

Sono passati esattamente settanta anni dalla nascita di quello che è stato universalmente riconosciuto come il primo computer della storia – lo Z1 costruito dal tedesco Konrad Zuse nel 1939 – e da allora gli enormi sforzi profusi in termini di sviluppo e distribuzione hanno portato il computer a essere uno strumento indispensabile per un quarto della popolazione mondiale. Lo Z1 aveva una velocità di clock di circa un hertz, ovvero era in grado di eseguire un'operazione elementare (precisamente una commutazione tra due livelli logici) in un secondo, mentre la frequenza di un microprocessore singolo in un computer degli ultimi anni varia tra i due e i quattro gigahertz, il che significa che gli innumerevoli miglioramenti susseguitisi a un ritmo forsennato per settanta anni hanno portato a una potenza di calcolo un miliardo di volte maggiore rispetto a quella originaria.

Sarà possibile nei prossimi anni migliorare di altrettante volte le prestazioni dei computer attuali? A sentire le cifre precedenti nessuno, probabilmente, si sognerebbe nemmeno di porsi una simile domanda, considerato anche che un limite alla velocità di calcolo di un microprocessore è dato dall'incapacità di raffreddarsi che interviene a frequenze troppo alte e ne compromette le prestazioni. Ci sono invece buone possibilità che la risposta sia positiva grazie ai principi della meccanica quantistica, che permetterebbero di costruire macchine, i computer quantistici appunto, che rivoluzionando totalmente il funzionamento degli odierni calcolatori sarebbero in grado di sfiorare velocità inimmaginabili con la tecnologia attuale.

I nostri computer sono infatti basati sul bit, che rappresenta l'unità di informazione della computazione classica, il quale può assumere due valori, 0 o 1, che corrispondono, a livello materiale, rispettivamente a una tensione pari a 0 volt e a 5 volt del transistor, il meglio noto interruttore acceso/spento. Il quanto di informazione della computazione quantistica è invece il qubit (*quantum binary digit*), il quale tuttavia non presenta un analogo a livello materiale, ma può essere considerato come un oggetto matematico con determinate proprietà rintracciabili nella rappresentazione matematica che modella i fenomeni

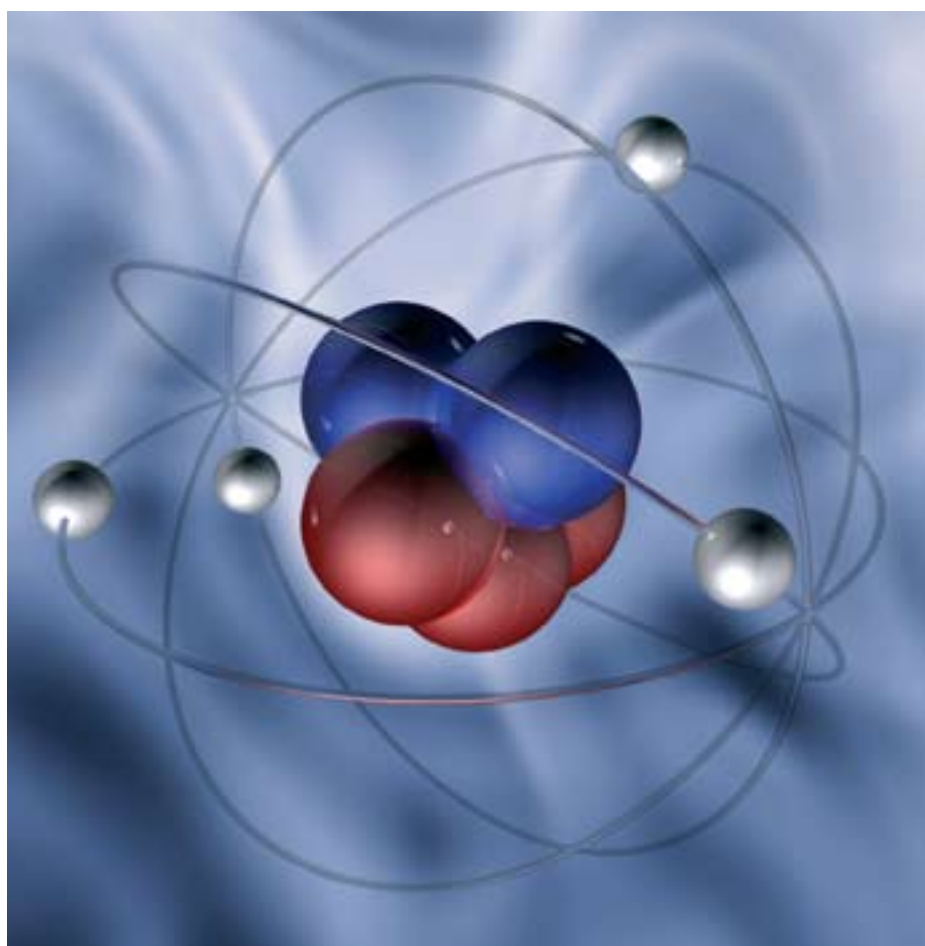
che occorrono in meccanica quantistica. Il vantaggio di lavorare con un oggetto astratto quale il qubit è quello di poter

I principi della meccanica quantistica che intervengono nella definizione del qubit sono i principi di *sovrapposizio-*

Super-computer DEL FUTURO

Come funzionano i computer quantistici, quanto sono veloci, quale impatto avranno sul mondo della computazione pratica.

di Emanuele Ghedin



sviluppare una teoria computazionale quantistica che non dipenda dal particolare sistema di realizzazione. Lo svantaggio è che non si sa se esista e su cosa si basi un tale sistema. Tuttavia le molteplici applicazioni pratiche della meccanica quantistica (laser, microscopio elettronico, risonanza magnetica nucleare) fanno ben sperare su un'effettiva progettazione di un computer basato sul qubit.

ne e di *correlazione* (o *entanglement*). Il primo sancisce l'esistenza di stati (uno *stato quantico* è la configurazione di una particella o di un loro insieme, matematicamente rappresentato da una funzione a valori complessi detta *funzione d'onda*) intermedi tra due stati ammissibili del sistema; a livello matematico è ammissibile ogni combinazione lineare a coefficienti complessi, le cui somme dei quadrati dei moduli siano pari ad uno, di due valo-



Sopra: un processore, il cuore dei computer attuali. In alto: il mainframe di un grande centro di ricerca.

ri ammissibili. Il secondo afferma che lo stato quantico di un insieme dipende dagli stati di ciascun elemento dell'insieme stesso, anche se tali elementi sono separati spazialmente. In accordo al principio di sovrapposizione, il qubit, oltre ai due stati del bit classico 0 e 1, ammetterebbe un'infinità di stati intermedi, il che consentirebbe una computazione talmente veloce da permettere di eseguire, in pochi secondi, calcoli per la cui esecuzione i computer classici impiegherebbero parecchi anni.

È stato stimato che un computer quantistico a 500 qubit avrebbe la stessa po-

tenza di calcolo di un analogo computer classico dotato approssimativamente di 10^{150} processori.

Appare chiaro come, nonostante con i computer quantistici non abbia più senso considerare la velocità di clock quale metro di valutazione della rapidità di calcolo (dato che non esistono degli stati, e quindi dei livelli logici, completamente determinati di cui calcolare la velocità di commutazione), essi racchiudano una potenzialità computazionale spaventosa, sulle cui conseguenze occorrerebbe riflettere adeguatamente. Una simile potenza di calcolo, ad esempio, sarebbe più che sufficiente a rompere in breve tempo le chiavi di criptazione con le quali vengono resi indecifrabili tutti i dati sensibili che viaggiano sulle reti informatiche, rendendo impossibile la trasmissione di dati sicuri che è, tra le altre cose, alla base delle transazioni economiche del sistema bancario. L'algoritmo di criptazione più largamente utilizzato è infatti l'Rsa, il quale sfrutta un'importante proprietà matematica posseduta dai numeri primi; essi possono essere moltiplicati con un numero intero, risalire alla

sua fattorizzazione in numeri primi è un problema la cui risoluzione richiede a un computer attuale migliaia di anni di calcolo (relativamente a numeri molto grandi). È dunque molto facile criptare un messaggio, ma è praticamente impossibile decrittarlo, il che rende tale algoritmo sicuro. Con l'ipotetico avvento dei computer quantistici tutto ciò verrebbe a cadere, dato che esiste un algoritmo di fattorizzazione degli interi, l'*algoritmo di Shor*, eseguibile unicamente dai computer quantistici, che ha un tempo di risoluzione sufficiente a rendere vulnerabile la criptazione tramite l'Rsa.

Non bisogna tuttavia allarmarsi prima del tempo. Nonostante a livello teorico la computazione quantistica rappresenti un argomento già molto sviluppato, sul piano pratico la costruzione dei computer quantistici è ancora molto lontana. Tuttavia, è molto probabile che si tratti solo di una questione di tempo e che prima o poi il primo computer quantistico faccia la sua comparsa, decretando uno dei più grandi avanzamenti nella scienza applicata, in grado di rivoluzionare completamente il mondo della computazione pratica. ■