

INTRODUCCIÓN A LA COMPUTACIÓN CUÁNTICA

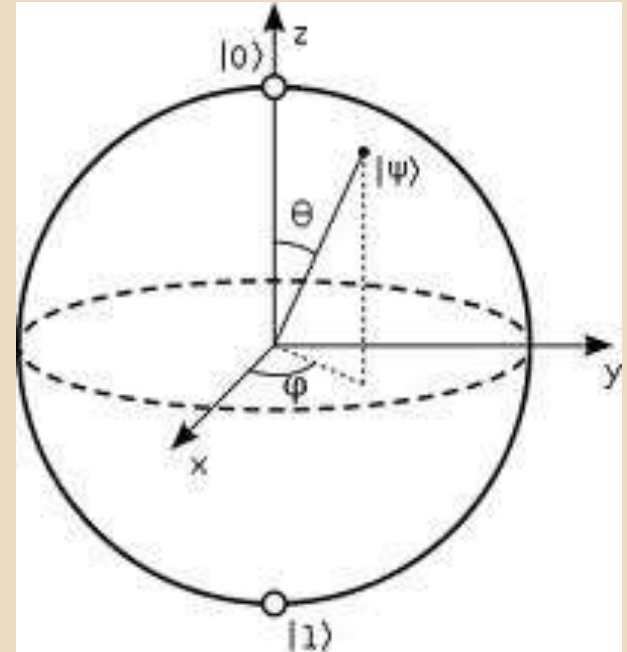


Características Principales

- Nuevo paradigma de computación diferente a la clásica
- Se basa en el uso de Qubits en vez de Bits
- Cambia la forma de realizar las tareas, aprovechando el paralelismo cuántico
- Los algoritmos cuánticos utilizan los conceptos de superposición de estados y entrelazamiento
- Se modifica la complejidad de las tareas, haciendo abordables problemas clásicamente intratables

El Qubit

- Bit: Unidad clásica de información
Toma los valores 0 ó 1
- Qubit: Quantum bit
Unidad cuántica de información
Sistema cuántico que puede tomar los valores $|0\rangle$ ó $|1\rangle$ al ser observado, pero se encuentra en una superposición de ambos estados $|\psi\rangle = a |0\rangle + b |1\rangle$ con $|a|^2 + |b|^2 = 1$ donde $|0\rangle$ y $|1\rangle$ es una base ortonormal del espacio vectorial (de dimensión 2) del qubit



Operación de Medición

- Al medir (observar) un qubit, colapsa su función de onda: el qubit toma un valor determinado, dejando el estado de superposición en que se encontraba.
- Si se mide en la base $\{|0\rangle, |1\rangle\}$
 $M(a|0\rangle + b|1\rangle)$ dará por resultado el estado $|0\rangle$ con probabilidad $|a|^2$ ó el estado $|1\rangle$ con probabilidad $|b|^2$

Sistema Clásico

- Un sistema clásico de n partículas, con 2 grados de libertad para cada una, se describe indicando el estado de cada partícula en forma independiente.
- El sistema se combina a través del producto cartesiano.
- El sistema tendrá $2n$ grados de libertad.

Sistema Cuántico

- Un sistema cuántico de n partículas, cada una representada en un espacio vectorial de 2 dimensiones, no puede describirse siempre considerando sus componentes en forma independiente.
- El sistema se combina a través del producto tensorial.
- Aparecen estados entrelazados.
- El sistema tendrá 2^n grados de libertad.

Producto Cartesiano vs. Tensorial

- Sean 2 espacios vectoriales de dimensión 2, con bases $\{v_1, v_2\}$ y $\{w_1, w_2\}$
- El producto cartesiano conduce a un espacio vectorial con base $\{v_1, v_2, w_1, w_2\}$
- El producto tensorial conduce a un espacio vectorial con base $\{v_1 w_1, v_1 w_2, v_2 w_1, v_2 w_2\}$

Múltiples Qubits

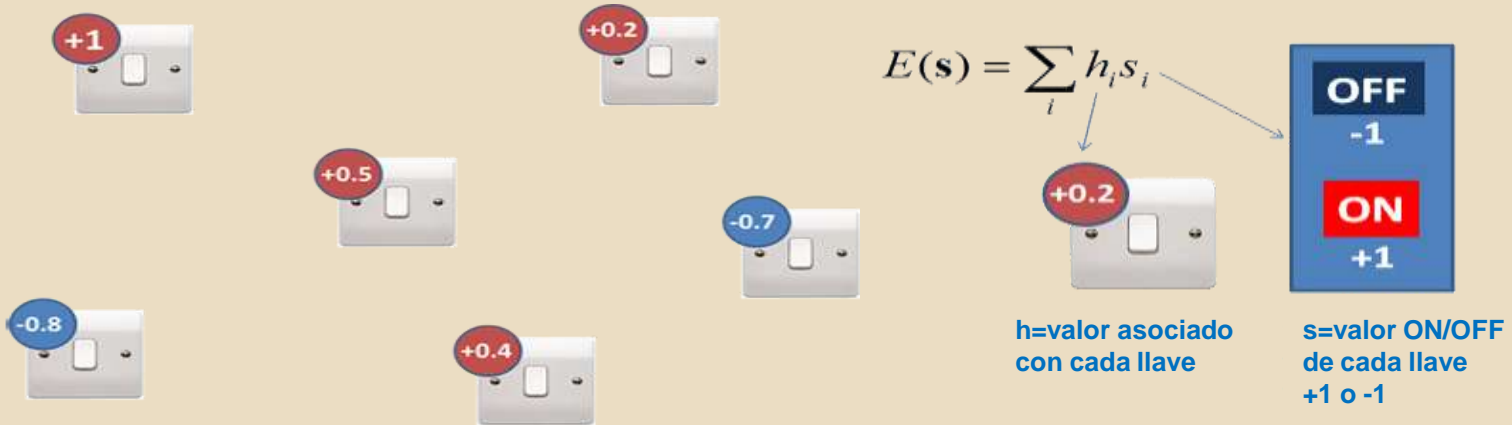
- El espacio de estado de 2 qubits, cada uno con base $\{|0\rangle, |1\rangle\}$, tiene base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ (dimensión 2^2)
- El espacio de estado de 3 qubits, cada uno con base $\{|0\rangle, |1\rangle\}$, tiene base $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$ (dimensión 2^3)
- Un registro de n qubits puede estar en un estado que es superposición de 2^n estados !!
Paralelismo cuántico en algoritmos de QC

Entrelazamiento de 2 Qubits

- El estado $|\Psi\rangle = \alpha |00\rangle + \beta |11\rangle$ no puede provenir del producto tensorial de 2 qubits independientes
 $(\alpha |0\rangle + \beta |1\rangle) \otimes (c |0\rangle + d |1\rangle) =$
 $ac |00\rangle + ad |01\rangle + bc |10\rangle + bd |11\rangle \neq \alpha |00\rangle + \beta |11\rangle$
- Estos estados “extras” entrelazados (entangled) que no tienen análogo clásico conducen a la famosa paradoja de EPR, de “acciones instantáneas a distancia”, usados para la teleportación de estados cuánticos

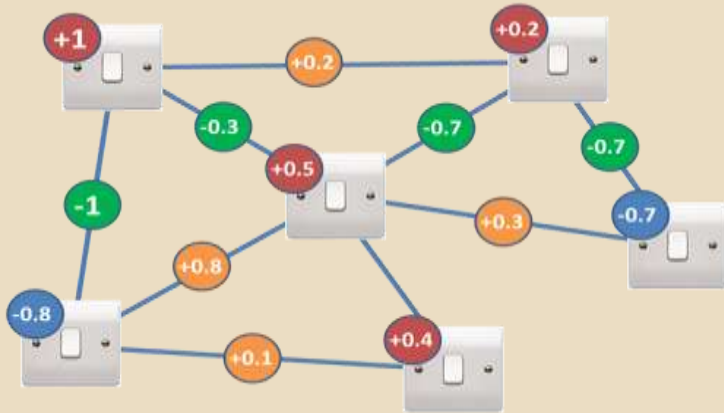
Problemas de Optimización Discreta

Ejemplo simple: Encontrar los valores de seteo (s_i) de cada llave, para obtener un mínimo de $E(s)$



Problemas de Optimización Discreta

Ejemplo complejo: Encontrar los valores de seteo (s_i) de cada llave, para obtener un mínimo de $E(s)$, pero ahora con un acoplamiento $J_{i,j}$ entre las llaves



$$E(\mathbf{s}) = \sum_i h_i s_i + \sum_{i,j} J_{i,j} s_i s_j$$

Agregando otro peso J , que multiplica al producto de los estados de dos llaves

Con 500 llaves no alcanzaría el tiempo del Universo para probar las 2^{500} configuraciones posibles (pero con 500 Qubits podría resolverse...)

Problemas de Factorización

- La imposibilidad de factorizar grandes números es la premisa en que se basan los actuales sistemas de encriptamiento, como RSA
- El algoritmo cuántico de Shor permite factorizar grandes números en una computadora cuántica en pocos minutos, contra años que demoraría el proceso en una computadora clásica
- Sólo es cuestión de que se disponga de computadoras cuánticas con la cantidad de qubits necesarios

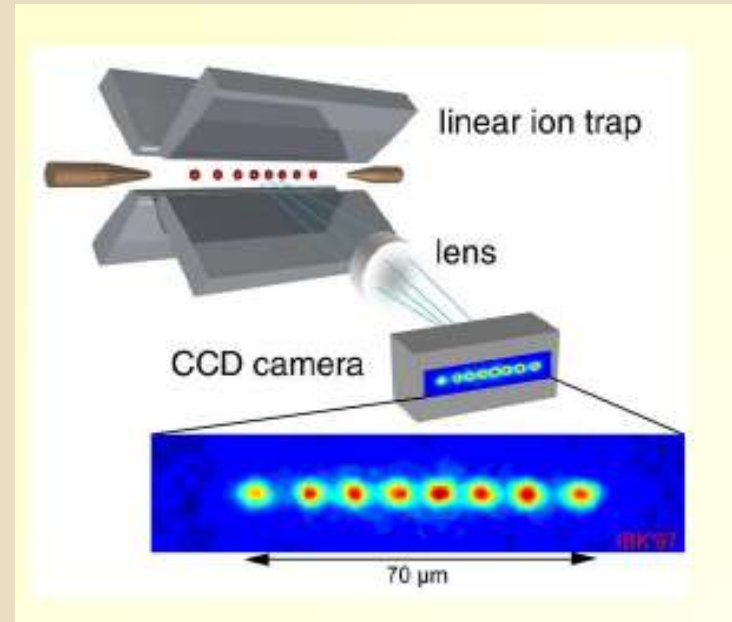
Realización Física de Qubits Requerimientos

- Memoria confiable: Los Qubits deben mantener su estado cuántico (coherencia)
- Manipulación: Debe ser posible cambiar los estados de los Qubits individualmente
- Compuertas Lógicas: Los Qubits deben poder relacionarse a través de operaciones lógicas
- Acoplamiento: Debe existir acoplamiento entre Qubits pero aislamiento del exterior

Realización Física de Qubits

Trampa Iónica

- Iones en trampas al vacío, levitados eléctricamente, se comportan como pequeños imanes
- Los estados $|1\rangle$ y $|0\rangle$ de cada Qubit corresponden a dos orientaciones posibles del momento magnético del ión
- Los iones se manipulan utilizando láseres



Realización Física de Qubits Espines Nucleares (RMN)

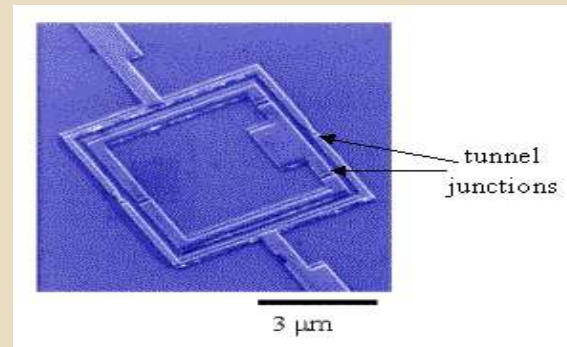
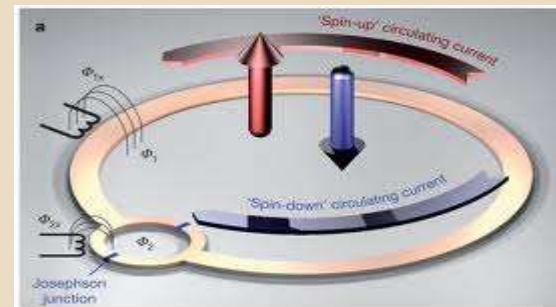
- Los núcleos atómicos de un grupo de moléculas en dilución, se comportan como pequeños imanes
- Los estados $|1\rangle$ y $|0\rangle$ de cada Qubit corresponden a dos orientaciones posibles del momento magnético
- Las moléculas se manipulan usando ondas de radio en equipos de RMN



Realización Física de Qubits

Flux Qubits

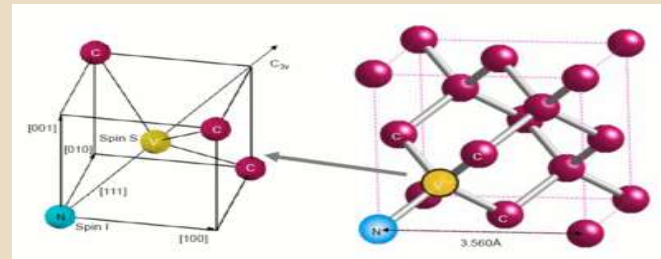
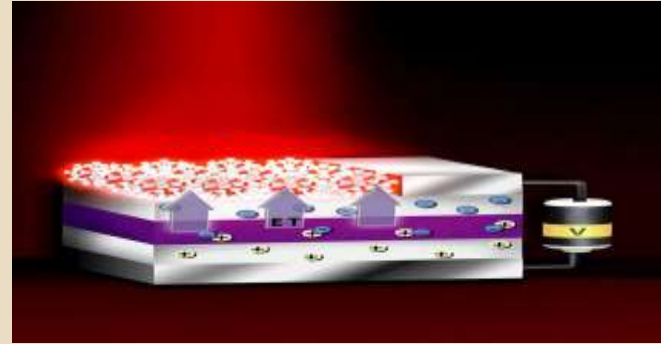
- Se establecen corrientes eléctricas en anillos superconductores micrométricos (interrumpidos por una o más juntas Josephson), a muy baja temperatura (pocos mK)
- Los estados $|1\rangle$ y $|0\rangle$ de cada Qubit corresponden a orientaciones horaria y antihoraria del sentido de circulación de la corriente en el anillo superconductor
- Las corrientes se manipulan utilizando campos magnéticos y radiación de microondas



Realización Física de Qubits

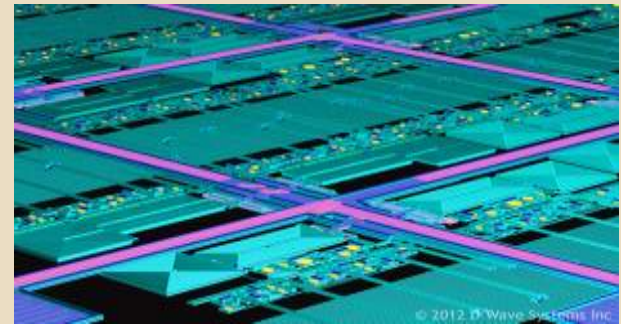
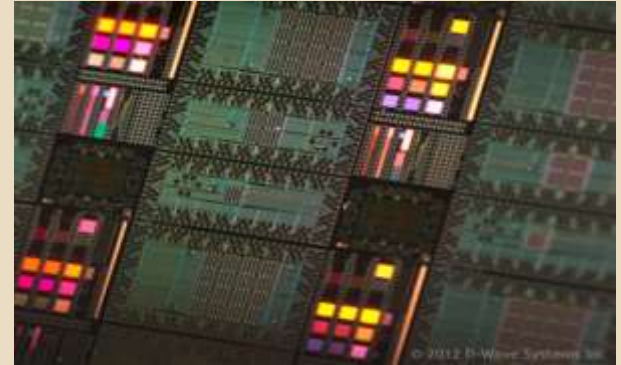
Otras Propuestas

- ❑ Defectos cristalinos en diamantes
- ❑ Puntos cuánticos
- ❑ Polarización de fotones
- ❑ Spin de electrones



Primeros Hardwares Cuánticos

- 1998: Isaac Chuang (Berkeley), primera computadora cuántica de 1 Qubit
- 2001: IBM, Computadora cuántica de 7 Qubits con la que factorizaron el número 15
- 2005: Rainer Blatt (Innsbruck), Computadora cuántica de 8 Qubits
- 2012: Jiangfeng Du (Universidad de Ciencia y Tecnología de Hefei, China), logran factorizar el número 143



Empresas desarrollando QC

- IBM
<https://quantum-computing.ibm.com/>
- Google
<https://research.google/teams/applied-science/quantum/>
- Microsoft
<https://www.microsoft.com/en-us/quantum>
- DWave
<https://www.dwavesys.com/>
- Honeywell
<https://www.honeywell.com/en-us/company/quantum>
- ... y la lista sigue ...

