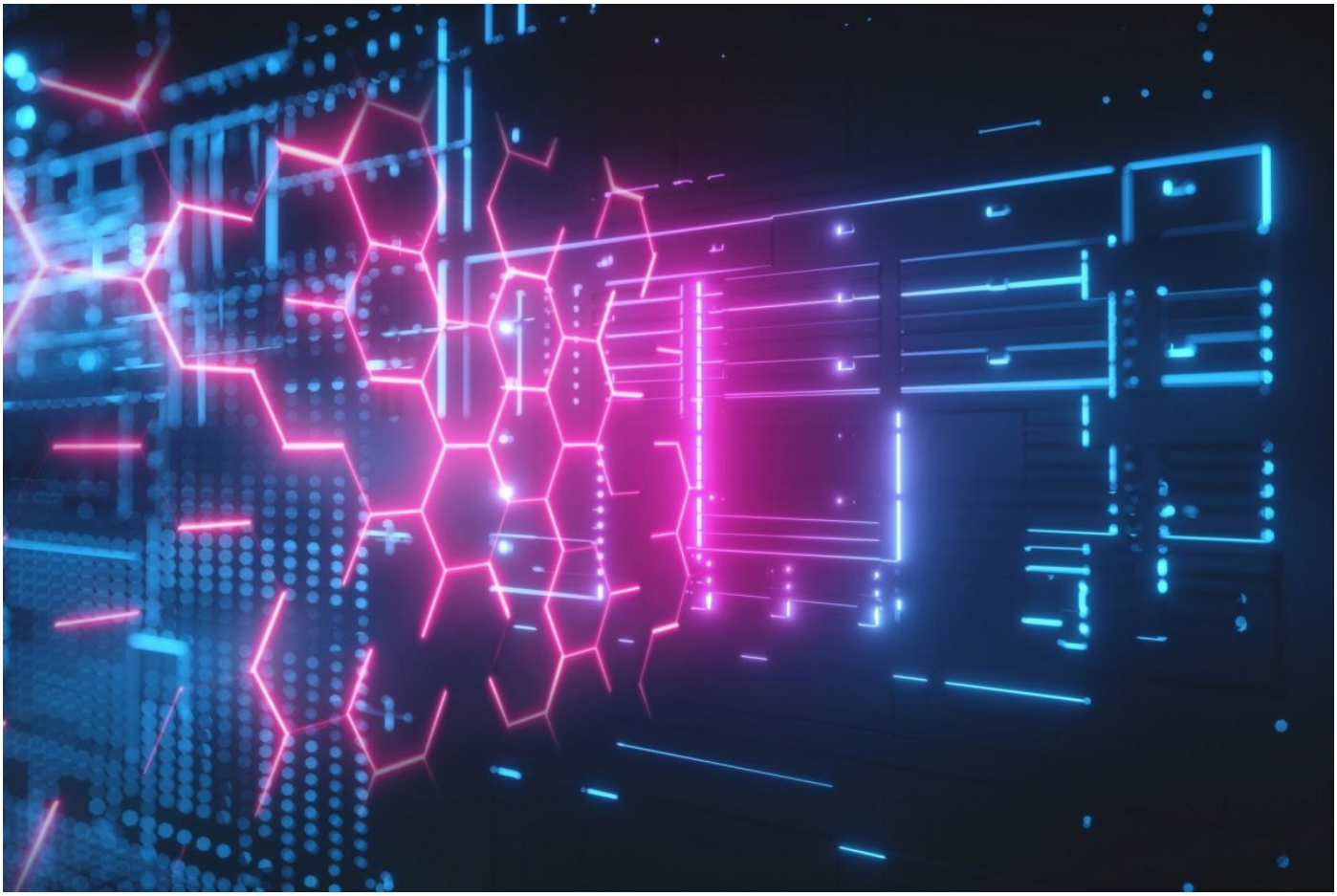

Le frontiere della computazione II – I computer quantistici

Cara lettrice, caro lettore,
nell'articolo di gennaio abbiamo parlato di uno dei limiti delle macchine di Turing: attualmente, ci sono problemi la cui risoluzione richiede un numero di operazioni che cresce in modo più che polinomiale rispetto alla lunghezza dell'input. Alcuni di questi problemi, però, si possono risolvere rapidamente utilizzando tecniche di computazione alternative alle macchine di Turing. In questo articolo parleremo di una di esse: il quantum computing.

UN SALTO DI PARADIGMA

Le macchine di Turing e tutti i modelli di calcolo equivalenti si basano su una concezione dei bit legata alla fisica classica: a prescindere da come siano fisicamente realizzati all'interno di un computer, i bit possono assumere solo due valori: 0 o 1. La fisica classica non è però l'unico paradigma che conosciamo: per descrivere dei fenomeni che avvengono a livello atomico e subatomico, la fisica quantistica fornisce dei modelli più accurati.
La descrizione quantistica dello spin di una particella, per esempio, è un'alternativa al bit classico. Infatti lo spin può assumere i due valori su (indicato anche con $|1\rangle$) e giù (indicato anche con $|0\rangle$), ma anche tutte le combinazioni $a|1\rangle + b|0\rangle$ al variare dei numeri reali a e b che verificano $a^2+b^2=1$. Questa proprietà è nota come principio di sovrapposizione. I valori a^2 e b^2 indicano la percentuale di ciascuno stato. Quindi, per

esempio, una particella che si trova nello stato $\frac{1}{\sqrt3}|1\rangle + \sqrt{\frac{2}{3}}|0\rangle$ si trova per $\frac{1}{3}$ nello stato su e per $\frac{2}{3}$ nello stato giù.

I BIT QUANTISTICI

Un qubit, ovvero un bit quantistico, è l'unità elementare di informazione codificata dallo spin di una particella. Di conseguenza, un qubit si può trovare in uno degli stati puri $|0\rangle$ o $|1\rangle$ o in uno stato del tipo $a|1\rangle + b|0\rangle$. Utilizzando i qubit al posto dei bit è possibile progettare algoritmi che permettono una certa misura di calcolo non deterministico, cioè che permette di eseguire più operazioni in contemporanea.

I BIT QUANTISTICI E LE MISURE

Alla fine di una computazione quantistica, per vedere quale risutato è codificato in un qubit dobbiamo effettuare una misurazione. Però il risultato di una misura è un bit classico che non può presentare una sovrapposizione di stati. Di conseguenza, nel momento in cui misureremo il valore di un qubit, esso assumerà solo uno dei due valori $|1\rangle$ o $|0\rangle$. Questo però non è un ostacolo per lo sviluppo degli algoritmi quantistici. Anzi, permette di sfruttare altre proprietà della fisica quantistica, come l'entanglement.

L'ENTANGLEMENT

L'entanglement quantistico è un altro fenomeno presente a livello microscopico ma non in quello macroscopico. Secondo questo principio, esistono sistemi il cui stato non è descrivibile singolarmente, ma solo come sovrapposizione di più stati. Un esempio di stato entangled a due qubit è $\frac{|11\rangle + |00\rangle}{\sqrt2}$.
Una delle conseguenze dell'entanglement è che, osservando una delle componenti di questo sistema, per esempio quella $|11\rangle$, l'intero stato viene determinato. In altre parole, allo stesso tempo in cui una componente è misurata, viene determinato anche il valore di tutte le altre.

SUPREMAZIA QUANTISTICA

I bit quantistici e l'entanglement permettono di svolgere compiti impossibili per i computer classici, come il trasporto istantaneo di informazioni a grandi distanze (il cosiddetto teletrasporto quantistico). Inoltre consentono di sviluppare algoritmi alternativi a quelli classici per la risoluzione di problemi che con i computer tradizionali richiedono tempi di calcolo immensi. Un esempio è l'algoritmo di fattorizzazione Shor, pubblicato nel 1994, che permette la risoluzione di un problema classicamente difficile in un tempo polinomiale su un computer quantistico. Un algoritmo simile è stato implementato nell'ottobre 2020 dal team di AI Quantum: il computer quantistico realizzato dal team di Google ha eseguito in soli 200 secondi un calcolo che, eseguito su un supercomputer tradizionale, avrebbe richiesto circa diecimila anni.

APPLICAZIONI E LIMITI DEI COMPUTER QUANTISTICI

Nonostante i recenti successi dei computer quantistici, non dobbiamo aspettarci di poterli acquistare presto come dei comuni personal computer. I computer quantistici, infatti, devono realizzare al loro interno condizioni fisiche molto particolari necessarie per creare i qubit. Inoltre, i calcoli sui computer quantistici non sono più veloci di quelli sui tradizionali chip classici. Di conseguenza, per tutti i problemi già risolubili velocemente, cioè con algoritmi polinomiali, i computer tradizionali rimangono imbattuti. Invece, si ipotizza che i computer quantistici verranno utilizzati solo su richiesta per applicazioni molto specifiche, per esempio quelle legate alla sicurezza informatica.
Nonostante i computer quantistici siano ancora in fase di sviluppo, possiamo già simulare l'esecuzione di algoritmi su un computer quantistico per esempio utilizzando il linguaggio Q#, un'estensione di C# per il quantum computing.

RIFERIMENTI

- Nel 2020 è stato effettuato un primo esperimento sul teletrasporto quantistico. Puoi leggerne un reportage giornalistico alla pagina https://tg24.sky.it/scienze/2020/12/29/teletrasporto-quantistico-record
- Una discussione approfondita sulle potenzialità e sui limiti del quantum computing si trova sull'articolo di Scott Aaronson pubblicato nel 2008 su Scientific American: https://www.cs.virginia.edu/~robins/The_Limits_of_Quantum_Computers.pdf
- Per iniziare a programmare in Q#, Microsoft fornisce un tutorial reperibile alla pagina https://docs.microsoft.com/it-IT/azure/quantum/tutorial-qdk-explore-entanglement
- I computer quantistici sono presentati nel Capitolo 1 e nel Capitolo 4 del volume del V anno di #NetGeneration.