

# Storia del quantum computing

---

Mattia Papaccioli

Università degli studi dell'Insubra



Libro

Dalla teoria alla pratica

Le regole del gioco

Come funziona il computer quantistico?

Considerazioni finali

**Libro**

---

Gli argomenti che mi sono piaciuti di più sono stati la storia sui navajo, la storia del tesoro perduto e seppelito in America e la parte finale sul computer quantistico.

## **Dalla teoria alla pratica**

---

- Vecchie teorie fisica quantistica (1900)
  - Black Body radiation
- Teorie fisica quantistica moderna (1920)
  - Niels Bohr
  - Erwin Schrodinger

- (1982) Richard Feynman immagina il computer quantistico
- (1985) David Deutsch descrive il computer quantistico universale
- (1994) Peter Shor descrive un algoritmo per la fattorizzazione dei numeri primi
- (1996) Lov Grover descrive un algoritmo per la ricerca di collezioni non ordinate in  $O(\sqrt{n})$
- (2000) Eddie Farhi sviluppa un'idea per il computer quantistico adiabatico
- (2009) Surface Code for Error Correction
- (2020) Ricercatori cinesi annunciano di aver raggiunto la supremazia quantistica con un cq a 76-qubit

## Computer Classico

- utilizza particelle macroscopiche
- e basato sulle leggi di Newton e Maxwell
- lo stato del sistema è definito dallo stato dei transistor
- lo stato seguente può essere predetto con certezza

## Computer Quantistico

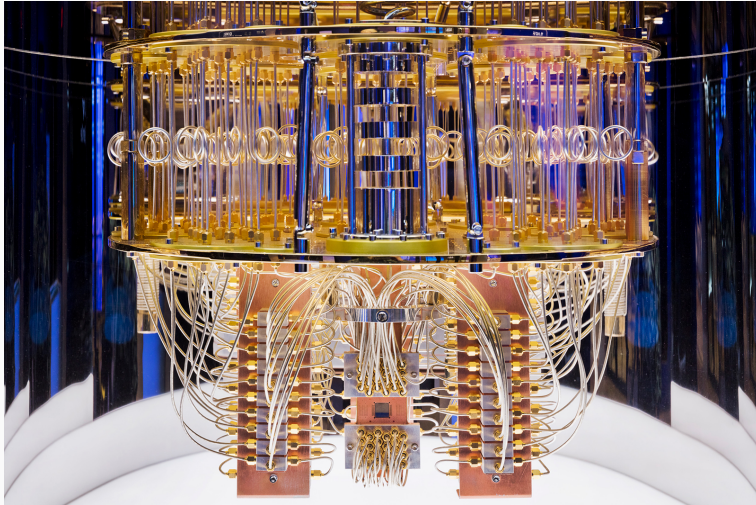
- utilizza particelle microscopiche
- e basato sulle leggi di Schroedinger
- lo stato del sistema non può essere determinato con certezza, a causa della duale natura della materia (sia particella che onda simultaneamente)



# Esempio di computer quantistico



UNIVERSITÀ DEGLI STUDI  
DELL'INSUBRIA



## Le regole del gioco

---

**ket**  $|\nu\rangle$

rappresenta un vettore in uno spazio di vettori complesso e  
fisicamente rappresenta un sistema quantistico

**bra**  $\langle f|$

rappresenta un mappa lineare che fa corrispondere ad ogni vettore  
un numero complesso.

Per operare una funzione lineare  $\langle f|$  su un vettore  $|\nu\rangle$  si scrive  
 $\langle f|\nu\rangle \in \mathbb{C}$

## Superposizione

Possibilità di un qubit di trovarsi nello stato  $|0\rangle$  o  $|1\rangle$ :

$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

dove  $a$  e  $b$  sono numeri complessi e  $|a|^2 + |b|^2 = 1$ .

Esempio gatto di Schroedinger.

## Entanglement

Quando un gruppo di particelle è generato in modo che ogni particella di esso non può essere descritta indipendentemente dalle altre, anche se esse sono separate nello spazio. Misurando lo stato di una particella, si vengono a conoscere gli stati delle altre particelle.

## **Decoherence**

perdita dello stato di superposizione a causa di interazioni spontaneo di un sistema quantico e il suo ambiente.

## **Misurazione**

ogni volta che misuriamo un quantum system esso perde il suo stato di superposizione.

## **No-cloning theorem**

e impossibile creare una copia di un quantum state arbitrario perche non esiste un sistema di misurazione che non faccia collassare il quantum state.

# **Come funziona il computer quantistico?**

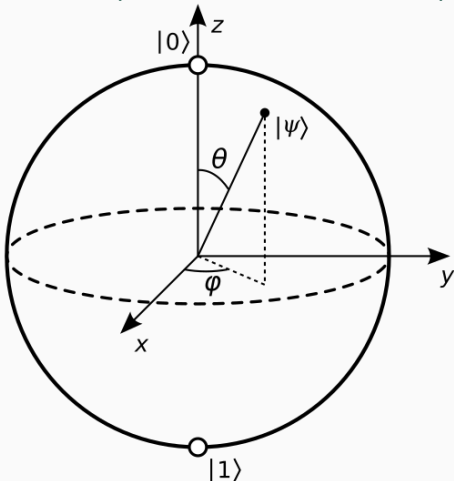
---

**Qubit:** unità base di informazione quantistica, equivalente quantistico del bit classico. È un sistema a due livelli (es. spin dell'elettrone o polarizzazione di un fotone).

**nota:** un computer quantistico può simulare un computer classico e viceversa.














Lo stato di Superposizione viene rappresentato graficamente con la sfera di Bloch. Ai poli sono rappresentate le basi vettoriali  $|0\rangle$  e  $|1\rangle$  che corrispondono nella realtà allo spin di un elettrone.



Il resto della superficie della sfera rappresenta le superposizioni intermedie tra le basi vettoriali  $|0\rangle$  e  $|1\rangle$ . Il vettore  $|\Psi\rangle$  è una superposizione.

$\theta$ : controlla la latitudine di  $|\Psi\rangle$ , cioè quanta probabilità hanno  $|0\rangle$  e  $|1\rangle$

$\phi$ : controlla la longitudine, cioè la phase relativa tra  $|0\rangle$  e  $|1\rangle$

Operator	Gate(s)	Matrix
Pauli-X (X)	 	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

## Quantum gate

circuito quantistico di base che opera su qubit. Sono analoghi alle porte logiche nei computer classici (and, or, xor, not etc...). A differenza delle porte classiche, quelle quantistiche sono reversibili

per esempio, i gate Pauli-XYZ ruotano nelle 3 dimensioni la direzione di  $|\Psi\rangle$  sulla sfera di Bloch

il gate di Hadamard invece crea uno stato di superposition con uguale probabilità di  $|0\rangle$  e  $|1\rangle$

il gate cnot invece agisce su due qubit e corrisponde all'operazione classica di xor

combinando questi ed altri gates possiamo costruire un computer quantistico ed effettuare computazioni in modo più efficiente rispetto ad un computer classico. Sono stati teorizzati algoritmi di ricerca e di fattorizzazione più veloci grazie ad:

- parallelismo quantico. tramite la sovrapposizione il computer esegue l'algoritmo su tutti i possibili input allo stesso momento
- dimensione dello spazio di Hilbert quantistico. la dimensione dello spazio degli stati è esponenzialmente più grande. aggiungendo un qubit raddoppiamo lo spazio di Hilbert mentre in un computer classico dovremmo raddoppiare il numero di bit
- capacità di entanglement

## Considerazioni finali

---

- Shor per fattorizzazione numeri primi
- Quantum Fourier Transform
- Quantum Cryptography



La maggior parte delle tecniche di cifratura usate al giorno d'oggi non sono resistenti alla decifrazione quantistica. Se qualcuno registra una sessione HTTP oggi, potrebbe essere in grado di decifrarla tra 5-10 anni.

Il computer quantistico non sar  accessibile a tutti nel breve periodo, a causa delle condizioni di isolamento che deve mantenere per evitare la decoerenza e a causa del quantum error correction. Resta comunque un arma potente che da potere enorme a chi la controlla.