23. Febbraio

Quantum computing: per una medicina quantistica

Parte prima le sfide del calcolo quantistico

Il concetto di computer quantistico fu proposto per la prima volta dal fisico teorico e premio Nobel **Richard Feynman** nel 1981.
Feynman raggiunse la maggiore età agli albori della meccanica quantistica, quando gli scienziati iniziarono a riconoscere che *atomi, elettroni, luce e altri oggetti sub-nanoscopici*, elementi costitutivi di ogni cosa nell'universo, obbediscono a ***regole fondamentalmente diverse*** rispetto agli oggetti della vita quotidiana.

A differenza, ad esempio, di una palla, che segue le semplici regole della meccanica classica, gli elettroni si comportano simultaneamente come particelle e onde e la loro posizione non può essere definita con esattezza.

L'intuizione di Feynman fu che per comprendere veramente il mondo della meccanica quantistica, e il funzionamento generale dell'universo stesso, sarebbe stato necessario costruire un computer che funzionasse secondo le stesse leggi. ***"La natura non è classica, accidenti"***, disse***, "e se vuoi fare una simulazione della natura, faresti meglio a renderla meccanica quantistica".***

L'intuizione di Feynman si è rivelata lungimirante. Negli oltre quattro decenni successivi, i computer che seguono il design ***"classico"*** hanno trasformato completamente il pianeta: i cellulari tascabili di oggi sono un milione di volte più potenti dei massicci personal computer desktop degli anni '80.

La legge di Moore, la previsione secondo cui il numero di transistor su un chip di computer sarebbe raddoppiato ogni due anni, ha continuato a essere ampiamente valida nell'industria dei semiconduttori, nonostante le molteplici previsioni della sua scomparsa. I migliori supercomputer odierni possono gestire un ***quintilione, ovvero un miliardo di miliardi di operazioni al secondo.*** Tuttavia, mentre questa rivoluzione continua a maturare, è diventato sempre più chiaro che alcuni calcoli sono e rimarranno al di là persino dei migliori computer classici.

Questo perché le tecnologie informatiche esistenti sono vincolate dalla premessa di base su cui operano. Tutte le forme di elaborazione classica, che si tratti di un abaco, di un portatile personale o di un cluster di macchine ad alte prestazioni in una struttura di sicurezza nazionale, seguono quella che gli studiosi chiamano ***logica booleana.***

In questo sistema, l'unità di base delle informazioni è un ***bit***, che è un oggetto che può assumere uno dei due stati, convenzionalmente indicati come **0 o 1**. Sebbene questo sistema abbia dimostrato di essere altamente efficiente per molti tipi di calcoli, non può eseguire quelli di

complessità eccessiva, come la *fattorizzazione di un numero di mille cifre*, il calcolo della dinamica di reazione di *una molecola con centinaia di atomi* o la risoluzione di determinati tipi di problemi di ottimizzazione comuni in molti campi.

Al contrario, sfruttando la ***meccanica quantistica,*** il calcolo quantistico non ha gli stessi vincoli. Una lezione della fisica quantistica, sorprendente e controintuitiva, è che le particelle possono esistere in una combinazione simultanea di più stati. Di conseguenza, invece dei bit, con la loro operazione 0-O ***il calcolo quantistico utilizza un bit quantistico, o qubit, che è un sistema che può essere simultaneamente negli stati 0 e 1.***
Questa capacità di entrambi allo stesso tempo, nota come sovrapposizione, conferisce un enorme vantaggio computazionale, che aumenta quando ***più qubit*** lavorano insieme. Mentre un computer classico deve elaborare uno stato dopo l'altro in sequenza, un computer quantistico può esplorare molte possibilità in parallelo.

Immagina di cercare di trovare il percorso corretto in un labirinto: un computer classico deve provare ogni percorso uno alla volta; un computer quantistico può esplorare più percorsi simultaneamente, il che lo rende ordini di grandezza più veloce per determinati compiti.

È importante notare che, contrariamente alla semplificazione popolare, un computer quantistico non è semplicemente un enorme set di computer classici che lavorano in parallelo. Sebbene vi siano esponenzialmente molte possibili risposte che possono essere esplorate tramite un processore quantistico, alla fine è possibile misurare solo una combinazione. Derivare una soluzione da un computer quantistico richiede quindi una programmazione intelligente che amplifichi la risposta corretta. Le macchine quantistiche potrebbero portare a innovazioni paragonabili a quelle che ora si prevede arriveranno dall'intelligenza artificiale.

Una sfida importante è capire come costruire processori quantistici che siano abbastanza grandi e stabili da produrre risultati coerenti per problemi significativi. Tali processori tendono a essere estremamente sensibili al loro ambiente e possono essere facilmente influenzati da cambiamenti di temperatura, vibrazioni e altri disturbi, che possono portare a una serie di errori nel sistema.

Poiché la fedeltà computazionale si basa sui ***qubit*** che mantengono la coerenza, i ricercatori stanno investendo molto in metodi per migliorare la qualità dei ***qubit,*** tra cui nuovi design, processi di fabbricazione dei chip e tecniche per correggerne gli errori.
Attualmente, esiste un'ampia gamma di approcci alla loro progettazione***,*** ognuno con i suoi vantaggi e svantaggi.

In linea di principio, qualsiasi sistema meccanico quantistico (atomi, molecole, ioni, fotoni) potrebbe essere trasformato in un ***qubit.*** In pratica, fattori come la ***producibilità***, la ***controllabilità***, le ***prestazioni e la velocità di calcolo*** determinano i percorsi più praticabili. Gli sforzi principali di oggi includono ***qubit superconduttori***, ***atomi neutri***, ***fotonici*** e ***trappola ionica***. Non è chiaro in questa fase iniziale quale, se ce ne sarà uno, si rivelerà un successo.

Oltre alla costruzione del processore, altre sfide includono come confezionare i qubit, trasmettere i loro segnali ed eseguire le applicazioni. I ricercatori devono utilizzare ***frigoriferi criogenici***, che possono raffreddare i qubit superconduttori fino a millesimi di grado sopra lo zero assoluto, per fornire un ambiente ultrafreddo, buio e silenzioso per il funzionamento. Le competenze su questi componenti altamente specializzati provengono da fonti diverse in molti paesi.

Oggi, ci sono varie aziende di calcolo quantistico **"full-stack",** tra cui Amazon, Google, IBM e QuEra, che stanno cercando di integrare componenti in un prodotto finale.
In breve, il calcolo quantistico oggi affronta una moltitudine di sfide e incognite, e lo sviluppo continuo richiederà una serie di innovazioni ingegneristiche.
Ciò che è chiaro è che affinché uno qualsiasi degli approcci abbia successo, deve essere affidabile, scalabile e conveniente.
To be continued…

Qubit, contrazione di quantum bit, è il termine coniato da Benjamin Schumacher per indicare il bit quantistico ovvero l'unità di informazione quantistica.
Per definire il qubit è indispensabile introdurre innanzi tutto il concetto nuovo di quanto di informazione, cioè la più piccola porzione in cui una qualsiasi informazione codificata può essere scomposta; è quindi l'unità di misura dell'informazione codificata.
Così come il bit è il quanto di informazione della computazione classica, la computazione quantistica si basa su un concetto analogo: il quantum bit. Al pari del bit, il qubit è un oggetto matematico con sue specifiche proprietà. Il vantaggio nel trattare i qubit come entità astratte risiede nella libertà di costruire una teoria generale della computazione quantistica che non dipende dagli specifici sistemi utilizzati per la sua realizzazione.
Un qubit, o bit quantistico, è l'unità di informazione utilizzata per codificare i dati nel quantum computing e può essere inteso come l'equivalente quantistico del bit tradizionale utilizzato dai computer classici per codificare le informazioni in formato binario.
Il termine "qubit" è attribuito al fisico teorico americano Benjamin Schumacher. I qubit sono generalmente, anche se non esclusivamente, creati manipolando e misurando particelle quantistiche (i più piccoli elementi costitutivi dell'universo fisico), come fotoni, elettroni, ioni intrappolati, circuiti superconduttori e atomi.
Grazie alle proprietà uniche della meccanica quantistica, i computer quantistici utilizzano i qubit per archiviare più dati rispetto ai bit tradizionali, migliorando notevolmente i sistemi crittografici ed eseguendo calcoli molto avanzati che richiederebbero migliaia di anni (o sarebbero impossibili) da completare anche per i supercomputer classici.
Basati sui qubit, i computer quantistici potrebbero presto rivelarsi fondamentali nell'affrontare molte delle più grandi sfide dell'umanità, tra cui la cura del cancro e altre ricerche in campo medico, il cambiamento climatico, il machine learning e l'intelligenza artificiale (AI).

Glossario quantistico “essenziale”

Cos'è un qubit?

Un qubit, o bit quantistico, è l'unità di informazione utilizzata per codificare i dati nel quantum computing e può essere inteso come l'equivalente quantistico del bit tradizionale utilizzato dai computer classici per codificare le informazioni in formato binario.

Quantum computing

Il quantum computing, che rappresenta la nuova frontiera della potenza di calcolo, utilizza tecnologie specializzate, tra cui hardware e algoritmi che sfruttano i principi della meccanica quantistica, per risolvere problemi complessi che i computer o i supercomputer classici non possono risolvere (o non possono risolvere abbastanza rapidamente).

Qubit vs. bit

Esistono molti tipi diversi di bit e qubit, ma tutti i qubit devono rispettare le leggi della fisica quantistica ed essere in grado di esistere in una sovrapposizione quantistica.

bit

Nell'informatica tradizionale o classica, un singolo bit può essere pensato come un'informazione binaria, indicata come 0 o 1. I computer moderni in genere rappresentano i bit come una tensione elettrica o un impulso di corrente (o come lo stato elettrico di un circuito flip-flop).

In questi sistemi, quando non c'è corrente, il circuito può essere considerato spento, e questo stato è rappresentato come uno 0. Quando c'è corrente, il circuito è considerato acceso, e questo stato è rappresentato come un 1.

Il termine "bit" è una parola che deriva da "binary digit" e i bit binari sono la base fondamentale di tutta l'informatica. Sia che si tratti di registrare un video digitale, di animare un modello 3D o di utilizzare un'applicazione per il calcolo, tutti i dati, dai sistemi operativi ai software, sono costituiti da un codice binario, ovvero da un insieme di bit. Un byte informatico è composto da otto bit, il numero minimo di bit necessario per trasmettere un singolo carattere testuale in binario.

I bit possono essere rappresentati elettricamente, ad esempio facendo passare (o non facendo passare) corrente attraverso un chip di silicio. I bit possono anche essere rappresentati fisicamente, come un foro o l'assenza di un foro in un foglio di carta, come nelle vecchie schede perforate. Qualsiasi sistema a due livelli in cui lo stato del sistema può essere descritto solo tramite una delle due posizioni potenziali (ad esempio, su o giù, sinistra o destra, acceso o spento) può essere utilizzato per rappresentare un bit.

qubit

Sebbene le tecnologie quantistiche utilizzino effettivamente il codice binario, i dati quantistici derivati da un sistema quantistico, come un qubit, codificano i dati in modo diverso dai bit tradizionali, con alcuni notevoli vantaggi. I ricercatori hanno stabilito diversi modi per creare qubit o utilizzare sistemi quantistici presenti in natura come qubit. Tuttavia, in quasi tutti i casi, i computer quantistici richiedono una refrigerazione estrema per isolare i qubit e prevenire le interferenze.

Teoricamente, qualsiasi sistema quantistico a due livelli può essere utilizzato per creare un qubit. Un sistema quantistico è descritto come a due livelli quando alcune proprietà del sistema possono essere misurate in posizioni binarie, come su o giù. Anche i sistemi quantistici multilivello possono essere utilizzati per creare qubit, a condizione che due aspetti del sistema possano essere isolati efficacemente per produrre una misura binaria. Così come i computer tradizionali possono utilizzare più tipi di bit, come la corrente elettrica, la carica elettrica o i fori (o non fori) in un foglio di carta per il calcolo con schede perforate, i computer quantistici possono utilizzare più tipi di bit. Alcuni bit sono più adatti a determinate funzioni, e un computer quantistico avanzato utilizzerà probabilmente una combinazione di tipi di bit per ottenere operazioni diverse.

Poiché ogni bit può rappresentare uno 0 o un 1, accoppiando due bit di informazione, possiamo creare fino a quattro combinazioni binarie uniche:

1. 00
2. 01
3. 10
4. 11

Mentre ogni bit può essere uno 0 o un 1, un singolo qubit può essere uno 0, un 1 o una sovrapposizione. Una sovrapposizione quantistica può essere descritta sia come 0 che come 1, o come tutti i possibili stati compresi tra 0 e 1, perché rappresenta effettivamente la probabilità dello stato del qubit.

A livello quantistico, la probabilità dei qubit viene misurata come funzione d'onda. L'ampiezza di probabilità di un qubit può essere utilizzata per codificare più di un bit di dati ed eseguire calcoli estremamente complessi se combinato con altri qubit.

Quando si elabora un problema complesso, come la fattorizzazione di un numero primo molto grande, i bit tradizionali sono vincolati quando si tratta di grandi quantità di informazioni. I bit quantistici si comportano diversamente. Poiché i qubit possono contenere una sovrapposizione, un computer quantistico che utilizza i qubit può calcolare un volume di dati molto più grande.
Per comprendere la differenza tra i bit e i qubit, immagina di trovarti al centro di un labirinto intricato. Per uscire dal labirinto, un computer tradizionale dovrebbe risolvere il problema mediante una "forzatura", provando ogni possibile combinazione di percorsi per trovare l'uscita. Questo tipo di computer utilizzerebbe i bit per esplorare nuovi percorsi e ricordare quali sono i vicoli ciechi.

Al contrario, un computer quantistico potrebbe, in senso figurato, ricavare in una sola volta una vista d'insieme del labirinto, testando più percorsi simultaneamente e rivelando la soluzione corretta. In realtà, i qubit non "testano più percorsi" contemporaneamente. I computer quantistici misurano invece le ampiezze di probabilità dei qubit per determinare un risultato. Poiché queste ampiezze funzionano come onde, si sovrappongono e interferiscono tra loro. Quando le onde asincrone si sovrappongono, eliminano di fatto le possibili soluzioni a problemi complessi e l'onda o le onde coerenti realizzate presentano la soluzione.

Entanglement quantistico?

Descritto per la prima volta da Einstein come "azione spettrale a distanza", l'entanglement quantistico è un fenomeno in cui due qubit (o due o più particelle quantistiche) si intrecciano in modo tale che lo stato di una particella non può essere descritto indipendentemente dallo stato dell'altra, qualunque sia la distanza tra di loro.

Le sfide dei qubit

Pur essendo potenti, i qubit sono anche molto instabili. Per funzionare, i qubit devono essere raffreddati a una temperatura solo di una frazione di grado superiore allo zero assoluto, più bassa di quella dello spazio.