# Introduzione

**Computer classico** opera sulla base dei valori delle tensioni ai capi di dispositivi, circuiti e porte logiche, che possono essere modellizzati nell'ambito della fisica classica.
*Legge di Moore*. Il numero di transistor su chip raddoppia ogni 18 mesi. Si prevede che i circuiti a microprocessore saranno in grado di svolgere operazioni su scala atomica entro la prossima decade.
*Downscaling*. Il ridimensionamento della struttura e dei componenti del circuito ha peró una serie di effetti indesiderati per l'efficienza del calcolo. I conduttori metallici nanometrici (tracce metalliche nanometriche di rame o altri metalli) cristallizzano e cortocircuitano. Fenomeni quantistici si manifestano come per esempio i portatori di carica (es. elettroni) che attraversano barriere di potenziale (strato isolante tra conduttori) (effetto tunnel in questo caso indesiderato).
*Elaborazione seriale*: cioé funziona eseguendo un'operazione alla volta.

# Introduzione

**Computer quantistico**

Si tratta di un computer che per eseguire operazioni utilizza *fenomeni elementari della meccanica quantistica*, come la sovrapposizione e l'entanglement quantistico, e/o

É basato su *dispositivi e tecnologie quantistiche*, cioé sfrutta il potere di atomi e molecole, organizzati opportunamente in strutture operanti secondo fenomenologie quantistiche per eseguire attività di memorizzazione e di elaborazione.

*Elaborazione parallela*: milioni di operazioni alla volta
Il computer quantistico da 30 qubit equivale alla potenza di elaborazione del computer convenzionale che funziona a 10 teraflop (trilioni di operazioni in virgola mobile al secondo).

# Introduzione

**Bit classico** E' definito mediante due stati - on o off - 0, 1 - che si escludono a vicenda. Il bit é l'unitá indivisibile nell'ambito della informazione classica, puó assumere *solo* i valori 0 e 1.

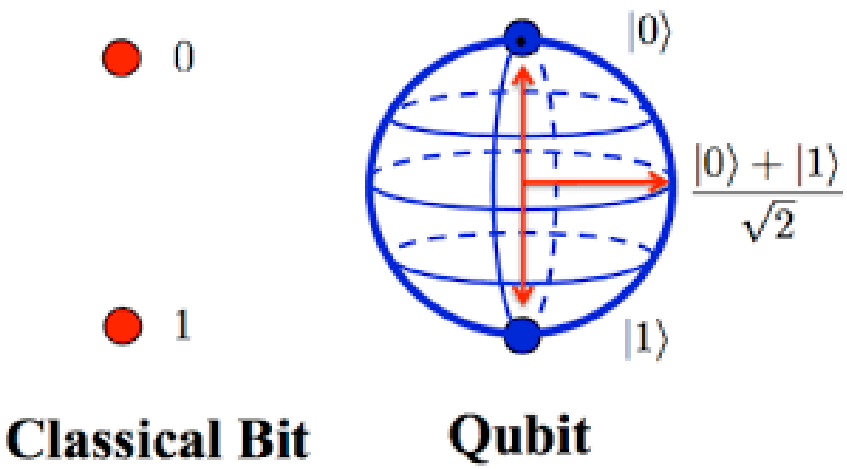
**Bit quantistico (Qubit)** Nell'ambito dell'informazione quantistica l'unitá fondamentale é il bit quantistico o qubit. Il qubit é un vettore in uno spazio vettoriale complesso (dotato di tutte le prorietá di uno spazio vettoriale quindi di prodotto interno, etc ). In analogia con il bit classico, possiamo indicare con $|0\rangle$ e $|1\rangle$ i due stati fondamentali del qubit. I due stati sono scelti in modo da costituire una base ortonormale dello spazio vettoriale. La sovrapposizione di entrambi gli stati è possibile (combinazione lineare dei vettori della base).

# Introduzione

Un generico vettore in questo spazio puó essere scritto nella forma:

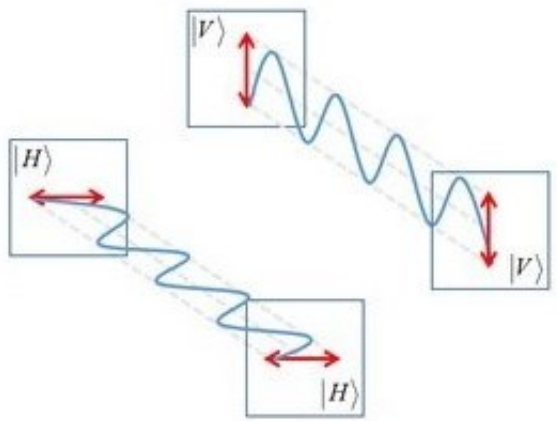
$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad |a|^2 + |b|^2 = 1 \qquad (1)$$

con $a, b \in \mathbf{C}$.
Si possono eseguire misure che proiettano $|\psi\rangle$ sulla base $|0\rangle, |1\rangle$.
Il risultato di questa operazione non é deterministico.
La probabilitá di ottenere il risultato $|0\rangle$ é $|a|^2$ .
La probabilitá che si ottenga il risultato $|1\rangle$ é $|b|^2$.



# Introduzione

*Esempio 1* I due livelli di energia dell'atomo di idrogeno possono essere presi come base per uno spazio vettoriale complesso H.
*Esempio 2* Gli stati di polarizzazione (orizzontale e verticale= di un fotone sono un altro esmpio di base per uno spazio vettoriale complesso H.




Un generico vettore in questo spazio puó essere scritto nella forma:

$$|\psi\rangle = a|H\rangle + b|V\rangle \quad (2)$$

# Introduzione

Consideriamo alcuni semplici processi implementabili quantisticamente:

**Fattorizzazione a numeri interi** Impossibile per i computer digitali fattorizzare grandi numeri che sono i prodotti di due numeri primi di dimensioni quasi uguali.
Il computer quantistico con 2n qubit può fattorizzare numeri con lunghezze di n bit (binario)

**Quantum database search** Esempio: per cercare un informazione in un datodatabase non ordinato Computer quantistico impiegherebbere ordini di grandezza di tempo inferiori ad un computer classico.

# Introduzione

**Simulazioni** di meccanica quantistica per esempio nell'ambito della chimica, scienza dei materiali, nanotecnologia, biologia e medicina. Il computer può calcolare milioni di variabili contemporaneamente. Tutti i computer attuali sono limitati dalla bassa velocità delle simulazioni di tipo meccanico-quantistico.

**Crittografia** Capace di decifrare codici estremamente complicati Crittografia RSA Utilizza in genere numeri con oltre 200 cifre

# Introduzione

Per dare un'idea dello sforzo dedicato a questa impresa, ricordiamo qui solo alcuni dei passi miliari della ricerca che ha portato alla concettualizzazione e prototipazione del computer quantistico.

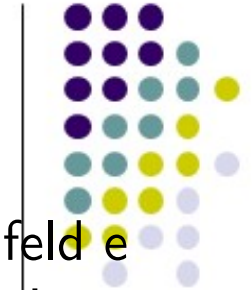
**1973** - Alexander Holevo pubblica un articolo che mostra che n qubit non può contenere più di n bit classici di informazioni.

**1976** - Roman Ingarden mostra che la teoria dell'informazione di Shannon non può essere generalizzata direttamente al caso quantistico.

**1981** - Richard Feynman stabilisce che è impossibile simulare in modo efficiente un'evoluzione di un sistema quantistico su un computer classico.

**1985** - David Deutsch descrive la prima macchina quantistica universale.

**1993** - Dan Simon introduce un algoritmo che contiene le idee principali poi sviluppate nell'algoritmo di factorizzazione di Peter Shor.
**1994** - Peter Shor propone l'algoritmo per fattorizzare rapidamente interi di grandi dimensioni. L'algoritmo di Shor potrebbe in principio invalidare molti dei sistemi alla base della moderna crittografia.
**1995** - Shor propone il primo schema per la correzione di errori quantistici.
**1996** - Lov Grover, presso Bell Labs, inventa l'algoritmo di ricerca di database quantistici.



**1997** - David Cory, A.F. Fahmy, Timothy Havel, Neil Gershenfeld e Isaac Chuang pubblicano i primi articoli su computer quantistici basati sulla risonanza di spin di massa o su complessi termici.
**1998** - Dimostrazione del primo computer NMR a 2 qubit funzionante all'Università della California, Berkeley.

...

**2001** - Il primo computer NMR a 7 qubit funzionante viene presentato all'Almaden Research Center di IBM. Prima esecuzione dell'algoritmo di Shor.

...

**2019** - Google ha proposto un nuovo algoritmo quantistico capace di operare in presenza di rumore (quantum approximate optimisation algorithm QAOA)

# Introduzione

Ricordiamo allo stesso modo solo alcune delle numerose soluzioni tecnologiche proposte:

- Superconduttori (inclusi computer quantistici registrati su SQUID)
- Trappole ioniche
- Risonanza magnetica nucleare su molecole in soluzione
- Quantum dots
- Laser su ioni galleggianti (nel vuoto))
- Elettrodinamica quantistica in cavità (CQED)
- Magneti molecolari
- Electron Spin Resonance con fullerene
- Kane NMR a stato solido (a base di silicio)

# Introduzione

Sono ancora numerose le sfide tecnologiche su cui i ricercatori si stanno impegnando.

Per esempio tra i limiti già menzionati alla fattibilità del computer quantistico è quello che i sistemi quantistici sono intrinsecamente rumorosi: non possiamo controllarli con precisione e non possiamo descriverli con precisione.

Per apprezzare questa limitazione, descriveremo un'ipotesi ottimistica di rumore quantistico (faremo una stima del limite inferiore del rumore) che consentirebbe il calcolo quantistico e un'ipotesi pessimistica che non lo consentirebbe (corrispondente ad una stima del limite superiore del rumore).