IL GIORNALE DI VICENZA

diffusione:23162
tiratura:30879

Stasera a Valdagno

La quantistica stravolge i computer

• Simone Montangero, docente a Padova, spiega che questo ramo della fisica può affrontare problemi complessi

GIANMARIA PITTON

Se di questi tempi è l'intelligenza artificiale l'argomento principe in ambito scientifico e tecnologico, al secondo posto viene il computer quantistico. Nell'uno e nell'altro caso, però, non è facile entrare nei meandri di innovazioni che promettono di rivoluzionare la vita quotidiana. Nel 2025, in cui si celebra il centenario della meccanica quantistica, offre un approccio accessibile il libro "Il computer impossibile. Come il calcolatore quantistico cambierà il mondo" (Raffaello Cortina editore) di Giuliano Benenti, Giulio Casati e Simone Montangero. Quest'ultimo, professore ordinario all'università di Padova, dove dirige il Centro di simulazione e calcolo quantistico, e all'Università di Ulm, sarà oggi alle 20.30 a Palazzo Festari a Valdagno per l'ultimo appuntamento della "Via delle scienze".

Professore, partiamo dalla base. Cos'è il computer quantistico e come si differenzia da quello tradizionale?
Nel computer quantistico cambia tutta la fisica che c'è sotto il "cofano". Il calcolatore tradizionale si basa sull'elettromagnetismo, sulle correnti elettriche, che conosciamo dall'Ottocento e usiamo dal Novecento per fare la tecnologia che ci circonda. L'unità minima di informazione è il bit, che può essere 1 oppure 0, se passa o non passa corrente. Può anche essere un singolo atomo, in due stati differenti.

Invece con la meccanica quantistica?
L'atomo si comporta in maniera diversa da come siamo abituati, perché può stare in due stati diversi contemporaneamente: non un bit, ma un qbit. È controintuitivo, ma tantissimi esperimenti ormai dimostrano che le cose stanno proprio così.

E questo perché migliora le prestazioni di un computer?
Perché cambiano le regole del gioco. Posso fare degli algoritmi che risolvono i problemi in modo diverso, specie i problemi molto complessi. Ad esempio, se un'azienda deve distribuire delle squadre di tecnici in un territorio e raggiungere diverse destinazioni nel minore tempo possibile, può rivelarsi un rompicapo molto difficile. Il computer quantistico ha la capacità di esplorare molte configurazioni nello stesso momento.

Quando sarà disponibile?
Ci sono già, ma sono limitati, hanno poca memoria. Anche negli anni Cinquanta i calcolatori c'erano, ma avevano poca memoria rispetto ai computer moderni. Stiamo facendo progressi di anno in anno, alcune aziende li stanno testando per capire come programmarli.

È questione di materiali non adatti?
Costruirli è complicatissimo. Gli oggetti quantistici esistono in sovrapposizione di stati, una particella, ad esempio, può stare al di qua e al di là di una barriere contemporaneamente, è l'"effetto tunnel" per cui è stato dato l'ultimo Nobel per la fisica. Ma gli stati sono fragilissimi, se qualcosa, come un fotone, interagisce con gli oggetti quantistici, questi decadono in uno dei due stati.

Quindi bisogna isolarli.
Sì, però man mano che aumentiamo il numero di atomi, isolarli è difficilissimo. Al momento arriviamo a macchine da 50 a 200 qbit, ma stiamo migliorando. Dare un orizzonte temporale è rischioso.

Un esempio di un'altra applicazione?
Pensiamo alla chimica. Ora siamo in grado di manipolare singoli atomi, ma le cose sono più complesse quando interagiscono nelle molecole, o nelle grandi molecole. Col computer quantistico si possono simulare i processi chimici di grandi molecole, con risvolti in molti settori.

L'intelligenza artificiale sarà più efficiente?
Abbiamo già gli algoritmi per un'IA quantistica migliori di quella classica. Ma al momento un confronto è ingiusto, perché un computer quantistico perfetto ancora non c'è. In teoria, però, sarebbe ancora più potente. E se anche facesse le stesse cose di un'IA tradizionale, consumerebbe molta meno energia.

Il computer quantistico è più sostenibile?
Un supercalcolatore odierno consuma la stessa energia di una media cittadina, come Vicenza. Un computer quantistico di analoga potenza consumerebbe come un boiler.

Il fisico vicentino Federico Faggin ha inventato il microchip, che ha portato i computer ovunque, anche negli smartphone. Il computer quantistico arriverà a essere alla portata di tutti?
Le previsioni sono rischiose. Credo che non tutti ne avran-


Cultura&Spettacoli
La quantistica stravolge i computer

IL GIORNALE DI VICENZA

diffusione:23162
tiratura:30879

no bisogno. Forse sarà sufficiente avere dei computer quantistici al posto dei supercalcolatori, ai quali ci si collegherà per dare un'accelerazione quantistica ai propri calcoli. Forse però sì, li avremo in casa. Già ora la meccanica quantistica garantisce comunicazioni più sicure.

Perché le protegge dall'essere decifrate?
La crittografia si basa sullo scambio di chiavi per decifrare il messaggio. Ma c'è il rischio che la chiave sia intercettata. Utilizzando le leggi della meccanica quantistica, quindi gli stati quantistici di singoli atomi, si codificano messaggi tali che, se si prova a intercettarli, lo si vede subito, perché l'intercettazione altera gli stati. Cina, Stati Uniti, in parte anche l'Europa si servono di questo sistema. D'altra parte, anche il computer quantistico è una potenziale minaccia.

Perché?
L'informatico Peter Shor ha detto che un computer quantistico potrebbe facilmente violare tutto il sistema che usiamo oggi per crittografare i messaggi, che si basa sui numeri primi. Non è ancora possibile, ma bisogna prepararsi. L'hanno detto anche gli esperti del G7. È un pericolo, ma speriamo prima di riuscire, con il computer quantistico, a fare cose che fanno bene.

Simone Montangero Docente ordinario all'università di Padova