y plantearía un gran problema para ellos.

2.- Computación cuántica

Es una nueva tecnología que nace del cruce de la teoría de la Información y de la Mecánica Cuántica, que rige el comportamiento de los sistemas microscópicos, es decir a escala atómica. A dicha escala, la física se vuelve muy extraña, es inesperada y antiintuitiva. Los electrones, átomos y otras partículas cuánticas interactúan de manera diferente a los objetos ordinarios, macroscópicos, lo que permite utilizarlos para procesar la información de una manera distinta y más potente, superando los ordenadores clásicos. Por ejemplo, para el problema de factorización de números enteros, que hemos comentado antes, existe ya un algoritmo de computación cuántica, capaz de realizar la factorización en tiempo polinomial, con un error acotado. Ya se han construido algunos computadores cuánticos de unos pocos bits cuánticos (qubits), capaces de factorizar números pequeños. Los ordenadores cuánticos grandes serán capaces de descomponer números suficientemente grandes para descifrar la mayor parte de los sistemas criptográficos existentes, que se basan en esta dificultad de factorización.

2.1.- Qubits, los bits cuánticos

Un bit cuántico, o qubit, es en cierto modo similar a un bit clásico, pero difiere en aspectos muy importantes. Al igual que un bit clásico, un qubit puede tomar dos valores, 0 o 1, pero esta vez se utiliza la notación de la física cuántica, es decir, encerrados entre una barra vertical y un corchete angular: $|0\rangle$, $|1\rangle$, para denominarlos. Con esta notación, los estados cuánticos, que son los que rigen en sistemas atómicos o subatómicos, se distinguen de los clásicos, que se refieren a estados de sistemas físicos macroscópicos. Algunos posibles sistemas cuyos estados cuánticos pueden utilizarse como valores de un qubit se representan en la figura 6.

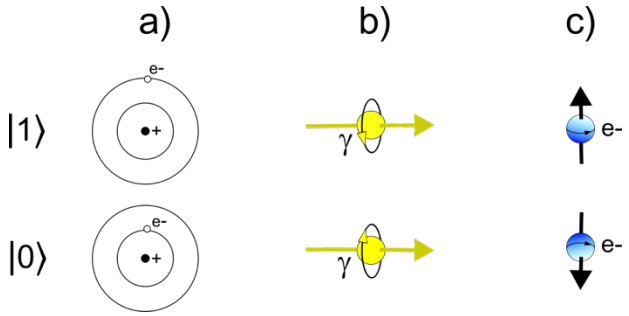


Figura 6.- *Posibles estados cuánticos que pueden representar los valores de los "qubits": a) estados de un electrón (e^-) en un átomo o ión; b) polarización de un fotón (γ), a izquierdas o derechas respecto a la dirección en que se propaga; c) dirección del espín de un electrón respecto a un eje determinado por el campo magnético. En este último caso, a veces, se denominan estados "up" (arriba) y "down" (abajo) y se escriben como $|\uparrow\rangle$, $|\downarrow\rangle$ en lugar de $|0\rangle$, $|1\rangle$*

El espacio de estados de un qubit: El espacio de estados de un sistema físico clásico o cuántico es el conjunto de todos los estados posibles del sistema. Un estado del sistema consiste en cualquier combinación de posiciones, momentos, polarizaciones, espines, energía, etc. de las partículas del sistema. Cuando consideramos solo los estados de polarización de un solo fotón, por ejemplo, el espacio de estados son todas las polarizaciones posibles del fotón. De manera más general, el espacio de estados para un solo qubit, sin importar en qué consiste dicho qubit (ver más abajo), es el conjunto de posibles valores:

$$\{a|0\rangle + b|1\rangle\},$$

donde $|0\rangle$ y $|1\rangle$ son dos estados cuánticos posibles del sistema físico (dados por sus funciones de onda de Schrödinger) y a y b son números complejos, llamados amplitudes de probabilidad, tales que sus módulos $|a|$ y $|b|$ cumplan

$$|a|^2 + |b|^2 = 1$$

Es decir, que la probabilidad total de que el sistema esté en algún estado es siempre 1= certeza. Estos valores de qubits corresponden a ***superposiciones*** de los estados cuánticos "puros", permitidos, $|0\rangle$ y $|1\rangle$. Son difíciles de llevar a la práctica y, sobre todo, de durar el tiempo suficiente (***coherencia***) para permitir usarlos en un cálculo, sin decantarse por uno u otro de los estados permitidos $|0\rangle$ o $|1\rangle$. Esta superposición es la base de la famosa, y mal entendida, paradoja del "gato de Schrödinger", que podía estar vivo y muerto a la vez, si fuese un sistema cuántico (que no lo es). Otra paradoja cuántica es la representada (figura 7). Un esquiador encuentra un árbol en su camino. Evidentemente un esquiador, que es un objeto macroscópico, como el gato anterior, NO puede pasar por un lado y otro del árbol a la vez, y tiene que rodarlo por un lado o por el otro, pero un electrón, que es un objeto cuántico, SI que puede pasar por un lado y otro de un obstáculo. Los qubits también pueden estar en cualquier estado "intermedio" entre $|0\rangle$ y $|1\rangle$, cosa que un bit "clásico" no puede hacer.

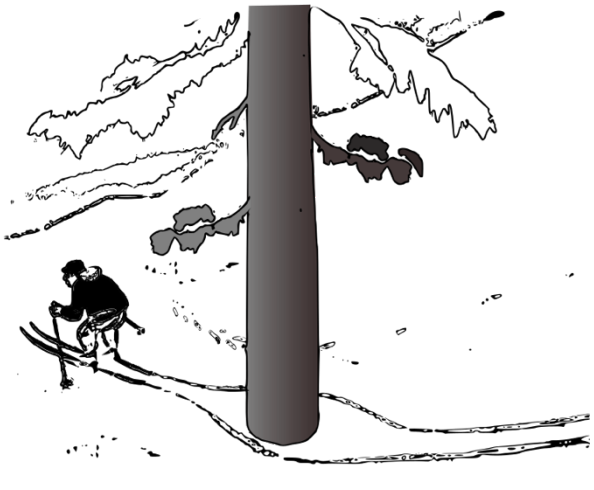


Figura 7.- *Paradoja cuántica: Un "esquiador cuántico" (un electrón, por ejemplo) podría pasar por ambos lados del obstáculo, cosa imposible para un esquiador real, macroscópico.*

Podemos visualizar los dos estados distintos, $|0\rangle$ y $|1\rangle$, como los polos norte y sur de una esfera de radio 1 llamada esfera de Bloch (figura 8). Las superposiciones de estos estados nos darán todos los posibles valores del qubit. Dichos valores cubren entonces todos los puntos de la esfera de Bloch. Si los coeficientes a y b fuesen números reales estaríamos solamente sobre la circunferencia del plano y-z, pero al poder ser números complejos (que constan de una parte real y otra imaginaria) se extienden a toda la superficie de la esfera,

lo que multiplica enormemente el espacio de estados y, consecuentemente, la capacidad de almacenar información en un solo qubit.
Esta capacidad de los qubits hace que la computación cuántica sea muy prometedora como método de cálculo mucho más eficiente que la computación clásica, limitada a solo dos estados por bit. Los algoritmos cuánticos funcionan almacenando y manipulando información de una manera inaccesible para las computadoras clásicas, lo que puede proporcionar una rapidez de cálculo extraordinaria para ciertos problemas. Sin embargo, al final del cálculo, cada qubit solo puede generar un único bit de información, es decir, cuando se mide (se lee) la información que contiene, solamente se obtiene un estado "puro". Así, si leemos, o medimos, el qubit: $a|0\rangle + b|1\rangle$ tendremos una probabilidad $|a|^2$ de obtener un $|0\rangle$ y una probabilidad $|b|^2$ de obtener un $|1\rangle$. La medida (lectura) de un qubit obliga, pues, al sistema cuántico a adoptar uno de los estados permitidos, o puros, que son los únicos observables.

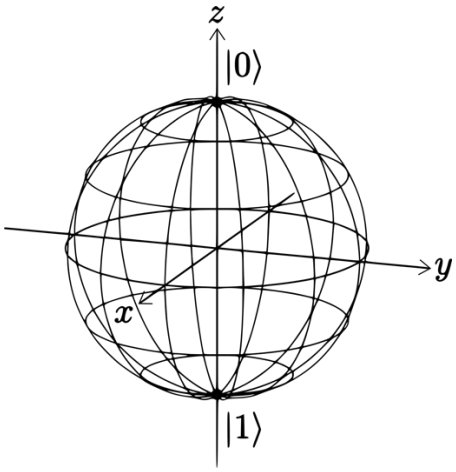


Figura 8.- *El espacio de valores de un qubit comprende toda la superficie de la esfera de Bloch y no solamente los estados "puros"* $|0\rangle$ y $|1\rangle$

Además de la **Superposición** de estados, por la que el sistema cuántico puede presentarse en una combinación cualquiera de estados permitidos, hay otras características cuánticas como:

- Entrelazamiento: es el proceso por el que varios sistemas cuánticos tienen estados que se correlacionan fuertemente (están vinculados), incluso cuando se separan a distancias muy grandes (macroscópicas) entre ellos. El entrelazamiento de los qubits produce una relación o vínculo entre ellos que les impide actuar de forma independiente.

- Decoherencia: es el proceso por el que los sistemas cuánticos superpuestos decaen o cambian, por interferencias externas, y se convierten en estados puros, medibles. Si esto ocurre antes de finalizar el cálculo que involucra un qubit, la información se pierde y el cálculo no puede terminarse correctamente.

- Interferencia: es el fenómeno en el que los sistemas cuánticos pueden interactuar y producir estados superpuestos de distinta probabilidad.

Varias de estas propiedades, en particular la superposición y el entrelazamiento, son extremadamente útiles en la tecnología informática, pues permiten a los ordenadores cuánticos procesar más información que los bits convencionales, que solo pueden estar en un único estado y actuar independientemente unos de otros.
Cuando se combinan varios qubits y se superponen, su capacidad de almacenar información aumenta exponencialmente. Dos qubits equivalen a cuatro piezas de información, tres a ocho y cuatro a dieciséis. Esto es así porque los qubits se combinan como partículas cuánticas, no como objetos clásicos y el espacio de estados cuánticos de

N partículas es 2^N, exponencialmente más grande que el de N objetos clásicos, que es solamente N^2. No hay análogo clásico de este hecho y los sistemas entrelazados no se pueden describir en términos de los estados de las partículas individuales.

Tabla1: *Capacidad de almacenamiento y procesamiento de información de bits y qubits*

N	Bits (N^2)	Qubits (2^N)
1	2	2
5	25	32
10	100	1.024
15	225	32.768
20	400	1.048.576
25	625	33.554.432
30	900	1.073.741.824

2.2.- ¿Cómo funciona la Computación cuántica?

Los ordenadores cuánticos utilizan qubits en lugar de bits para almacenar información exponencialmente. Aunque la computación cuántica también utiliza código binario, los qubits procesan la información de manera diferente a los ordenadores clásicos.

Una analogía que puede ser útil para entender cómo funcionan los ordenadores cuánticos sería la de un laberinto. Para salir del laberinto, una persona que se encuentra dentro, o un ordenador tradicional, tendría que resolver el problema por "fuerza bruta", probando todos los posibles caminos hasta encontrar la salida. Este tipo de ordenador utilizaría bits para explorar nuevos caminos y recordar cuáles no tienen salida. El cálculo de un ordenador cuántico equivaldría a tener una vista aérea del laberinto, y probar varios caminos simultáneamente (en paralelo) para obtener la solución correcta.

Sin embargo, la analogía no es perfecta. Los ordenadores cuánticos solo trabajan y miden las amplitudes de probabilidad de los qubits para determinar un resultado. Un cálculo en un ordenador cuántico funciona preparando una superposición de estados de los qubits, que constituye la "entrada". Luego, utiliza un circuito cuántico para generar entrelazamiento, lo que lleva a una interferencia entre estos diferentes estados, según una secuencia determinada, establecida por un algoritmo. Las interferencias hacen que muchos resultados posibles se cancelan (su probabilidad disminuye drásticamente), mientras que otros se amplifican (su probabilidad aumenta muchísimo). Los resultados amplificados son las soluciones del cálculo, pero la computación cuántica, por su propia naturaleza, solamente da soluciones probabilísticas.

Los procesadores cuánticos no resuelven ecuaciones matemáticas de la misma manera que lo hacen los ordenadores clásicos. Los ordenadores clásicos deben calcular cada paso de un cálculo complicado, mientras los circuitos cuánticos pueden procesar enormes conjuntos de datos simultáneamente lo que, para ciertos problemas, mejora la eficiencia en muchos órdenes de magnitud.

Los ordenadores tradicionales son deterministas, y requieren cálculos laboriosos para determinar un resultado singular específico para cualquier entrada. Los ordenadores cuánticos, en cambio, suelen proporcionar rangos de posibles respuestas. Este tipo de soluciones puede hacer parecer a la computación cuántica menos precisa que la clásica; sin embargo, para los tipos de problemas increíblemente complejos que los ordenadores cuánticos podrán resolver, esta forma de computación es suficientemente precisa y ahorrará cientos de miles de años de computación tradicional.

2.3.- Hardware cuántico

Las operaciones descritas deben llevarse a cabo en sistemas físicos cuánticos, hardware cuántico, tanto para almacenar la información (qubits) como para manipularla y extraer finalmente la solución. Veamos algunas posibles formas de hardware cuántico.

Qubits: Los qubits necesarios para la computación cuántica se puede implementar en diversas tecnologías específicas, que son muy distintas unas de otras. Además de la computación, las diferentes tecnologías cuánticas pueden ser útiles para la detección cuántica o para las comunicaciones cuánticas a través de la red. Aún no se ha decidido qué tecnología de qubits será la mejor, pues algunas tecnologías pueden ser más adecuadas para determinadas aplicaciones que otras.

Enfoques básicos para construir qubits

1) Qubits superconductores aprovechan las propiedades de los materiales superconductores para conducir electricidad sin resistencia cuando se enfrían a temperaturas muy bajas, cerca del cero absoluto. Han sido ampliamente desarrollados por empresas como **IBM** y **Google**. Los qubits superconductores se basan en pequeños circuitos hechos de materiales superconductores que permiten que los estados cuánticos de las corrientes y los campos magnéticos se puedan manipular y leer fácilmente. Esta tecnología permite un control y una escalabilidad precisos, que son fundamentales para las aplicaciones prácticas de la computación cuántica. Los qubits superconductores son también relativamente fáciles de integrar con las tecnologías de semiconductores existentes, pero necesitan estar a temperaturas del orden de 0,01-0,02 Kelvin (10-20 mK), es decir, unas 10-20 milésimas de grado por encima del cero absoluto.

2) Qubits de iones atrapados implican atrapar iones (átomos cargados) utilizando campos electromagnéticos y láseres para manipular sus estados cuánticos. Esta tecnología proporciona largos tiempos de coherencia, lo que la hace ideal para operaciones cuánticas precisas.

3) Qubits fotónicos utilizan fotones, o cuántos de luz, para transportar información cuántica. A diferencia de otros enfoques, la computación cuántica fotónica no requiere enfriamiento hasta casi el cero absoluto y podrían operar a temperatura ambiente, lo que es una gran ventaja. Los qubits fotónicos sean especialmente adecuados para la transmisión de información basada en las redes de fibra óptica existentes. Sin embargo, los fotones son difíciles de almacenar y manipular, lo que dificulta la implementación de puertas cuánticas y esquemas de corrección de errores.

4) Qubits topológicos, propuestos por **Microsoft**, se basan en los ***anyones***, o ***modos cero de Majorana*** unas cuasi-partículas*) que solamente se dan en sistemas bidimensionales y que, debido a su naturaleza exótica, teóricamente llevan incorporada la corrección de errores. Aunque todavía se encuentran en la etapa experimental, los qubits topológicos prometen reducir significativamente la necesidad de corrección de errores.

5) Qubits de espín en silicio son los más similares a las CPU tradicionales y utilizan el espín de los electrones en el silicio para codificar información cuántica. Este enfoque podría aprovechar las tecnologías de fabricación de semiconductores existentes. **Intel**, que es el más importante fabricante de semiconductores, utiliza este enfoque.

**)Una cuasi-partícula es una forma de describir el comportamiento colectivo de un gran número de partículas cuánticas como si fuese el de una sola partícula ficticia. En semiconductores, por ejemplo, si a la banda de valencia le falta un solo electrón para estar llena, el comportamiento de todos los electrones de dicha banda se puede describir como el de un solo "hueco", que sería una partícula de carga positiva que representa la falta de un solo electrón.*

Procesadores cuánticos: Son los componentes centrales de un ordenador cuántico. Un procesador cuántico contiene un chip con los qubits físicos del sistema y las estructuras necesarias para mantenerlos en su estado y actúan como el cerebro del ordenador

cuántico. Las unidades de procesamiento cuántico (QPU) incluyen el chip cuántico, la electrónica de control y el hardware de cómputo clásico necesario para la entrada y la salida de información. Un chip cuántico de IBM (o de Google) no es mucho más grande que los chips de silicio que se encuentran en una computadora portátil. Sin embargo, los sistemas criogénicos que se utilizan para mantener los instrumentos a una temperatura ultra baja, y los componentes electrónicos adicionales, a temperatura ambiente, para controlar el sistema y procesar los datos cuánticos, tienen aproximadamente el tamaño de un automóvil (figura 10). El tamaño de un sistema de hardware cuántico completo hace que la mayoría de las computadoras cuánticas sean cualquier cosa, menos portátiles, pero los investigadores y los científicos informáticos pueden acceder a ellas desde fuera de las instalaciones, a través de la red.

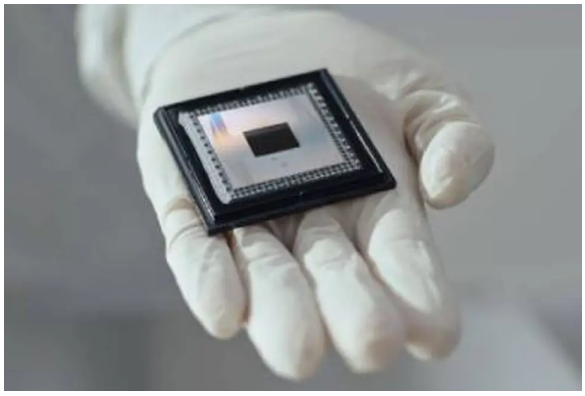


Figura 9.- *El chip cuántico "Willow", de Google, presentado el 9 de diciembre de 2024. Este procesador contiene 105 qubits superconductores y, según sus creadores, ha hecho, en menos de cinco minutos, un cálculo de referencia estándar, que llevaría entre 10 y 25 años a una supercomputadora convencional.*

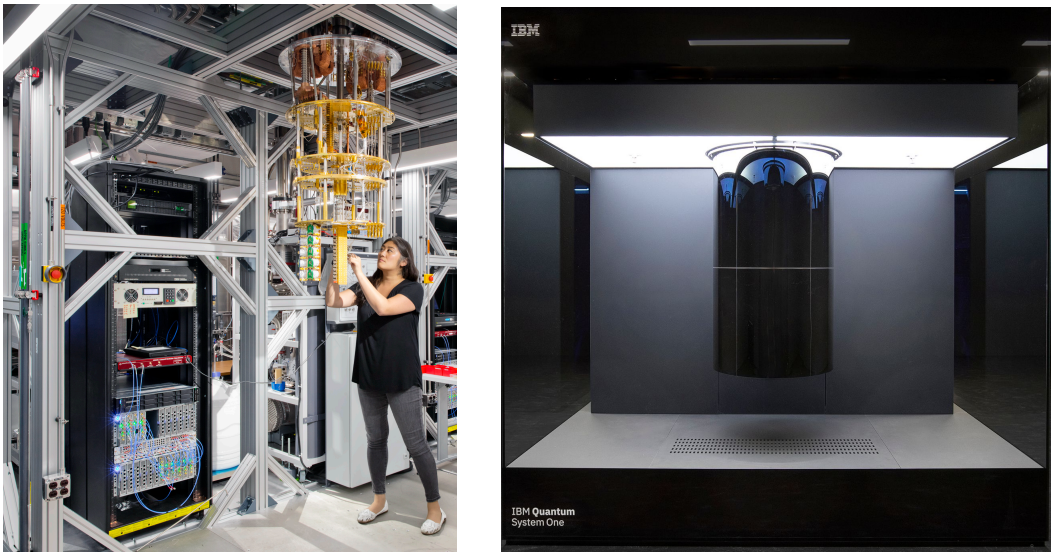


Figura 10.- *Izquierda: La Dra. Maika Takita con el corazón de un procesador cuántico (dorado) de IBM. Éste tiene un tamaño considerable y debe estar refrigerado con Helio líquido. Además, los equipos electrónicos necesarios ocupan varios armarios, Derecha: el computador IBM System One (2019). El cilindro central azul encierra el procesador y los equipos de refrigeración.*

Hitos en el desarrollo del hardware cuántico
- En **1998** se fabrican los primeros qubits. Investigadores de Los Álamos y el Instituto Tecnológico de Massachusetts consiguen transportar un qubit. Ese mismo año, nació la primera **máquina de 2 qubits**, en la Universidad de Berkeley.

- En **1999**, en IBM-Almaden, se creó la primera máquina de **3 qubits** y además fue capaz de ejecutar por primera vez el algoritmo de búsqueda de Grover (ver más abajo).

- En **2000**, IBM creó un ordenador cuántico de **5 qubits** y el Laboratorio Nacional de Los Álamos anuncia un ordenador cuántico de **7 qubits**.

- En **2006** científicos en Waterloo y Massachusetts diseñan métodos para mejorar el control del estado cuántico y consiguen desarrollar un sistema de **12 qubits**.

- En **2019**, IBM presentó el IBM Q System One (figura 10), el primer **ordenador cuántico para uso comercial**, con un procesador de **20 qubits.** A finales de año, Google logró la **supremacía cuántica** con su procesador Sycamore, de **53 qubits**, al resolver, en 200 segundos, tareas que los superordenadores tardarían unos 10.000 años en completar (Nature, **574** (2019) 505-510)

- En **2022,** IBM presenta un procesador cuántico de **433 qubits**

- En diciembre de **2024** Google presenta "Willow" (figura 9) con "sólo" **105** qubits pero que lleva incorporado un sistema de corrección de errores.

- En febrero de **2025** Microsoft ha presentado "Majorana 1", un chip cuántico basado en los modos cero de Majorana. Aunque este primer chip basado en estas cuasi-partículas solo tiene **8 qubits**, promete una escalabilidad que puede llegar a 1 millón de qubits, lo que ha generado tanto entusiasmo como escepticismo dentro de la comunidad científica.

Tabla 2: *Resumen de logros de hardware cuántico*

Año	Nº qubits	Laboratorio
1998	1	Los Alamos
1998	2	U Berkeley
1999	3	IBM
2000	5	IBM
2000	7	Los Alamos
2006	12	Waterloo, MIT
2019	20	IBM
2019	53*)	Google
2022	433	IBM
2024	105**)	Google (Willow)
2025	8**)	Microsoft (Majorana 1)

*) supremacía cuántica
**) con corrección de errores incorporada

Puertas cuánticas: Además de los qubits, los principales componentes de hardware de una computadora cuántica, son las **puertas cuánticas** (quantum gates) que permiten realizar operaciones con los qubits. El estado de un qubit se puede manipular aplicando puertas lógicas cuánticas, de forma análoga a cómo se puede manipular la memoria clásica con puertas lógicas clásicas. Una puerta cuántica es la puerta NO (NOT) o inversora, que actúa sobre los estados cuánticos de un qubit según:

$$\text{NOT: } |0\rangle = |1\rangle \text{ y NO: } |1\rangle = |0\rangle$$

Lo que puede representarse por una matriz 2x2 :

$$\text{NOT: } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

El efecto de una puerta NO sobre un qubit en un estado superpuesto: $a|0\rangle + b|1\rangle$, es:

$$\text{NOT: } (a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle = b|0\rangle + a|1\rangle$$

Las puertas cuánticas para memorias de varios qubits entrelazados pueden actuar de dos maneras distintas. Puede seleccionar un qubit y aplicar la puerta a dicho qubit sin afectar el resto de la memoria. O bien, puede aplicar la puerta al qubit seleccionado, solo si otra

parte de la memoria (otros qubits) está en un estado específico. Por ejemplo, los cuatro estados posibles de una memoria cuántica de dos qubits son:

$$|00\rangle; |01\rangle; |10\rangle; |11\rangle$$

Una posible puerta NO que actúa sobre el segundo qubit, controlada por el estado del primer qubit, una puerta NO controlada (CNOT), puede representar por la matriz 4x4 :

$$\text{CNOT:} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

y su acción sobre los estados cuánticos del conjunto de 2 qubits sería:

$$\text{CNOT: } |00\rangle=|00\rangle; \text{ CNOT: } |01\rangle=|01\rangle; \text{ CNOT: } |10\rangle=|11\rangle; \text{ CNOT: } |11\rangle=|10\rangle$$

En otras palabras, esta puerta CNOT aplica una puerta NO al segundo qubit si y solo si el primer qubit está en el estado $|1\rangle$. Si el primer qubit está en $|0\rangle$, no se hace nada en ninguno de los qubits.

Cualquier puerta cuántica se puede construir utilizando solamente un pequeño conjunto de todas las posibles, lo que se denomina **conjunto de puertas universales**. El mismo caso se daba en las puertas clásicas, que se pueden construir con solamente 3 de ellas.

En resumen, el hardware de la computación cuántica se puede describir como una red de puertas y mediciones (lecturas) de lógica cuántica que actúan sobre los qubits. La lectura de los qubits puede posponerse hasta el final del cálculo cuántico, por lo que la mayoría de los circuitos cuánticos consisten únicamente en una red puertas lógicas cuánticas sin ninguna medición.

En lo que se refiere a la tecnología superconductora, tanto los qubits como las puertas cuánticas, no utilizan transistores, sino ***uniones Josephson***, compuestas por dos materiales superconductores, separados por un óxido aislante. En ellas, la corriente puede atravesar la barrera aislante sin necesidad de voltaje. Las uniones Josephson confieren a los qubits sus propiedades únicas, como la capacidad de exhibir estados cuánticos como la superposición y el entrelazamiento. Las puertas cuánticas manipulan los estados cuánticos de los qubits superconductores mediante pulsos de microondas cuidadosamente diseñados para cada función.

2.4.- Software cuántico

Aunque la mejora de los componentes de hardware cuántico es fundamental, es solo la mitad del problema. El aprovechamiento de las ventajas de la computación cuántica debe incluir un software cuántico específico que permita aprovechar las capacidades del hardware. Los algoritmos cuánticos. Éstos vienen desarrollándose desde los años 90, antes de que se hubiese construido un solo qubit donde implementarlos, pero necesitan seguir mejorando.

Cronología del software cuántico
- En **1980**, Paul Benioff introdujo la **máquina de Turing cuántica**, para describir una computadora cuántica conceptual. – En **1981**, **Richard Feynman** (en su charla: "Simulating Physics with Computers" en el MIT) sugiere que el hardware basado en fenómenos cuánticos podría ser mucho más eficiente para la simulación de problemas cuánticos. - En **1984**, Charles Bennett y Gilles Brassard aplicaron la teoría cuántica a los protocolos de **criptografía** y demostraron que la distribución de **claves cuánticas** mejoraría la seguridad de la información.

- En los años siguientes surgieron algoritmos cuánticos concretos, que, aunque no resolvieron problemas prácticos, demostraron matemáticamente que se podía obtener más información utilizando un estado cuántico en superposición.
- En **1995** Peter Shor de AT&T Bell Laboratories definió el **algoritmo de Shor**, que permite calcular los factores primos de grandes números a una velocidad mucho mayor que cualquier computador tradicional, lo que permitiría romper muchos de los sistemas de criptografía utilizados actualmente.
- En **1996** Lov Grover inventó el **algoritmo Grover** de búsqueda de datos. Aunque la velocidad conseguida no es tan drástica como en los cálculos factoriales, su rango de aplicaciones es mucho mayor. Como el resto de algoritmos cuánticos, se trata de un algoritmo probabilístico con un alto índice de acierto.
- A partir de aquí se desarrollan gran número de lenguajes de programación, algoritmos y paquetes de cálculo y desarrollo de software cuántico
- En **2017**, IBM presentó **Qiskit,** la primera versión estable de un Kit de Desarrollo de Software (SDK) de código abierto, que utilizan ya más de 600.000 usuarios y 700 universidades de todo el mundo para desarrollar clases de computación cuántica.
- Hoy en día (**2024**), IBM ofrece una "Plataforma Cuántica" que da acceso a sistemas, documentación y recursos de aprendizaje, con 10 minutos gratuitos de tiempo de ejecución por mes en un sistema de 127 qubits (https://www.ibm.com/quantum)

Algunos algoritmos cuánticos, como el algoritmo de Shor para factorización y otros similares, presentan una aceleración muy superior a la polinómica respecto al algoritmo clásico. No se ha demostrado que no se puede descubrir un algoritmo clásico igualmente rápido, pero la evidencia sugiere que esto es poco probable.
Otros problemas, incluyendo la simulación de procesos físicos cuánticos de la química y la física del estado sólido, tienen algoritmos cuánticos que parecen dar aceleraciones superpolinómicas.
Finalmente, el algoritmo de Grover y otros similares, solamente dan aceleraciones cuadráticas, comparativamente modestas, pero son aplicables a una amplia gama de problemas, por lo que pueden ser de gran utilidad.

3.-¿Qué se puede esperar de la Computación Cuántica?

A día de hoy (2024), las computadoras clásicas superan a las cuánticas en todas las aplicaciones del mundo real. Si bien las computadoras cuánticas actuales pueden acelerar el cálculo de problemas matemáticos particulares, que se usan como prueba para medir su velocidad de cálculo, no brindan ninguna ventaja computacional para tareas prácticas. Aunque las computadoras cuánticas han empezado a ser más robustas y accesibles, todavía están en sus inicios y quedan muchas limitaciones que superar, la mayoría de ellas relacionadas con el hardware, para competir con los sistemas tradicionales, que se han desarrollado durante décadas y representan alternativas más robustas.

3.1.-Desafíos pendientes

Los qubits son muy delicados y deben estar completamente aislados del entorno, ya que cualquier interferencia o ruido (interferencias electromagnéticas o fluctuaciones térmicas) podría afectar a su estado, rompiendo así el proceso de cálculo.
Los principales problemas de la tecnología cuántica surgen de dos fuentes principales:

1) El hecho de que los qubits tienen un **período de coherencia** muy corto (que depende mucho de la tecnología de los qubits) y pierden sus datos con mucha frecuencia.

2) Los **errores**, ya que los procesos cuánticos en sí tienen una elevada tasa de errores, que necesitarían una elevada duplicación de qubits para su manejo. La corrección de

errores en la tecnología cuántica es mucho más desafiante que en la computación convencional debido a que: i) los errores cuánticos son continuos en todas las etapas del cálculo ii) no es posible replicar estados cuánticos desconocidos y iii) la evaluación puede degradar un estado cuántico y borrar la información en los qubits.

Hoy en día, la capacidad de computación de los equipos se mide por su número de qubits. Sin embargo, esta medida no es correcta, pues se necesita una elevada redundancia de qubits físicos para ejecutar un algoritmo cuántico con éxito. Esto plantea interrogantes sobre la viabilidad de las máquinas cuánticas al nivel de supercomputadoras, es decir con miles o millones de qubits. Es el llamado problema de **escalabilidad**.

Sin embargo, mejorar la fiabilidad de los cálculos no solo pasa por un hardware más confiable. Las técnicas de software para mejorar los cálculos tradicionales y tolerar fallas de hardware son hoy en día una práctica común en ingeniería informática. Un desafío pendiente es extender dicha práctica a los programas cuánticos.

3.2.- Futuras Aplicaciones

Una vez que se consigan superar los problemas actuales, los ordenadores cuánticos serían muy superiores a los ordenadores clásicos para resolver ciertos tipos de problemas, pero no son la solución ideal para todos los problemas, ni siquiera para la mayoría de ellos. Las computadoras cuánticas son excelentes para resolver problemas muy complejos, y podría ser la clave para lograr avances en una serie de campos críticos que requieren grandes conjuntos de datos o la factorización de grandes números. Estos van desde el desarrollo de nuevos medicamentos y el aprendizaje automático de las IA, hasta la optimización de las cadenas de suministro y los desafíos del cambio climático. Algunos ejemplos serían:

- Simulaciones cuánticas avanzadas Siguiendo la conjetura de Feynman, los "simuladores cuánticos" permitirían modelar cuestiones **físicas, químicas y biológicas,** complicadas. Muchos problemas importantes de la física, especialmente la física de bajas temperaturas y la física de muchos cuerpos, siguen sin comprenderse porque la mecánica cuántica subyacente es enormemente compleja. Las supercomputadoras convencionales son inadecuadas para simular sistemas cuánticos de 30 partículas, porque la dificultad crece exponencialmente con el número de partículas. Se necesitan mejores herramientas computacionales para comprender y diseñar racionalmente **moléculas** complejas y **materiales** cuyas propiedades dependen del comportamiento cuántico colectivo de cientos de partículas. Por otro lado, los ordenadores cuánticos no proporcionan ninguna potencia adicional en términos de computabilidad, pero se cree que pueden resolver ciertos problemas más rápido que los ordenadores clásicos y que hay problemas que solo las computadoras cuánticas pueden resolver en una cantidad de tiempo factible. Así, un sistema cuántico de muchas partículas podría ser simulado por un ordenador cuántico utilizando una cantidad de qubits similar a la cantidad de partículas en el sistema original.

- Recocido cuántico. El recocido cuántico o Quantum Annealing (QA) es un paradigma de Computación Cuántica para problemas de optimización de muchos tipos. Si se puede representar un problema de optimización específico como uno de minimización de energía de un sistema físico, podemos llevar a cabo una simulación del “recocido” del sistema, hasta que alcance el estado de mínima energía, que corresponderá a la solución del problema de optimización original. Para ello se requiere, claro está, encontrar un sistema físico que represente fielmente el problema de optimización propuesto.

- Química. Al igual que las computadoras cuánticas podrían ayudar en la investigación física, también podrían proporcionar la estructura y propiedades de nuevos productos químicos, ayudando a mitigar otros peligrosos o destructivos. La computación cuántica

podría conducir a catalizadores mejorados que permitan alternativas más limpias o la mejora energética de procesos industriales, para combatir las emisiones que amenazan el clima.

- Medicina. Las computadoras cuánticas capaces de simular el comportamiento molecular y las reacciones bioquímicas podrían acelerar enormemente la investigación y el desarrollo de nuevos fármacos y tratamientos médicos. También pueden analizar grandes conjuntos de datos del genoma para identificar patrones genéticos y mutaciones de manera más eficiente, lo que permite avanzar en la medicina personalizada, así como mejorar el reconocimiento de imágenes en los diagnósticos médicos (por ejemplo, resonancias magnéticas y tomografías computarizadas), lo que llevaría a una detección más temprana y precisa de enfermedades.

- Big Data. La QC puede acelerar el análisis de conjuntos masivos de datos, al permitir un reconocimiento de patrones, detección de anomalías y extracción de datos más rápidos. Esto puede permitir una mejor toma de decisiones en diversos campos, como las finanzas, la atención médica y la investigación.

- Aprendizaje automático. La QC puede permitir entrenarse más rápido y de manera más eficiente en conjuntos de datos más grandes. Lo que llevaría a modelos más precisos y predicciones mejoradas.

- IA. La QC proporcionará métodos de entrenamiento acelerados, lo que permite el desarrollo de modelos de IA más complejos y sofisticados. También puede abordar problemas de IA actualmente intratables para las computadoras clásicas, como el diseño de fármacos, la ciencia de los materiales y los modelos financieros ya mencionados.

- Criptografía y criptomonedas. La computación cuántica puede suponer un punto de inflexión para la criptografía debido a su capacidad de resolver ciertos problemas matemáticos mucho más rápido que las computadoras clásicas. El algoritmo de Grover puede, teóricamente, acelerar el proceso de minado de bitcoins, pero solo proporciona una ventaja competitiva moderada y no "rompería" el sistema. Las operaciones de minería actuales siguen siendo seguras.
Una computadora cuántica que ejecute el algoritmo de Shor podría romper de manera eficiente la encriptación, pero, para contrarrestarlo, ya se están desarrollando métodos criptográficos resistentes a la computación cuántica, la **criptografía postcuántica**. Si la computación cuántica llegara a una etapa en la que ninguna actualización criptográfica pueda proteger la red, Bitcoin (y muchos otros sistemas digitales) podrían perder confianza y valor. Sin embargo, es probable que ese escenario se produzca dentro de décadas o que no se materialice nunca debido a los avances en criptografía postcuántica.

- Modelado del clima. Aunque la predicción del tiempo ha avanzado mucho últimamente con computadoras convencionales, las proyecciones del cambio climático, inundaciones, modelado de flujo subterráneo, etc., requieren mejoras significativas que superan la potencia de procesamiento actual. Las computadoras cuánticas podrían ser capaces de resolver las ecuaciones diferenciales parciales complicadas en tres dimensiones en el aire y el mar naturales, para dar un detalle temporal y espacial significativamente mayor.

3.3.- ¿Cuándo estará madura la computación cuántica?

Todas las tecnologías emergentes atraviesan una serie de etapas antes de llegar al mercado como innovación productiva. Es lo que se conoce como el Ciclo de Gratner o ciclo de sobrexpectación (Hype cicle) (figura 11) Si bien este gráfico no es en absoluto científico (ninguno de sus ejes está cuantificados y la escala de tiempo pueden ser muy variables en

las diversas etapas), vamos a intentar situar la Computación Cuántica (QC) en él, para hacernos una idea de por dónde van los tiros.

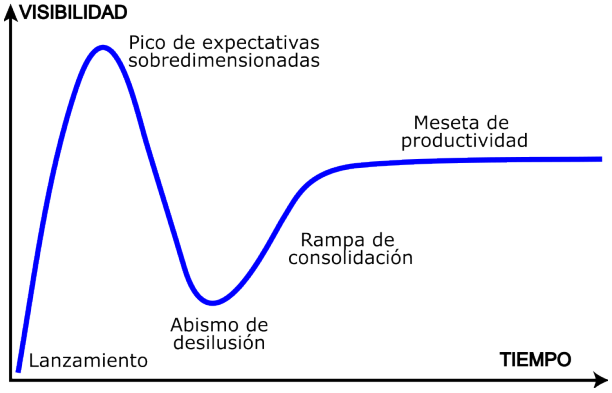


Figura 11.- *Ciclo de Gratner o de sobrexpectación para tecnologías emergentes (Wikipedia)*

1. Lanzamiento: *La primera fase en que genera interés y presencia en los medios.* La computación cuántica superó esta etapa hace años, cuando se demostraron los principios fundamentales y empresas como IBM, Google y otras comenzaron a hacer públicos sus primeros dispositivos.

2. Pico de expectativas sobredimensionadas: *El impacto en los medios y algunos éxitos generan un entusiasmo y expectativas poco realistas.* La QC puede que haya alcanzado esta fase alrededor de 2019-2021, con una amplia cobertura mediática, afirmaciones de "supremacía cuántica" y una fuerte inversión de los gobiernos y las empresas privadas. También puede que el pico se prolongue un poco gracias a nuevos logros recientes, como el microchip Willow de Google

3. Abismo de desilusión: *La tecnología deja de estar de moda porque no se cumplen las expectativas, y, en consecuencia, la prensa abandona el tema.* La computación cuántica podría estar entrando en esta zona, a medida que se vuelven más evidentes las limitaciones de los dispositivos cuánticos por el ruido y los errores. Muchos de los primeros usuarios y observadores reconocen que las ventajas significativas a gran escala están a años, si no décadas, de distancia.

4. Rampa de consolidación, o "pendiente de la iluminación": *Aunque la prensa ha dejado de cubrir la tecnología, algunas empresas siguen experimentando para entender los beneficios de la aplicación práctica de la tecnología*. Ciertos nichos de aplicaciones, como la simulación cuántica para problemas de química o de optimización, están comenzando a mostrarse prometedoras. Estos avances podrían significar que el ascenso hacia la consolidación se puede dar en los próximos 5 a 10 años.

5. Meseta de productividad: *Los beneficios quedan demostrados y aceptados. La tecnología se vuelve estable y evoluciona en segunda y tercera generación. La altura final de la meseta depende de si la tecnología es ampliamente aplicable o sólo tiene un nicho de mercado.* Es probable que la integración de la QC en el mundo real y la industria esté a unos 10 o 20 años de distancia, dependiendo de los avances en hardware, corrección de errores y escalabilidad.

Desde el punto de vista de las inversiones, existe un compromiso financiero creciente con la computación cuántica, lo que indica una gran confianza en su potencial. Así, por ejemplo (según ChatGPT), hasta 2024, la inversión pública global en tecnología cuántica alcanzó los 42.000 millones de dólares, y varios países han asumido compromisos financieros sustanciales para los años que vienen (AIMULTIPLE). En el sector privado

se han invertido ya más de 55.000 millones de dólares en tecnologías cuánticas, una parte muy significativa de ellos en computación cuántica (FORBES). Por otra parte, se prevé que estas inversiones crezcan a una tasa anual del 11,5 % entre 2023 y 2027, alcanzando 16.400 millones de dólares en 2027 (IDC), y que lleguen a crear hasta 850.000 millones de dólares de valor económico para 2040, lo que sustentaría un mercado de entre 90 mil millones y 170 mil millones de dólares para los proveedores de hardware y software (BOSTON CONSULTING GROUP)

En resumen, es poco probable que la computación cuántica esté "lista para su uso generalizado" antes de mediados de la década de 2030, aunque su impacto comenzará a sentirse antes en algunos campos específicos. Se espera que durante la próxima década dominen pequeños nichos de aplicaciones y las soluciones híbridas, y solo más tarde se extienda a campos más amplios, a medida que maduren los sistemas tolerantes a errores y se superen los desafíos de escalabilidad. Las grandes inversiones públicas y privadas indican una gran confianza en el sector.