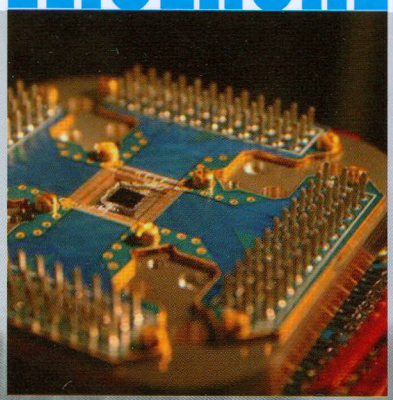
BRESCIA RICERCHE



N. 65 - anno XVIII
dicembre 2008

spedizione in abbonamento postale,
70% filiale di Brescia
autorizzazione del Tribunale
di Brescia, n. 17/1990

I Computer Quantistici

Fausto Borgonovi
Dipartimento di Matematica e Fisica,
Università Cattolica del Sacro Cuore, Brescia

E' molto difficile immaginare la vita nel XXI secolo senza il computer. Oggi, grazie ad esso, possiamo compiere operazioni sino a 50 anni fa inimmaginabili. Possiamo trasferire soldi da un conto corrente ad un altro o pagare una bolletta con un semplice click attraverso l'home banking, prenotare in pochi minuti un viaggio a Capoverde dopo aver controllato in tempo reale le condizioni meteorologiche, trovare l'indirizzo di una via in una qualsiasi città del mondo (con relativa fotografia, "street view" in gergo). I grandi motori di ricerca presenti nella rete globale permettono inoltre di eseguire ricerche dettagliate su ogni tipo di argomento: su cosa è stato fatto, su cosa si conosce e soprattutto su cosa ancora c'è da fare. Una grande ed immensa biblioteca multimediale è presente, a nostra disposizione 24 ore su 24 e ci evita il ricorso alla nostra labile memoria o ad affannose ricerche bibliografiche su polverosi scaffali di immense biblioteche. Una gigantesca quantità di informazioni in ogni istante a disposizione dell'intera umanità (magari anche incontrollate oppure false, ma anche in altri tempi la situazione non era troppo diversa) con l'unico vincolo di avere a disposizione un computer (magari veloce) per poterne usufruire in modo completo. Per chi fa ricerca il computer rappresenta un modo per entrare in contatto immediato con tutto quello che di simile si sta facendo in tutto il mondo, per comunicare i propri risultati e leggere gli altrui, oltre che, ovviamente, un indispensabile strumento di calcolo scientifico.

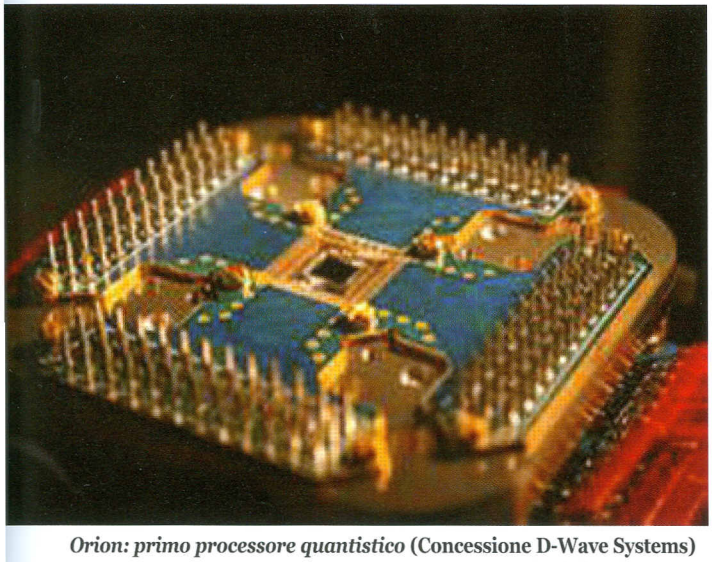
Al di là dell'uso attuale, è proprio questo il motivo per cui i computer sono stati creati: questi immensi ammassi di luci colorate, pulsanti e suoni, così come descritti nell'immaginario collettivo, dovevano avere una funzione di calcolo. Dovevano cioè supplire a quella mancanza di tempo che sarebbe servita all'uomo per compiere in modo deterministico e ripetitivo certe operazioni matematicamente elementari.

Il computer classico, ovvero il computer che abbiamo oggi a disposizione, utilizza per le sue innumerevoli operazioni sequenze di caselline, dette bit, che possono essere accese o spente (a seconda del passaggio o meno di corrente elettrica) e a cui si attribuisce un significato convenzionale di 0 oppure 1. Questa lunga, ma finita, sequenza di zeri ed uno (in gergo, una "stringa") rappresenta un numero scritto nell'alfabeto binario, detto appunto così per essere caratterizzato da una sola coppia di simboli. Nello stesso modo, i numeri come li intendiamo noi, sono scritti nel sistema decimale perché vengono usati dieci simboli differenti (come le dita delle nostre mani) : 0,1,...,9. Ogni operazione su un computer classico è una opportuna manipolazione di stringhe di 0 ed 1; mentre con algoritmo intendiamo una procedura che permetta, attraverso tale manipolazione, di risolvere certe tipologie di problemi.

Sempre rimanendo sul vago, due sono le caratteristiche di un computer classico a cui siamo maggiormente interessati. La prima è la velocità di calcolo e la seconda la miniaturizzazione dei computer stessi. Rispetto ai primi, vecchi computer, la moderna tecnologia ci offre oggigiorno strumenti incredibilmente più veloci, anche rispetto a quelli di un solo decennio fa, e incredibilmente più piccoli (oggetti che stanno sul palmo di una mano riescono a gestire con grande rapidità formidabili quantità di informazioni). Per quanto riguarda la prima delle due caratteristiche, nel 1965 Moore (fondatore della Intel) osservò che nel periodo 1959-1965 il numero dei transistor all'interno dei chip era raddoppiato ogni anno. Formulò allora la cosiddetta "legge (empirica) di Moore": ossia che le prestazioni dei microprocessori sarebbero raddoppia-

→

te di lì ad ogni anno a venire. Anche se ci furono alcune correzioni nei decenni successivi possiamo dire che, in linea generale, ancor oggi si assiste ad un raddoppio della frequenza dei microprocessori (in qualche modo una misura della velocità di calcolo) circa ogni 18 mesi. Di pari passo, ad un continuo aumento di tale velocità si è avuta una contemporanea riduzione volumetrica degli stessi fino quasi ad arrivare oggi non lontano dal raggiungimento della scala atomica.
E qui sorge un primo problema: la materia è costituita da atomi, ma gli atomi non sono palle da biliardo e soprattutto le leggi che ne determinano il comportamento non sono le leggi della meccanica classica (per intenderci le leggi della dinamica di Galileo e Newton che studiamo alle scuole Superiori). Un'opportuna teoria, detta "Meccanica Quantistica" e nata nella prima metà del XX secolo, descrive, con una perfezione e precisione strabilianti, difficilmente raggiunte in altri ambiti della fisica, il comportamento della materia su scala atomica.

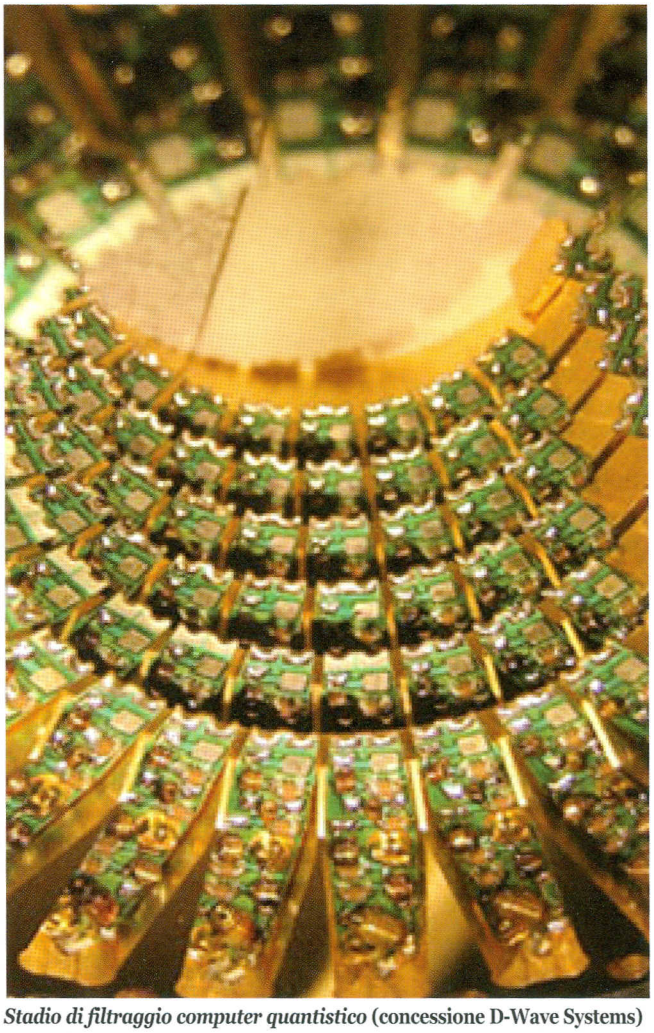


Orion: primo processore quantistico **(Concessione D-Wave Systems)**

Sono tante le caratteristiche inquietanti della Meccanica Quantistiche che turbarono i sonni di grandi fisici, tra i quali lo stesso Einstein, che pur tanti contributi determinanti aveva dato per la sua nascita. Una prima caratteristica importante è che, ad esempio, un elettrone all'interno di un atomo non può avere una qualsiasi energia a suo piacere: le possibili energie sono quantizzate, ovvero ne esiste solo un numero discreto. Il valore più basso si chiama energia dello stato fondamentale, quello immediatamente successivo primo stato eccitato, etc, etc. Una ulteriore caratteristica è quella che i fisici chiamano "spin" (perché inizialmente pensato in qualche modo legato ad una rotazione della carica su se stessa). Senza entrare nei dettagli, possiamo dire che questo spin, messo in un campo magnetico, può assumere solo due valori che chiameremo convenzionalmente + e - (oppure 1 e 0). Questa naturale discretezza della Meccanica Quantistica fa pensare immediatamente alla possibilità di utilizzare questi due stati discreti + e - per lo spin oppure lo stato fondamentale (0) ed il primo stato eccitato (1) di un elettrone all'interno di un atomo come possibili caselle o bit di un computer; ma le loro proprietà e caratteristiche risultano talmente diverse dai bit classici da aver coniato per loro un nuovo nome: "qubit" o "quantum-bit".
Per capire l'importanza e soprattutto la differenza tra il bit classico e quello quantistico occorre fare un passo indietro e considerare quelle che avevo chiamato caratteristiche inquietanti della Meccanica Quantistica.
Anche se lo spin di un elettrone può assumere solo due valori quando posto in un campo magnetico, questo è in realtà quello che si ottiene quando si effettua una misura dello stesso (o meglio del suo momento magnetico). E' il risultato della misura che fa assumere i due valori chiamati + e -. Se non si effettua alcuna misura il nostro sistema (ovvero l'elettrone) può tranquillamente vivere in una sovrapposizione dei due stati, ovvero essere nello stesso tempo un po' + e un po' - ed è solo attraverso il processo di misura che decide se essere + o -. La Meccanica Quantistica ci fornisce le leggi con cui stabilire la probabilità (di meglio non si sa fare) con cui lo spin dell'elettrone decide se essere in uno stato + oppure in uno stato - . Parafrasando Einstein, l'elettrone, o chi per lui, lancia i dadi per stabilire in che stato precipitare.
La possibilità di vivere, fino a prima della misura, in sovrapposizioni di stati apre la strada, in linea di principio, all'utilizzo senza precedenti di un massiccio calcolo parallelo su vasta scala. Per capire l'enormità della cosa facciamo presente che un semplice sistema costituito da circa 300 spin ha a sua disposizione 2 X 2 X 2.... (fatto 300 volte) stati quantistici. Questo esorbitante numero di stati (in notazione esponenziale circa 10^90) rappresenta la dimensione naturale in cui vive il sistema di 300 spin e se si volesse scrivere uno di questi stati su una stringa di un computer classico non basterebbero tutti gli atomi dell'universo (ci si può dunque immaginare che computer servirebbe per descrivere poi l'evoluzione di tale stringa). Per rappresentare e descrivere il comportamento, ovvero l'evoluzione di tale sistema, occorre necessariamente un apparato quanto-meccanico di 300 sistemi quantistici a due livelli: questa in sostanza la conclusione a cui arrivò il grande fisico americano R. Feynman nel 1982. I computer classici risultano assoluta-

→

mente inadeguati nella simulazione di un piccolissimo sistema quantistico nel senso che sono poco efficienti: l'aumento esponenziale del numero delle risorse disponibili (2 elevato alla 300) indica un dispendio di risorse enorme a fronte di una richiesta piuttosto esigua.
Ma non è solo nella simulazione di sistemi quantistici che i computer classici rivelano la loro inefficienza: due esempi solitamente citati sono il problema del commesso viaggiatore e la fattorizzazione dei numeri interi. Nel primo caso si tratta di calcolare il percorso minimo che un commesso viaggiatore deve compiere per raggiungere un certo numero N di città, interconnesse tra loro, senza passare due volte per la stessa città. La soluzione di un tale problema richiede un tempo esponenzialmente grande nel numero N e diventa praticamente intrattabile con un computer attuale anche per un numero modesto di città (ad esempio un migliaio). Il secondo problema, che sembra di natura squisitamente matematica, consiste nel determinare i numeri primi diversi da 1 che costituiscono un certo numero intero dato, ad esempio 21=7 X 3. Moltiplicare tra loro due numeri interi di qualche centinaio di cifre è un semplice esercizio per un qualsiasi computer classico. Il problema inverso, ovvero calcolare i fattori primi che compongono un numero intero di qualche centinaio di cifre,costituisce invece un problema intrattabile poichè il tempo di calcolo dipende, ancora una volta, in modo esponenziale dal numero delle cifre che costituiscono l'intero stesso. Perché questo problema è rilevante per la vita di tutti i giorni? Ad esempio, per proteggere i dati sui nostri computer, utilizziamo tecniche note come crittografie a chiave pubblica in cui le informazioni che vengono trasmesse sono formate da coppie di numeri primi che fattorizzano un numero molto grande, in genere di 256 cifre. Un eventuale truffatore, che riuscisse ad intercettare e leggere tale numero, per poter accedere ai nostri dati dovrebbe essere in grado di risalire ai fattori primi di tale numero, compito, come detto, arduo per un qualsiasi computer classico.
L'eventuale computer quantistico rimase però un puro concetto teorico sino a quando Peter Shor nel 1994 costruì il primo algoritmo quantistico dimostrando come sia possibile fattorizzare, su un computer quantistico, un numero costituito da qualche centinaio di cifre semplicemente utilizzando qualche centinaio di qubits. Il vantaggio rispetto ad un qualsiasi computer classico risiede nel fatto che si può sfruttare appieno il principio di sovrapposizione degli stati per far fare ad un ipotetico computer quantistico molte operazioni tutte in parallelo. Ogni operazione coinvolge cioè contemporaneamente tutti gli stati del sistema! Per mezzo di questo enorme parallelismo su grande scala una operazione così complessa come la fattorizzazione di un numero intero, che avrebbe richiesto un tempo esponenziale nel numero delle cifre dell'intero in questione, necessita in questo modo di un tempo (solo) polinomiale, ossia che cresce come una legge di potenza nel numero delle cifre.
Naturalmente il problema consiste tutto in due importanti caratteristiche di carattere teorico e pratico. La prima rappresenta la possibilità di mantenere, durante l'esecuzione del calcolo, il sistema in una sovrapposizione coerente di stati. La seconda consiste nell'essere in grado di riuscire a leggere il risultato, visto che in generale le risposte possono essere solo di tipo probabilistico. Mentre il secondo difficile compito è demandato alla bravura di chi costruisce particolari algoritmi, il primo dipende in modo cruciale dalle caratteristiche tecnico-teoriche del computer quantistico.
Facciamo ancora una volta un passo indietro per dire



Stadio di filtraggio computer quantistico **(concessione D-Wave Systems)**

→

due parole su cosa si intende esattamente con la frase: "permettere al computer quantistico di eseguire i calcoli contemporaneamente su tutti gli stati del sistema". Consideriamo, a tal fine, un qubit che sia un po' + (1) e un po' - (0), e chiamiamo il suo stato semplicemente |0> + |1>. Un secondo qubit può facilmente essere posto nello stesso stato sovrapposizione |0> + |1>. E' sempre possibile, e relativamente facile, creare uno stato del sistema del sistema |00> + |11> in cui cioè entrambi i qubit siano un po' + e un po' - . Questo stato prende il nome di stato entangled (intrecciato o non separabile) e introduce in modo nascosto quella che Einstein chiamava "la subdola azione a distanza". Cosa possiamo dire su questo stato? Innanzitutto che entrambi i qubit sono indeterminati (0 oppure 1), ma che se si esegue una misura sul primo qubit ottenendo 1 allora possiamo essere certi che, ovunque il secondo qubit si trovi, troveremo 1 anche per il secondo e analogamente se il risultato della prima misura fosse 0. Abbiamo cioè creato una correlazione tra qubit non necessariamente vicini, anche se, a voler guardare meglio le cose non vi è stata alcuna azione a distanza. Infatti, la misura sul primo qubit non cambia lo stato del secondo, semplicemente aumenta l'informazione in nostro possesso sul suo stato. Questo intreccio o entanglement, tipico della Meccanica Quantistica e sconosciuto nel mondo macroscopico in cui viviamo, è il principio base su cui si fonda il computer quantistico. La possibilità di operare contemporaneamente su tutti gli stati viene meno se l'entanglement viene meno. Perché mai questa particolarità dovrebbe venir meno? Perché il mondo in cui viviamo ed in cui leggiamo i risultati delle misure è un mondo classico in cui questo fenomeno non compare (sarebbe come ammettere, come diceva Schrodinger, uno dei padri fondatori della Meccanica Quantistica, che possa esistere un gatto che sia contemporaneamente un po' vivo e un po' morto). Qualunque interazione con l'ambiente esterno, osservazione o procedimento di misura fa sì che l'entanglement venga meno: a questo processo viene dato il nome di decoerenza ed è praticamente ineliminabile. Il meglio che possiamo fare è cercare di svolgere il calcolo quantistico in un tempo minore del tempo in cui il sistema perde questa fantastica proprietà di intreccio e diventa classico.

Fino ad oggi vari modelli di computer quantistico sono stati proposti, basati su atomi, ioni, elettroni, fotoni e anche correnti superconduttrici. Per essere davvero competitivi nella risoluzione di particolari problemi rispetto a quelli classici dovrebbero contenere qualche migliaio di qubits. Siamo ancora molto lontani da questa soglia e soprattutto dal riuscire ad evitare il fenomeno della decoerenza, che ineluttabilmente aumenta all'aumentare del numero dei qubits. Nonostante ciò la sfida è stata lanciata e speriamo che in tempi brevi siano disponibili delle tecnologie quantistiche in modo da tener vivo l'interesse delle grandi imprese nel finanziamento di questa importante ricerca del XXI secolo. ■