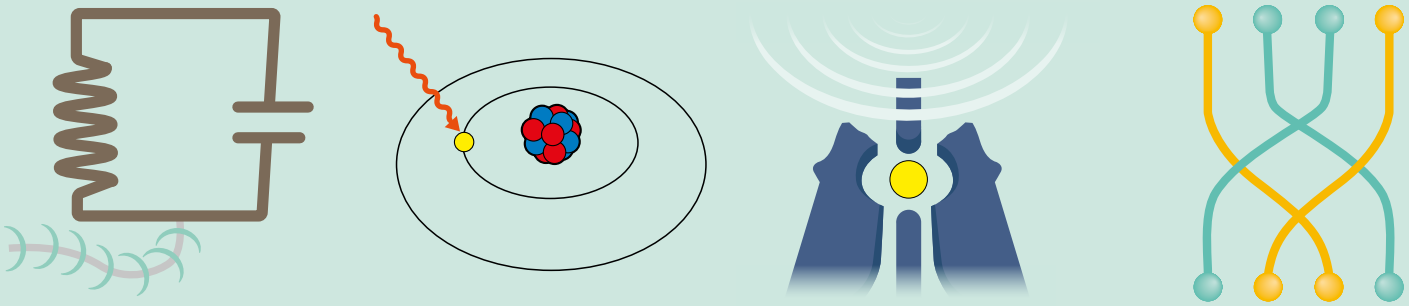
Vantaggio o supremazia?

La ricerca sui computer quantistici

di Massimo Palma



Anelli superconduttori

Una corrente elettrica in assenza di resistenza oscilla avanti e indietro in un circuito ad anello. Iniettando un segnale di microonde si crea una sovrapposizione di stati quantistici.

Pro: Velocità. Basato su tecnologia a semiconduttori già esistente.

Contro: Lo stato quantistico collassa facilmente. Il circuito deve essere raffreddato.

Trappole ioniche

Atomi carichi elettricamente (cioè ioni) hanno livelli energetici quantistici che dipendono dalla posizione degli elettroni.
Con dei laser opportuni è possibile "raffreddare" e "intrappolare" gli ioni in sovrapposizioni di stati quantistici.

Pro: Stati molto stabili, con il più basso tasso di errore per operazione logica.

Contro: Processo lento. Servono molti laser.

Quantum dot

"Atomi artificiali" ottenuti aggiungendo un elettrone a dei piccoli frammenti di silicio puro. Mediante microonde si controlla lo stato quantistico dell'elettrone.

Pro: Stabilità. Basato su tecnologia a semiconduttori già esistente.

Contro: Non si riesce a creare correlazioni quantistiche fra molti dot.

Qubit topologici

Il comportamento di elettroni che si propagano attraverso strutture semiconduttrici artificiali può essere descritto in termini di "quasi-particelle". L'intreccio delle loro traiettorie puo essere utilizzato per codificare informazione quantistica.

Pro: Possibilità di ridurre notevolmente gli errori.

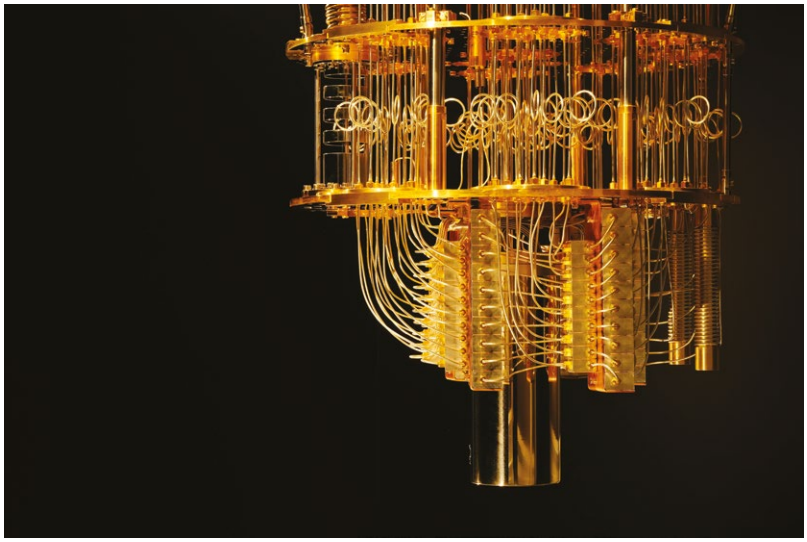
Contro: Esistenza non ancora confermata.

a.
Panoramica delle piattaforme fisiche già utilizzate o candidate per la realizzazione di dispositivi di calcolo quantistici.

Non è semplice orientarsi tra i titoli di testa di pagine web e di riviste online che spesso, con toni sensazionalistici, parlano dell'avvento della cosiddetta "supremazia quantistica" e farsi una idea chiara delle promesse e delle reali possibilità aperte nel campo dei calcolatori (o computer) quantistici. La stessa comunità scientifica oscilla tra grandi entusiasmi e grande prudenza. Oggi, con la realizzazione dei primi veri calcolatori quantistici e con un crescente interesse per le ricadute scientifiche ed economiche che ne derivano, è bene avere un quadro equilibrato e chiaro di cosa dobbiamo realisticamente attenderci dai computer quantistici nell'immediato futuro.
Il primo passo per comprendere cosa si intende per supremazia quantistica è quello di chiarire il concetto di complessità di un algoritmo. Per algoritmo si intende la sequenza di operazioni necessarie per risolvere un problema. La complessità di un problema viene misurata dal numero di operazioni dell'algoritmo che lo risolve in funzione della lunghezza dei dati del problema. Se codifichiamo i dati di un problema in stringhe di bit, ovvero in sequenze di numeri binari che possono assumere il valore 0 o 1, è immediato, ad esempio, rendersi conto che il numero di operazioni necessarie per

b./c.
David Deutsch (a sinistra) ha introdotto il concetto di computer quantistico e di macchina di Turing quantistica nel 1985. A destra, Richard Josza. L'algoritmo di Deutsch-Josza del 1992 è il primo esempio di algoritmo quantistico.

sommare due numeri è direttamente proporzionale alla lunghezza delle stringhe che li codificano, mentre per moltiplicarli è necessario un numero di operazioni proporzionale al quadrato della loro lunghezza. Le operazioni di un algoritmo che opera su stringhe di bit vengono descritte in termini delle cosiddette "porte logiche" (AND, OR, ecc.).
Un calcolatore è semplicemente un sistema fisico – l'hardware – che elabora i dati seguendo le indicazioni di un programma che esegue l'algoritmo – il software. Per essere più concreti, in un moderno calcolatore i bit sono codificati nella differenza di potenziale ai capi degli elementi circuitali delle singole celle di memoria e le porte logiche che agiscono su questi bit cambiano lo stato logico di tali celle secondo regole che dipendono dal programma. In altre parole, un computer traduce una sequenza di operazioni logiche in una sequenza di stati del suo hardware. È importante notare che se un calcolatore è più veloce di un altro significa semplicemente che essi attraversano la stessa sequenza di stati con velocità differenti, ovvero eseguono lo stesso algoritmo – la stessa sequenza di operazioni – ma uno dei due è più veloce nel compiere le singole operazioni.
Nel giro di pochi decenni abbiamo assistito a uno spettacolare processo di miniaturizzazione dei circuiti integrati che costituiscono l'hardware dei moderni computer. Le dimensioni delle singole celle di memoria stanno raggiungendo rapidamente la scala atomica. Quando le singole celle di memoria del computer raggiungono dimensioni microscopiche il loro comportamento non può più essere descritto dalle leggi della fisica classica, ma deve essere descritto dalle leggi della meccanica quantistica. In particolare, per il principio di sovrapposizione, un singolo bit può trovarsi contemporaneamente nei suoi stati logici 0 e 1, in altre parole diventa un quantum bit – ovvero un qubit.
La grande intuizione dei padri del calcolo quantistico fu che un hardware quantistico può eseguire algoritmi impossibili da far eseguire da un hardware classico, in quanto può elaborare in parallelo i dati codificati nella sovrapposizione dei suoi stati interni.
I primi algoritmi quantistici furono proposti da David Deutsch e Richard Jozsa alla fine degli anni '80 e nei primi anni '90. Se tali algoritmi ci appaiono oggi di interesse puramente accademico, essi ebbero il merito di attrarre l'attenzione della comunità scientifica interessata ai fondamenti della meccanica quantistica. Il vero punto di svolta ebbe luogo in quegli anni con la scoperta da parte di Peter Shor di un algoritmo efficiente per la fattorizzazione. Ciò che rende importante l'algoritmo di Shor è il fatto che la fattorizzazione è classicamente un problema complesso, nel senso che gli algoritmi classici noti richiedono un tempo molto lungo per fattorizzare grandi numeri. Inoltre, sul piano pratico, molti protocolli crittografici di uso comune si basano sulla complessità degli algoritmi di fattorizzazione (vd. p. 33, ndr).
La nascita dei primi algoritmi quantistici pose la necessità di capire quali problemi potessero essere risolti efficientemente su un computer quantistico. È importante notare che sebbene un calcolatore quantistico, potendosi trovare in una sovrapposizione coerente di stati interni, possa elaborare in parallelo più dati, a causa del collasso del suo stato a seguito di una misura solo parte del risultato del processo di calcolo è accessibile. Come conseguenza l'attenzione si concentrò inizialmente su algoritmi quantistici in grado di calcolare in modo efficiente proprietà globali della funzione di interesse, ad esempio la sua periodicità, piuttosto che i suoi singoli valori al variare dell'input. In pratica quasi tutti i primi algoritmi



d.
Particolare del Quantum System One, il computer quantistico della IBM.

(incluso l'algoritmo di Shor) si basavano sul calcolo efficiente del periodo di opportune funzioni. Quale sia la classe di problemi che sicuramente sono risolubili in modo più efficiente da parte di un calcolatore quantistico descrivibile in termini di porte logiche quantistiche resta tuttora un problema aperto.
Un cambiamento di prospettiva ha iniziato ad aver luogo negli ultimi anni con l'avvento dei primi dispositivi di calcolo quantistici realizzati da IBM, Google, Rigetti, DWave, ecc. Non entreremo nel merito delle diverse architetture o delle diverse piattaforme fisiche utilizzate per realizzare questi processori, quello che è importante sottolineare è che tutti questi calcolatori operano nel regime cosiddetto *Noisy intermediate-scale quantum (*NISQ). In tale regime i calcolatori quantistici sono ben lontani dal lavorare in condizioni di "*fault tolerance*", cioè, a causa delle loro dimensioni ancora ridotte, non è possibile eseguire programmi quantistici di correzione degli errori dovuti alla presenza del rumore ambientale, che distrugge rapidamente le sovrapposizioni coerenti di stati di qubit. In altre parole, l'ambiente fa collassare in tempi brevi lo stato dei qubit, trasformandoli a tutti gli effetti in bit classici e rendendo impossibile l'esecuzione di algoritmi quantistici.
In questo nuovo scenario nascono due nuove parole d'ordine: "supremazia quantistica" e "vantaggio quantistico". La prima cosa che i costruttori di questi primi calcolatori hanno voluto dimostrare è che, sebbene in regime NISQ, essi possono già risolvere problemi praticamente intrattabili su un calcolatore classico, regime appunto noto con il nome di supremazia quantistica. Diversi gruppi, fra cui Google, Xanadu e USTC (China) hanno dichiarato di aver raggiunto la supremazia quantistica. Tuttavia, si tratta di problemi dimostrativi, di interesse pratico molto contenuto.
Un secondo approccio più pragmatico è quello di progettare algoritmi che integrano programmi destinati a computer classici con programmi destinati a computer quantistici per risolvere problemi specifici, tipicamente di ottimizzazione, preoccupandosi non tanto di mostrare la supremazia o il carattere assolutamente ottimale dell'algoritmo rispetto agli algoritmi classici, quanto di migliorare rispetto all'esistente, ovvero di raggiungere il cosiddetto vantaggio quantistico. In questo spirito si stanno sviluppando algoritmi interamente classici ispirati ad algoritmi quantistici. Questa linea di ricerca è di grande interesse potenziale per la ricerca in chimica, in medicina, ma anche nell'ottimizzazione di processi di organizzazione aziendale.
Chiudiamo menzionando la ricerca tesa a esplorare algoritmi quantistici basati non sul paradigma delle porte logiche ma su modelli di reti neurali quantistiche. L'esplorazione di tale approccio promette interessanti sviluppi a breve.

Biografia
Gioacchino Massimo Palma ha lavorato presso l'Imperial College di Londra e il Clarendon Laboratory di Oxford. È direttore del Dipartimento di Fisica e Chimica "Emilio Segrè" dell'Università di Palermo. Si interessa di teoria quantistica dell'informazione dai primi anni '90.

10.23801/asimmetrie.2022.33.6