**Guion Computación Cuántica**

**Computadores convencionales**

Los computadores actuales se basan 3 tres elementos: Los bits, las puertas lógicas y los circuitos eléctricos.

Los bits son la unidad básica de almacenamiento y pueden tener un valor que es o 0 o 1. Así con n bits tendremos 2n posibles combinaciones. De estas combinaciones, un computador actual sólo puede tomar 1 valor de ellos.

Las puertas lógicas son dispositivos electrónicos que realizan operaciones booleanas. Los ordenadores actuales se basan en los niveles más bajos en puertas lógicas. Los procesadores (a muy baja medida) están basados en las ALUs. Estas son unidades aritmético-lógicas. Es un circuito que puede realizar tanto operaciones lógicas booleanas como aritméticas.

La electricidad proporciona alimentación a los ordenadores –obviamente-. Pero también se usa para crear las puertas lógicas. Como por ejemplo una puerta NAND. En estos circuitos, lo que marca si es un 1 o un 0 es el voltaje, siendo comúnmente 5V y 0V. Cualquier valor entre esos dos es indeterminado y da lugar a errores.

Problemas y motivación para la computación cuántica

En la búsqueda de aumentar la velocidad de los chips convencionales, se reduce el tamaño de los transistores. Una vez llegados a tamaños bastante pequeños, comienzan a surgir errores. Esto produce resultados indeterminados que no nos sirven. Este error es el efecto túnel.

Nos encontramos a una escala tan pequeña que los electrones se pueden comportar como una onda y atravesar las puertas que no deberían atravesar (el aislante).

El material aislante de la puerta del transistor también da problemas puesto que al reducir el tamaño cuesta más retener a los electrones. Para esto se aportan soluciones como la *triple gate* o el proceso de fabricación *finfet*. Pero esto se tratan de “parches” puesto que a medida que queramos ir a tamaños más pequeños nos volveremos a encontrar con estos problemas.

Esta es la razón de que cada vez se tarde más en desarrollar procesadores de menores nanómetros. Intel lleva unos años con 14nn++ (10nn en portátiles) y AMD recientemente consiguió los 7nn con la arquitectura Zen2.

El concepto de computación cuántica comienza cuando Paul Benioff propone un modelo cuántico de la máquina de Turing. Expuso sus ideas de que las leyes cuánticas se podrían aprovechar para la computación.

Más tarde, Richard Feynman sugirió que la computación cuántica superaría con creces a la convencional.

**Historia**

1921 - Principio de incertidumbre

De Heisenberg. Establece la imposibilidad de que determinados pares de magnitudes físicas observables y complementarias sean conocidas con precisión.

1970 – Teoría Cuántica de la Información

Primera teoría que sugiere el entrelazamiento cuántico como recurso para la comunicación.

1981 – Feynman reta la computación cuántica

En una conferencia del MIT e IBM, Feynman reta a los ingenieros informáticos a desarrollar un computador basado en la física cuántica.

1994 – Algoritmo de Shor

Este algoritmo es que propulsa exponencialmente la computación cuántica, las teorías y expectativas. Es con este algoritmo con el que se descubre el gran potencial de este tipo de computación. El algoritmo consiste en factorizar un numero en sus factores primos. Una tarea increíblemente compleja para los ordenadores clásicos pero que se resuelve en un tiempo reducido con computadores cuánticos. Algo fundamental para romper la criptografía actual de clave pública y privada.

1995 – Corrección de error cuántico

Distintos grupos de investigadores descubren que usando un poco de redundancia se puede proteger frente al ruido del escenario/ambiente.

1996 – Requisitos de un computador cuántico

1. El sistema debe poder inicializarse -> llevarse a un estado de partida conocido y controlado
2. Ha de ser posible hacer manipulaciones a los cúbits de forma controlada, con un conjunto de operaciones que forme un conjunto universal de puertas lógicas.
3. El sistema debe mantener su coherencia cuántica.
4. Se debe poder leer el estado final del sistema, tras el cálculo.
5. El sistema debe poder ser escalable.

1997 - Código de corrección de errores

El primer código de corrección de error cuántico topológico es propuesto por el California Institute of Technology. Este algoritmo es el más prometedor para realizar un sistema escalable, sin errores.

2001 – Test del algoritmo de Shor

La computación cuántica comienza a ser una realidad y se prueba en un computador real el algoritmo de Shor para 15 = 3·5.

2019 – Primer ordenador cuántico comercial

IBM lanza al mercado el IBM Q System One, el primer ordenador cuántico comercial.

2019 – Google prueba la supremacía cuántica

Demuestra que los ordenadores cuánticos son, efectivamente, más rápidos que los ordenadores clásicos. Y pueden hacer cualquier tarea que estos e incluso algunas que los clásicos no pueden.

**Computadores cuánticos**

Para entender los computadores cuánticos primero debemos entender 3 cosas principales

1. Propiedades cuánticas

2. Aleatoriedad y error

3. Computación

Propiedades cuánticas

1. Superposición

La superposición hace referencia a la combinación de dos estados que normalmente describiríamos de manera independiente. En este caso, lo que antes eran 1 y 0 ahora es 1, 0 y ambos a la vez.

2. Entrelazamiento

El entrelazamiento cuántico es un fenómeno, sin equivalente clásico, en el cual los estados cuánticos de dos o más objetos se deben describir mediante un estado único que involucra a todos los objetos del sistema, aun cuando los objetos están separados espacialmente. Esto conlleva a correlaciones entre las propiedades físicas observables.

Ejemplo. Imaginaos que tú y tu amigo tenéis un cubit cada uno y realizáis una operación conjunta que establece los cubits en un estado de entrelazamiento. Si ahora cada uno os vais a una punta de la galaxia y hacéis cálculos con esos cubits veréis que son aleatorios. Sin embargo, si os volvéis a encontrar los cálculos serán precisos, sin error.

Esto permite utilizar los cubits para realizar operaciones matemáticas con pares de estados cuánticos, a pesar de que no sepamos que hay en uno individual.

El entrelazamiento es muy importante, puesto que si necesitas enviar un estado cuántico debes mandar un par entrelazado.

3. Interferencia

Los estados cuánticos pueden pasar por interferencias debido al fenómeno conocido como fase. La interferencia cuántica puede entenderse como una interferencia de onda. Cuando están en fase sus amplitudes se suman y cuando no, se cancelan.

Aleatoriedad y Error

En el “mundo clásico” se da por hecho que, si tenemos un dispositivo en las condiciones perfectas y precisas, el cálculo que hagamos con él también será exacto. Sin embargo, este no es el caso no la mecánica cuántica. Podemos tener unas condiciones perfectas y seguir obteniendo un resultado aleatorio.

Esta aleatoriedad se da por la superposición. Esto lo podemos imaginar como un sistema en el que tenemos distintas flechas apuntado a la izquierda y preguntamos al sistema: ¿estás hacia arriba o hacia abajo? El resultado será aleatorio puesto que son 50% arriba y 50% abajo, una superposición. Por lo tanto, el resultado no es 100% seguro y da lugar a un resultado aleatorio. Este no sería el caso si, por ejemplo, todas estuviesen apuntando a arriba o abajo, donde la respuesta será 0% o 100% arriba.

Se puede pensar que es como tirar una moneda y ver si es cara o cruz, excepto que no tiene nada que ver con tirar una moneda. En el lanzamiento de una moneda podemos saber si cae cruz si disponemos de la energía inicial, el momento angular, etc. Existen algunos datos que no son visibles al observador.

Con la mecánica cuántica se pensaba de este modo, que faltaban datos. Sin embargo, en los años 60 se demostró que no faltan datos, es completamente aleatorio.

Los errores en los cómputos vienen dados por el efecto de la decoherencia cuántica. Debido a este efecto los cubits se convierten en bis cuando entran en contacto con alguno de los materiales de medida y se pierde o se corrompe la información.

Computación

1. Cubits

Los cubits son el equivalente cuántico a los bits. Son la unidad mínima de los ordenadores. La diferencia principal con un ordenador clásico es que un cubit puede tomar como valor un 0, un 1 o una superposición de ambos. Es entonces, una superposición de estados clásicos.

En el clásico teníamos 2^n posibilidades. Pero solo 1 de ellas es la tomada por el bit. Con los cubits tenemos 2^n posibilidades y el bit tiene también 2^n estados clásicos. Esto aumenta la capacidad de cálculo de manera exponencial frente al bit clásico y permite realizar cálculos en paralelo.

2. Puertas lógicas

Una puerta es cualquier operación que cambia el estado del cubit. Físicamente, se hace enviando pulsos microondas (calibrados con gran precisión) que están en resonancia con la frecuencia de transición del cubit.

Podemos imaginarnos el estado del cubit como un vector radio de una esfera. El sentido Norte indica un 0, el Sur un 1, y el resto una superposición.

X-gate: rota el cubit 180º en el eje x, cambiando el estado de 0 a 1.

H –gate: es una puerta que genera una superposición. Cambia el estado del 0 a una superposición de 0 y 1. Aplicarla sobre sí misma devuelve el valor original

CNOT – gate: sirve para producir entrelazamiento. Realiza cambios en la rotación de los cubits en función de un cubit de control. Si el cubit de control es 0, no pasa nada. Si q0 es 1, q1 rota 180º. Si q0 comienza en un estado de superposición (0+1) el resultado sobre q1 será 0,0+1,1 que es un estado entrelazado.

3. Algoritmos

En general, los algoritmos se han diseñado como una serie de pasos a seguir en para conseguir un resultado en función de una entrada. Este algoritmo era luego implementado en cualquier máquina. Digamos que se diseña el algoritmo de manera abstracta y luego se adaptaba sin ningún tipo de complicación a las distintas máquinas.

Esto no es así con los ordenadores cuánticos puesto que trabajan de manera muy distinta. Al fundamentarse en otras propiedades físicas distintas a las de los ordenadores clásicos, los primeros pueden realizar más procesos y algoritmos que uno clásico. Los algoritmos pueden explotar esos efectos cuánticos para obtener un resultado más rápido.

La manera en la que funciona un computador con un algoritmo es:

a. Toma la entrada

b. La procesa a un estado clásico que es una superposición de un numero exponencial de estados clásicos.

c. Transforma ese estado en uno que consigue la solución.

d. Se mide ese estado

Los algoritmos cuánticos son especialmente mejores que los clásicos en factorizar números en factores primos, buscar, y ciertos problemas numéricos.

Sin embargo, todo esto es teórico puesto que muchos de estos algoritmos necesitan una cantidad relativamente elevada de cubits, de las que no disponemos actualmente. Son algoritmos para el futuro. Se están diseñando para que cuando llegue un computador con más cubits, estemos preparados para usarlo.

**Problemas**

A pesar de lo interesante que es y el potencial que tienen los ordenadores cuánticos, no están exentos de problemas.

El problema principal y bastante potente es el problema de la decoherencia cuántica. Esto hace que un cubit pase a un simple bit. Esto es, un estado cuántico se convierte en uno clásico al entrar al contacto con los materiales de medida. -> Gato de Schrödinger.

Esto complica bastante la lectura del resultado final. Ya que da resultados aleatorios. Se están considerando soluciones desde distintos ángulos, mejorar la corrección de errores, encontrar maneras mejores de encontrar esos errores o realizar procesos cuánticos más robustos (más resistentes a estos errores).

**Supremacía Cuántica**

Se define la supremacía cuántica como la habilidad de un ordenador cuántico de superar los ordenadores clásicos. Esta meta es perseguida por empresas como IBM y Google y los gobiernos de EEUU y China, puesto que consideran un asunto de seguridad nacional al poder romper la criptografía actual.

En octubre Google reclamaba haber logrado y demostrado la supremacía cuántica. Consiguiendo que un ordenador cuántico resolviese un problema en cuestión de minutos cuando a uno clásico le hubiera llevado años.

Sin embargo, IBM desmintió el avance de google. Declararon que estábamos cerca de la supremacía cuántica pero que todavía no la habíamos alcanzado puesto que un superordenador de IBM podía realizar el mismo problema en poco más de un día.

Finalmente, no todo el mundo tiene claro que los computadores cuánticos merezcan la pena. Algunos matemáticos piensan que es prácticamente imposible sortear los problemas con los que nos encontramos al trabajar al nivel cuántico y que por tanto no es accesible.

Solo el tiempo dirá quién tiene la razón.

# Referencias

*IBM - Quantum Computation*. (s.f.). Obtenido de https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/

*IBM - Quantun Computing How it works*. (s.f.). Obtenido de https://www.ibm.com/blogs/research/2017/09/qc-how-it-works/

*IBM - What is quantum computing*. (s.f.). Obtenido de https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/

Science Alert. (s.f.). *Quantum Computers*. Obtenido de https://www.sciencealert.com/quantum-computers

*Wikipedia - Computación Cuántica*. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Computaci%C3%B3n\_cu%C3%A1ntica

*Wikipedia - Entrelazamiento Cuántico*. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Entrelazamiento\_cu%C3%A1ntico