# QUANTUM COMPUTING

Così come alla base dell'informatica classica vi sono le leggi della fisica tradizionale, sfruttate per permettere ai calcolatori di elaborare, trasferire e memorizzare dati e informazioni, allo stesso modo per l'informatica quantistica sono utilizzate leggi della fisica quantistica.

Questo comporta grandi differenze nel genere di problemi che vengono affrontati e il metodo per risolverli.

Una prima differenza è che l'informatica classica è una scienza deterministica, quindi da determinati dati e tramite un determinato algoritmo si ottiene sempre lo stesso risultato; al contrario l'informatica quantistica è una scienza probabilistica, cioè dagli stessi dati ed algoritmo non è detto che si ottenga lo stesso risultato, quindi, per verificare quale risultato è quello effettivamente corretto, è necessario ripetere più volte l'esperimento/calcolo e vedere con quanta probabilità si ottiene ogni risultato e considerare quello con la maggiore.

Inoltre l'informatica quantistica vede la sua applicazione per la risoluzione di problemi di diverso tipo, ad esempio problemi con complessità computazionale esponenziale, mentre per un semplice calcolo come potrebbe essere "1+2", risulterebbe meno adatta.

Infatti per eseguire un calcolo, un computer quantistico probabilmente risulta più lento rispetto ad un computer classico, ma la grande qualità del computer quantistico è la possibilità di effettuare più calcoli contemporaneamente, in parallelo.

Questo ci fa capire che i computer quantistici probabilmente non sostituiranno completamente i computer tradizionali, ma semplicemente verranno utilizzati per affrontare quei problemi che questi ultimi non riuscirebbero a risolvere in tempi utili.

## PRINCIPI

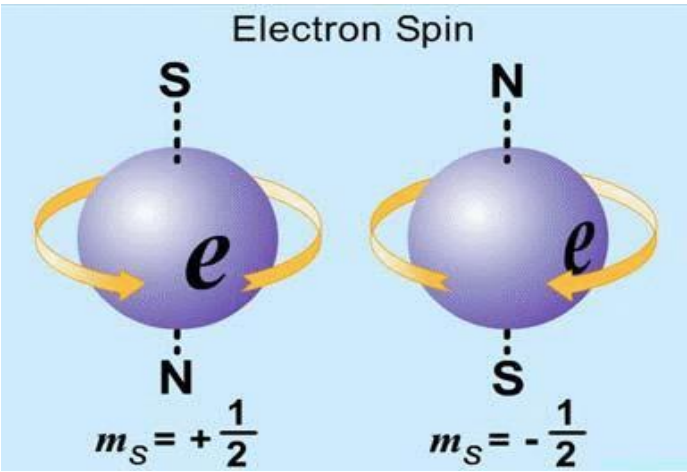
I principi fondamentali su cui si basa l'elaborazione quantistica sono:

- "**il principio di indeterminazione**"
- "**il principio di sovrapposizione degli stati**"
- "**l'entanglement quantistico**"

**QUBIT**

Il qubit (abbreviazione di quantum bit) è l'unità di informazione quantistica, l'equivalente del bit dell'informatica classica.

Questo si misura tramite lo "spin" che la particella ha rispetto al proprio orbitale (https://www.youtube.com/watch?v=Ch2nz8Ujrnk&feature=youtu.be).




Rispetto al "bit classico", il bit quantistico offre una maggiore versatilità e potenzialità di calcolo.

Mentre il bit classico può assumere solamente un valore ben definito ("0" o "1", "acceso" o "spento"), il qubit può assumere anche valori sovrapposti.

In base al Principio di indeterminazione di Heisenberg, un elemento quantistico – quale il qubit – non avrà mai uno stato (valore) ben definito, ma avrà valori sovrapposti e indeterminabili. Infatti essendo per noi impossibile determinare con certezza il valore di un qubit, finchè non viene misurato, non possiamo neanche dire che esso valga 0 o 1, ma una sovrapposizione di tutti i possibili valori che esso potrebbe assumere, quindi anche sia 0 che 1 allo stesso tempo.

Infatti considerando un registro composto da 3 bit fisici, esso può contenere esattamente uno degli 8 diversi valori possibili: in altre parole esso può trovarsi in una delle otto possibili configurazioni 000, 001, 010, ..., 111, rappresentazioni binarie dei numeri da 0 a 7.

A differenza di ciò, un registro quantistico composto da 3-qubit è in grado di contenere tutti gli 8 valori contemporaneamente in una sovrapposizione quantistica.

Il fatto che 8 valori differenti possano essere fisicamente presenti in contemporanea nello stesso registro è una diretta conseguenza delle proprietà dei qubit e ha delle grandi implicazioni dal punto di vista della Teoria dell'Informazione.

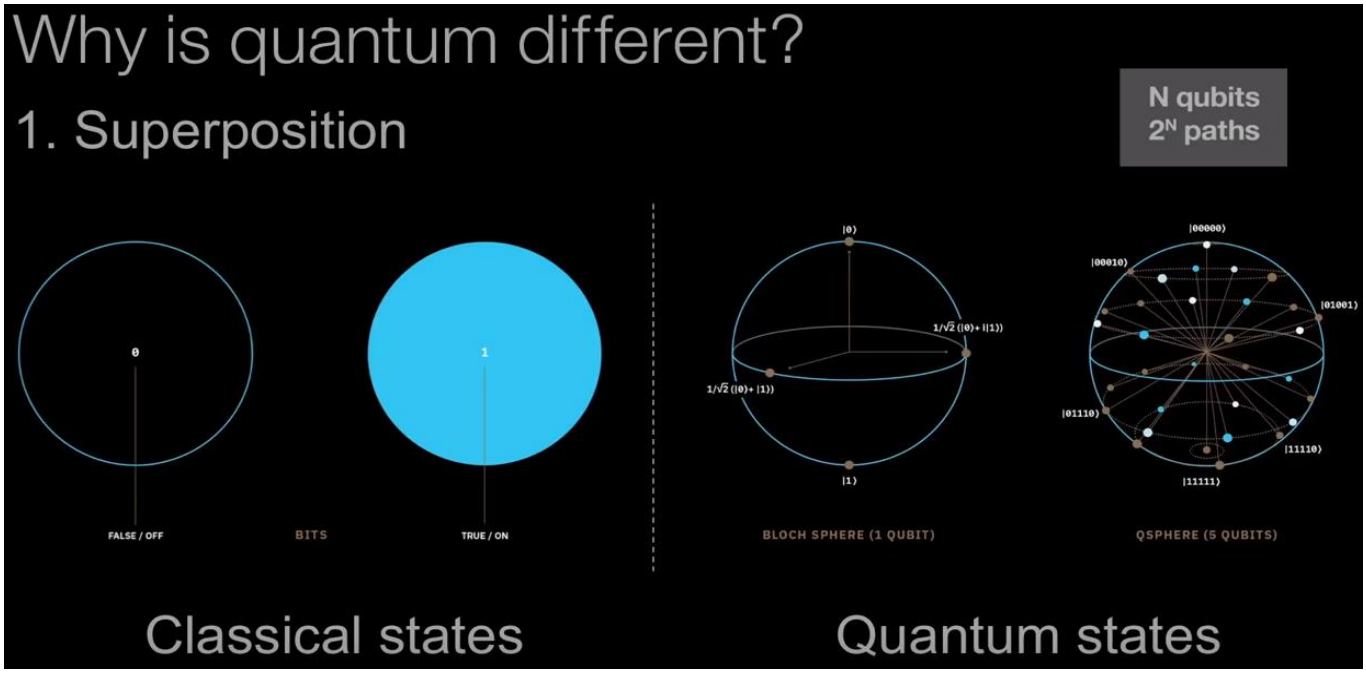
Se aggiungessimo più qubit al registro la sua capacità di memorizzare informazioni crescerebbe in maniera esponenziale: 4 qubit possono immagazzinare fino a 16 valori nello stesso tempo, ed in generale L qubit sono in grado di conservare 2^L valori contemporaneamente.

Un registro di 250-qubit, composto essenzialmente di 250 atomi, sarebbe capace di memorizzare più numeri contemporaneamente di quanti siano gli atomi presenti nell'Universo conosciuto.

Un dato senza dubbio scioccante. In termini pratici, però, quando misuriamo il contenuto di un registro siamo in grado di vedere solamente uno dei valori della sovrapposizione: ciò rappresenta sicuramente un problema nel caso di quantistica applicata a problemi tradizionali molto semplici.

Ma nel caso in cui dovessimo effettuare un calcolo quantistico più complesso, che consista di più passaggi e pertanto più operazioni sui registri, il vero vantaggio del computer quantistico inizierebbe a manifestarsi: quando un registro contiene una sovrapposizione di molti valori differenti, infatti, un calcolatore quantistico è in grado di effettuare operazioni matematiche su tutti questi contemporaneamente, allo stesso costo in termini computazionali dell'operazione eseguita su uno solo dei valori. E il risultato sarà a sua volta una sovrapposizione coerente di più valori.

In altre parole: è possibile eseguire un massiccio calcolo parallelo ad un costo computazionale irrisorio rispetto a quello richiesto dai calcolatori tradizionali, che avrebbero bisogno per compiere la stessa operazione di ripetere il calcolo 2^N volte o di poter contare su 2^N processori paralleli.




**PRINCIPIO DI INDETERMINAZIONE**

Questo principio è stato enunciato da Werner Karl Heisenberg ed è un fondamento della fisica quantistica.

Heisenberg sostiene che non è possibile conoscere con precisione e certezza tutte le caratteristiche riguardanti una particella in un preciso istante: tanto meglio si conosce, ad esempio, la posizione, tanto peggio possiamo sapere la velocità della particella (e viceversa).

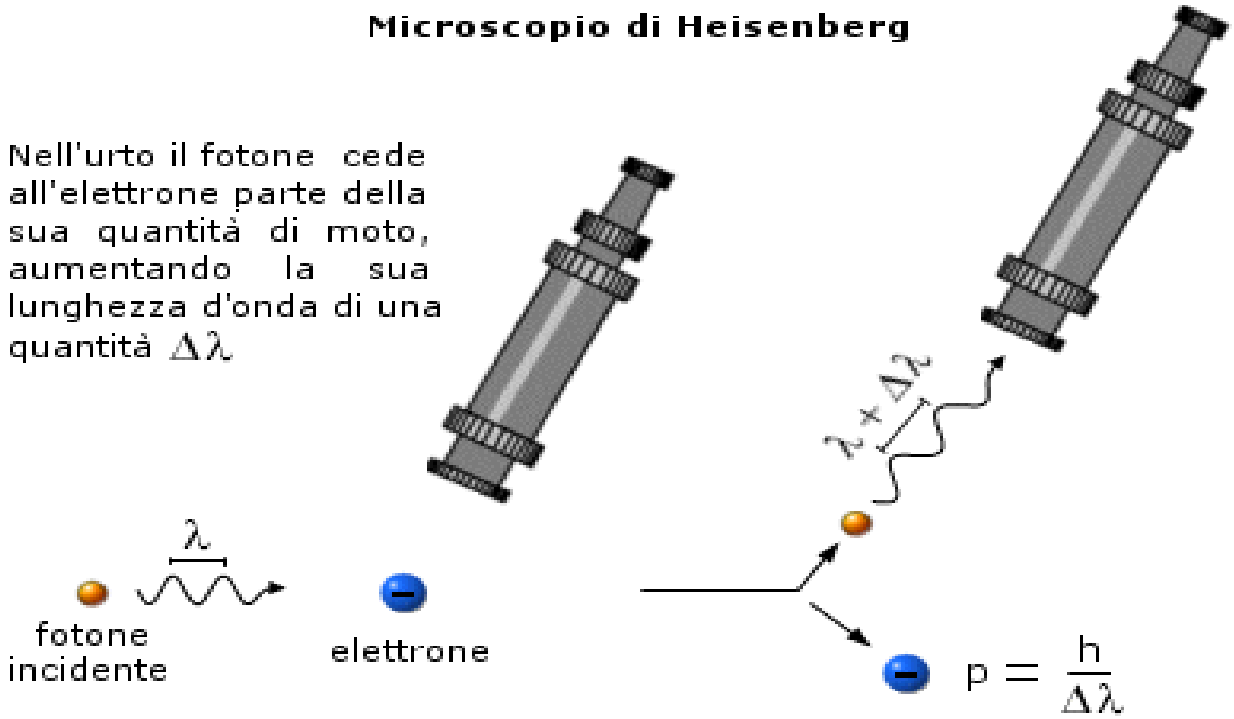
Per comprendere meglio questo principio si deve pensare al mondo del microcosmo ed analizzare, per esempio, un elettrone.

Per conoscere con precisione sia la sua posizione che la sua velocità ci "basterebbe" riuscire a vederlo, ma ciò è impossibile ad occhio nudo e neanche tramite un microscopio.

Allora dobbiamo usare delle radiazioni più potenti, quali i raggi X.

Però parte della energia dei fotoni viene trasmessa agli elettroni che repentinamente cambiano la loro velocità e quindi si comportano come particelle; è chiaro, allora, che essi hanno perso le caratteristiche ondulatorie iniziali e quello che si osserva sullo schermo è una distribuzione di elettroni che non è più equivalente a quella iniziale.

Come si può capire, questo fenomeno riguarda solo i corpi e le particelle a livello microscopico, mentre lo stesso principio non si riscontra per quelle a livello macroscopico: per questo non è ancora chiaro quale sia la dimensione minima di un oggetto al di sopra della quale il suo comportamento può essere descritto dalla fisica classica e non più da quella quantistica, e viceversa.




Per illustrare meglio questo principio Erwin Schrödinger ideò un esperimento teorico, noto come il paradosso del gatto do Schrödinger.

La condizione sperimentale è semplice da descrivere. Supponiamo di avere un gatto chiuso in una scatola dove un meccanismo (col quale il gatto non può ovviamente interferire) può fare o non fare da grilletto all'emissione di un gas velenoso. Per entrambe le situazioni la probabilità è esattamente del 50%.

Secondo Schrödinger, visto che è impossibile sapere, prima di aprire la scatola, se il gas sia stato rilasciato o meno, fintanto che la scatola rimane chiusa il gatto si trova in uno stato indeterminato: sia vivo sia morto.

Solo aprendo la scatola questa "sovrapposizione di stati" si risolverà, in un modo o nell'altro. La vita del gatto è di fatto nelle nostre mani: può sembrare paradossale, ma il senso è che l'osservazione determina il risultato dell'osservazione stessa.

**PRINCIPIO DI SOVRAPPOSIZIONE DEGLI STATI**

Questo principio è alla base del qubit ed afferma che non è possibile rappresentare un sistema quantico come un singolo stato, ma come sovrapposizione di tutti gli stati che esso può assumere.

Per questo che un qubit non rappresenta solo 0 o 1, ma anche tutti gli stati e le combinazioni intermedi a questi due valori.

Però tutto questo vale fino a quando noi non andiamo a misurare effettivamente il valore della particella: infatti a questo punto noi misureremo solo un determinato stato della particella, ovvero quello in cui essa si trova al momento della misurazione.

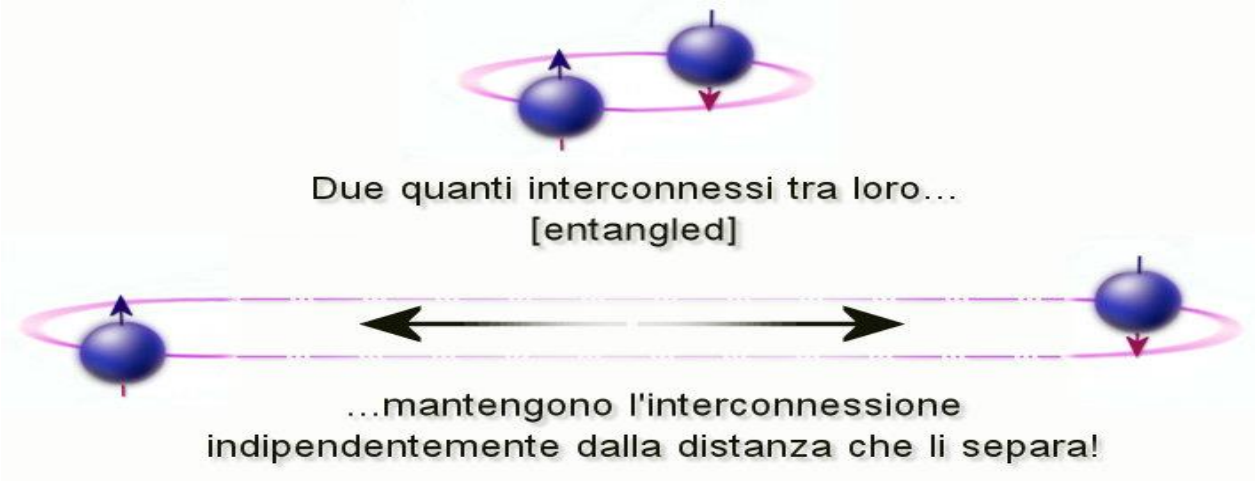
Tale valore potrebbe non essere lo stesso se effettuiamo un'altra misurazione, anche subito dopo.

**ENTANGLEMENT**

L' entanglement è un fenomeno alla base della fisica quantistica, ma che tutt'ora rimane misterioso e non completamente compreso.

Il concetto di entanglement (intreccio) è basato sull'assunzione che gli stati quantistici di due particelle microscopiche A e B inizialmente interagenti possano risultare legati tra loro in modo tale che, anche quando le due particelle vengono poste a grande distanza l'una dall'altra, la modifica che dovesse occorrere allo stato quantistico della particella A istantaneamente avrebbe un effetto misurabile sullo stato quantistico della particella B.

Esperimento quasar (https://www.focus.it/scienza/spazio/entanglement-quantistico-un-importante-test).




**TELETRASPORTO QUANTISTICO**

Il teletrasporto quantistico sfrutta il fenomeno dell'entanglement per trasferire in sicurezza i dati da un posto ad un altro.

Questo trasferimento è istantaneo e, basandosi sull'entanglement, non ha limiti di spazio.

Infatti, come già detto, prese due particelle legate tra loro (entangled) e poste a qualunque distanza tra loro, mantengono un legame: se una di esse viene messa in un sistema quantico con una terza particella, subisce una modifica, ma, immediatamente, anche quella legata alla prima subirà la stessa modifica, in questo modo siamo riusciti a trasferire l'informazione che volevamo.

Esempio:

*Diciamo che Alice è una ricercatrice nel laboratorio A, e Bob un suo collega nel laboratorio B. Hanno una coppia di fotoni (AB) entangled, che sono stati creati insieme nel laboratorio di Alice, e successivamente Bob ne ha preso uno e se l'è portato via.*

*Alice ha inoltre un terzo fotone, T, che desidera teletrasportare. Crea dunque un sistema speciale con il fotone A e il fotone T; lo misura e ottiene un risultato. Dato che A era entangled con B Bob può misurare la sua particella che ora ha lo stesso stato quantico che aveva la particella T nel laboratorio A.*

Però notiamo subito che la particella T è stata messa in sistema con la particella A, quindi a questo punto Alice non ha più a disposizione l'informazione contenuta in T, che invece è in possesso di Bob.

## APPLICAZIONI DELL'INFORMATICA QUANTISTICA

Ci sono certamente tantissimi ambiti in cui un computer quantistico potrebbe trovate applicazione, questi sono tra i più importanti:

**Sicurezza informatica:** la così elevata potenza di calcolo dei computer quantistici porterà sicuramente a dei cambiamenti nell'ambito della sicurezza informatica.

Infatti gli attuali algoritmi di cifratura sfruttano delle funzioni matematiche che sono difficilmente invertibili, poiché non esiste una vera e propria formula, ma si deve procedere per tentativi (brute force).

Questi algoritmi, quindi, richiedono un enorme complessità computazionale per la risoluzione degli algoritmi, e non esiste nessun calcolatore in grado di arrivare ad un risultato in tempi utili.

Ma con un computer quantistico si riuscirebbe ad arrivare ad una soluzione in pochi secondi, poiché questo è in grado di provare tutte le combinazioni contemporaneamente, e ciò comporterebbe al crollo di tutta la sicurezza informatica che oggi consociamo.

Per evitare che si presenti questo problema, man mano che la ricerca nell'ambito dell'informatica quantistica progredisce, sono già in fase di sviluppo diversi algoritmi di sicurezza, questa volta però di tipo quantistico, che, quindi, sfruttano proprietà della fisica quantistica per accertarsi che, durante un trasferimento di dati, nessuno li abbia intercettati e men che meno che possa accedere ad essi decodificandoli.

**Settore farmaceutico:** lo sviluppo di un computer quantistico porterebbe grandi vantaggi anche in ambito medico/farmaceutico.

Infatti per sviluppare nuovi farmaci, i ricercatori devono la combinazione di diverse molecole per trovare quella che con le proprietà migliori per contrastare una determinata malattia.

Il numero di combinazioni che si devono prendere in analisi è ovviamente enorme, e l'informatica tradizionale richiede molto tempo per trovare quella corretta, ma, al contrario, un computer quantistico potrebbe prendere in analisi tutte le combinazioni contemporaneamente e trovare immediatamente quella corretta.

## SVILUPPO ATTUALE COMPUTER QUANTISTICO

Attualmente la ricerca si è spinta a realizzare computer quantistici con processori 56 qubit, nel caso dell'IBM, e addirittura 72, per quanto riguarda Google.

Attualmente è anche possibile provare gratuitamente il computer quantistico dell'IBM, che mette anche a disposizione un editor grafico per la realizzazione di algoritmi quantistici.

Inoltre è stato sviluppato dalla D-Wave Systems un computer quantistico ad addirittura 2000 qubit, che per risolvere i problemi ha implementato un algoritmo in grado di mappare tutte le possibili soluzioni di un problema, partendo anche una grande quantità di dati in input, ed assegnando ad ognuna di esse un determinato stato quantico, per poi escludere le soluzioni meno probabili.

Però il D-Wave è stato attaccatto e criticato da molti studiosi e ricercatori dell'ambito, sostenendo che in realtà non è un vero e proprio computer quantistico, poiché solo per certi generi di problemi esso ha delle prestazioni degne di un computer quantistico, per molti altri "*mostra prestazioni paragonabili a quelle di un comune computer con un avanzato processore Intel*", come sostiene Matthias Troyer, docente dell'Università ETH di Zurigo.

SITOGRAFIA

Spin e qubit (inglese):

https://www.youtube.com/watch?v=g_IaVepNDT4&feature=youtu.be

Computer quantistico:

https://it.wikipedia.org/wiki/Computer_quantistico

Elaborazione quantistica:

https://it.wikipedia.org/wiki/Informatica_quantistica

Principio di indeterminazione:

https://it.wikipedia.org/wiki/Principio_di_indeterminazione_di_Heisenberg

Video teletrasporto quantistico:

https://youtu.be/ijmT9cB4nFw

Video spin particelle:

https://youtu.be/Ch2nz8Ujrnk

Qubit e porte quantiche:

https://systemscue.it/elaborare-qubit-computer-quantistico/8984/

Programmazione computer quantistico:

http://scienzapertutti.infn.it/component/content/article?id=947:0173-qual-e-il-linguaggio-di-programmazione-che-si-deve-usare-su-un-computer-quantistico

Paradosso del gatto di Schrödinger:

https://it.wikipedia.org/wiki/Paradosso_del_gatto_di_Schr%C3%B6dinger

Applicazioni future quantum computer

https://it.businessinsider.com/che-cose-il-computer-quantistico-e-perche-rivoluzionera-interi-settori-industriali-come-farmaceutica-meteorologia-ecc/

Sviluppo computer quantistico:

https://www.ai4business.it/intelligenza-artificiale/computer-quantistico/