COMPUTER QUANTISTICI: STATUS E PROSPETTIVE

LORENZO MACCONE (*)

Nota presentata dal m.e. Mauro D'Ariano
(Adunanza del 24 novembere 2016.)

SUNTO. – Il quantum computer è un sistema che è in grado di processare informazione quantistica. In questa presentazione spiegherò brevemente di cosa si tratta e quali sono i principali risultati della ricerca attuale in questo ambito.

***

ABSTRACT. – A quantum computer is a system that is able to process quantum information. In this presentation I'll briefly explain what is it and what are the main results of the current research in the field of quantum computation.

Strutturerò la mia presentazione come un dialogo tra una persona curiosa che pone domande e il sottoscritto che tenta di rispondere nel modo più chiaro possibile. Cercherò di comunicare i concetti di base piuttosto che entrare nel dettaglio tecnico dei risultati che presenterò.

– Cos'è un computer quantistico?

È un computer che usa fenomeni quantistici quali l'entanglement e la complementarità (che approfondirò di seguito) per svolgere calcoli.

– E cosa ci si guadagna?

Non si perde niente, nel senso che un computer quantistico può svolgere le stesse operazioni che può svolgere un computer convenzionale (che d'ora in poi chiamerò "computer classico"). Inoltre, si guada-

(*) Dipartimento di Fisica "A. Volta" & INFN Sezione di Pavia, Italia.
E-mail: maccone@unipv.it

gna in velocità per alcune specifiche computazioni (ma non per tutte). Quindi è sicuramente conveniente usare un computer quantistico, soprattutto se si vogliono svolgere questi tipi di computazioni.

– Come funziona?

Iniziamo a vedere come funziona un computer classico. Esso è un sistema che prende informazione, la elabora e restituisce un risultato. L'informazione in ingresso viene tradotta (tramite appropriate codifiche o alfabeti) in numeri ed è tipicamente codificata in bit. Infatti, invece di usare numeri in base 10 (quelli che usano gli umani), i computer usano numeri in base 2, cioè bit. Un bit può avere due soli valori, zero oppure uno. Si usano i bit nei computer elettronici perchè è semplice implementare un bit in elettronica: si suppone che si ha "uno" quando passa corrente e "zero" quando non passa corrente. Ad esempio il numero cinque si scrive come 101 in binario, che corrispone a un segnale elettronico dove ho corrente inizialmente, poi la corrente cessa, e alla fine la corrente passa nuovamente. L'elaborazione dei bit in ingresso viene svolta da circuiti elettronici che svolgono operazioni matematiche. Alla fine il computer restituisce il risultato.

I computer moderni sono talmente potenti che questi processi sono mascherati: invece di fornire numeri, possiamo fornire informazione tramite una tastiera, una telecamera, un microfono, internet, etc. Tutti questi segnali vengono tradotti in numeri e codificati in bit. Il computer elabora (matematicamente) questi numeri e restituisce il risultato che viene a sua volta tradotto come figure, filmati o lettere sullo schermo, suoni dall'altoparlante, etc.

Un computer quantistico funziona allo stesso modo: prende informazione, la elabora, e restituisce un risultato. La differenza con il computer classico è nel fatto che l'informazione è informazione quantistica, che non è facilmente traducibile in termini di numeri. Invece di usare bit, il computer quantistico usa quantum bit, chiamati "qubit". Sono sistemi *quantistici* a due livelli. L'elaborazione di informazione avviene tramite circuiti quantistici che sono in grado di elaborare l'informazione quantistica. Il risultato finale è, solitamente, qualcosa che un umano può utilizzare, e quindi è informazione classica, codificata in bit (ed, eventualmente, tradotta in immagini, filmati, lettere, suoni, etc.)

Quindi la filosofia dietro al computer quantistico è sostanzialmente la stessa che c'è dietro ad un computer convenzionale. Solo che

il computer classico elabora numeri, cioè bit, mentre il computer quantistico elabora informazione quantistica, cioè qubit.

– Cos'è un qubit?

È la generalizzazione quantistica del bit. Il bit può assumere due valori "zero" e "uno". Un qubit è un sistema quantistico a due livelli, a cui possiamo assegnare le etichette "zero" e "uno". Ad esempio, lo spin di un elettrone è un sistema quantistico a due livelli: lo spin può assumere valore $-1/2$ e $+1/2$ (a seconda se è orientato antiparallelamente o parallelamente al campo magnetico che si usa per definire la direzione di quantizzazione). Possiamo chiamare "zero" un elettrone con spin $-1/2$ e "uno" un elettrone con spin $+1/2$. Chiaramente, essendo questo un sistema quantistico, non è limitato ai valori "zero" e "uno", ma può accedere a fenomeni quantistici come l'entanglement e la complementarità.

– Complementarità?! Di cosa si tratta?

Ogni sistema quantistico può avere delle proprietà (complementari) che non si possono conoscere contemporaneamente con precisione. Per "proprietà" intendo qualunque cosa si possa misurare. Ad esempio, l'elettrone può avere spin con una proprietà di essere parallelo ("uno") o antiparallelo ("zero") al campo magnetico. Però può anche avere proprietà complementari.

Se "sovrappongo" più valori di una proprietà, ottengo un valore di una proprietà complementare. Questo è il principio di sovrapposizione della meccanica quantistica. Siccome non è intuitivamente chiaro a nessuno cosa vuol dire "sovrapporre" quantisticamente, preferisco parlare di complementarità, che è un concetto che si può comprendere.

Un modo per comprendere la complementarità è con una metafora. L'arancione si ottiene mescolando ("sovrapponendo") il giallo e il rosso. Quindi un'arancia non è nè gialla nè rossa. Si può dire che un'arancia sia contemporaneamente gialla e rossa. Quindi possiamo concludere che la proprietà di essere arancione ("arancionità") è complementare alla prorietà di essere giallo o rosso.

Purtroppo questa metafora è incompleta, perchè questi sono tutti valori di un'unica proprietà (il colore), mentre la complementarità quantistica riguarda proprietà diverse: sovrapponendo valori di una proprietà (ad esempio, sovrapponendo il giallo e il rosso) si dovrebbe ottenere il valore (arancione) di una proprietà diversa (qui la metafora fallisce perchè arancione è ancora un colore), e complementare alla prima.

La complementarità è alla base di una delle conseguenze più famose della teoria quantistica, la relazione di indeterminazione di Heisenberg. Questa dice che, meglio conosco una proprietà (ad esempio la posizione), meno conosco una proprietà complementare (ad esempio il momento). Matematicamente, questa relazione è espressa con $\Delta x \Delta p \geq \hbar$, dove Δx e Δp sono gli errori con cui determino la posizione e il momento rispettivamente, e dove $\hbar$ è una costante fisica. Questa disuguaglianza dice che non posso avere errori troppo piccoli per entrambi posizione e momento, perchè il prodotto degli errori deve essere maggiore di $\hbar$.

La nostra mente "classica" fatica a comprendere le implicazioni della complementarità e della indeterminazione: cosa vuole dire che la posizione della mia auto non è ben definita?! Dov'è la mia auto?! Sarebbe ben difficile guidare in autostrada se non potessi conoscere contemporaneamente sia la posizione che la velocità della mia auto! Nella vita di tutti i giorni non vediamo gli effetti dell'indeterminazione perchè la costante $\hbar$ ha un valore molto piccolo rispetto alle precisioni che possiamo raggiungere nella vita di tutti i giorni. La posizione della mia auto inizierebbe ad essere indefinita per qualche centimetro se io potessi determinare la sua velocità con una precisione di 32 cifre decimali. Una tale mostruosa precisione è irraggiungibile con la tecnologia odierna: le misure più precise che riusciamo a compiere attualmente non riescono a determinare nemmeno 20 cifre decimali. Questo è il motivo per cui riusciamo a guidare la nostra auto: possiamo conoscere sia la sua velocità che la sua posizione perchè non conosciamo nessuna delle due con precisione "quantistica". Il fatto che ciascuna delle due è determinata in modo "grossolano" (che è più che sufficiente per gli scopi ordinari), ci permette di definire entrambe.

– Perchè la complementarità è utile in un computer quantistico? Sembrerebbe più che altro una limitazione a quello che possiamo conoscere e definire!

Già, ma un quantum bit, un qubit, può accedere anche alle proprietà complementari a "zero" e "uno". Invece un bit di un computer classico è limitato a questa proprietà. Cioè un bit può solo avere valori {0, 1}. Invece un qubit può avere valori {0, 1}, ma anche {+, −}, {+i, −i}, etc., che sono tutte proprietà complementari. Ad esempio, la proprietà "+" si ottiene "sommando" (nel senso di sovrapposizione quantistica) le proprietà "zero" e "uno", e la proprietà "−" si ottiene "sot-

traendo" (di nuovo nel senso di sovrapposizione quantistica) le stesse proprietà.

Il fatto che queste siano proprietà complementari significa che posso accedere ad una sola di queste proprietà per volta. Ma se riesco ad essere sufficientemente furbo, posso usarle tutte nella mia computazione.

Un esempio di questo è l'algoritmo di Deutsch-Jozsa. Supponiamo di avere una scatola che accetta un bit come input e mi restituisce un valore *a* se il bit era zero o *b* se il bit era uno. Cioè la scatola calcola la funzione $f(0) = a$ e $f(1) = b$. Voglio scoprire se *a* è uguale a *b* oppure se sono diversi, *usando la scatola una volta sola*. (La scatola rappresenta una subroutine di una computazione.) Chiaramente questo è impossibile con una strategia classica: devo prima calcolare *a* e poi calcolare *b* per poterli confrontare, quindi devo usare la scatola due volte. Invece, con una strategia quantistica (che non descriverò qui), è possibile verificare se $a = b$ usando la scatola un'unica volta! Il trucco principale consiste nell'inserire nella scatola un qubit "+", che è complementare a "zero" o "uno". In un certo senso sto inserendo nella scatola "zero" e "uno" contemporaneamente e quindi riesco a scoprire se $a = b$ con un uso solo della scatola.

[Ho presentato una versione semplificata dell'algoritmo di Deutsch-Jozsa. La versione più generale è in grado di determinare se una funzione di *n* bit è costante oppure bilanciata, con una diminuzione esponenziale in *n* di calcoli della funzione rispetto a qualunque algoritmo classico deterministico. Se invece uno fa il confronto con gli algoritmi classici probabilistici, allora la diminuzione è solo di un fattore due come l'esempio semplificato che ho indicato sopra.]

– Questo esempio è interessante, ma poco utile in pratica. Ci sono esempi un po' più utili?

In realtà è molto difficile trovare algoritmi quantistici che hanno vantaggi rispetto ai corrispondenti algoritmi classici. Ma sono noti alcuni esempi importanti. I due più famosi sono i seguenti:

1. Fattorizzazione. Dato un numero *c*, voglio trovare i fattori *a* e *b* tali che $a \times b = c$. Ad esempio, se $c = 15$, devo trovare $a = 5$ e $b = 3$. Per numeri piccoli come 15, questo è semplice. Per numeri grandi (cioè numeri con centinaia di cifre) questo è estremamente complicato. È complicato a tal punto che tutti i principali protocolli crittografici in uso oggi su internet si basano sull'assunzione che fattorizzare numeri grandi sia talmente complicato che non sia possibile risolvere questo

problema in un tempo ragionevole. Questi protocolli sono quelli che usate ogni volta che fate un acquisto con la carta di credito oppure accedete al sito web della vostra banca: usate protocolli crittografici perchè non volete che nessuno possa scoprire il vostro numero di carta o possa accedere al vostro conto online.

L'assunzione che fattorizzare numeri grandi sia troppo complicato per un computer è falsa se usate un quantum computer! Questa fu la scoperta, ad opera di Peter Shor, che lanciò la quantum computation. Peter Shor trovò un algoritmo quantistico che può fattorizzare numeri di n cifre con un'efficienza esponenziale in n, cioè in modo molto più semplice che gli algoritmi classici.

In previsione dello sviluppo di quantum computers che siano in grado di eseguire l'algoritmo di Shor per numeri molto grandi, sono stati sviluppati nuovi protocolli crittografici "post-quantum" che sono robusti anche se attaccati da un quantum computer. Per ora stiamo ancora usando i vecchi protocolli perchè non esistono ancora quantum computer sufficientemente potenti da eseguire l'algoritmo di Shor per numeri sufficientemente grandi da creare un rischio di sicurezza per gli attuali protocolli crittografici.

2. Grover search: ricerca in un database non strutturato. Supponiamo di voler scoprire a chi è intestato un numero di telefono cercando il nome sull'elenco telefonico. Siccome l'elenco telefonico è ordinato per ordine alfabetico, dovrò cercare il numero in ogni pagina finchè non trovo il nome associato. (Al contrario di cercare il numero associato ad un nome che è molto semplice.) L'algoritmo di Grover permette ad un quantum computer di effettuare questa ricerca in modo più efficiente di un algoritmo classico.

Questo algoritmo ha anche un interesse concettuale, perchè ci dice che un computer quantistico è in grado di velocizzare tutti gli algoritmi NP, che sono gli algoritmi dove è difficile trovare una soluzione ad un problema, ma è facile verificare se ho una soluzione. L'algoritmo di Grover ci dice che un algoritmo quantistico può velocizzare gli algoritmi NP che non hanno struttura (come l'esempio dell'elenco telefonico) e dove devo ridurmi a testare tutte le possibili soluzioni una per una.

– Allora i quantum computer sono utili! Ma esistono?

Non ancora! O meglio, abbiamo quantum computer molto rudimentali che sono in grado di fare semplici operazioni su poche decine di qubit al massimo. Siamo ancora ad uno stadio della ricerca dove non

è neanche chiaro quale sia la tecnologia più promettente per implementare un quantum computer. Si stanno esplorando diverse possibili implementazioni: ad esempio, sistemi a stato solido (simili a quelli usati nei computer elettronici classici), ma anche molte altre possibilità, quali la risonanza magnetica nucleare, le trappole magneto ottiche, l'ottica quantistica, etc.

Se avete 10 milioni di dollari da buttare, potete acquistare un "quantum computer" dalla D-Wave, una ditta canadese che mette in commercio un computer basato sulla tecnologia del quantum simulated annealing. È stato acquistato da NASA, Google, Lockeed (che sono organizzazioni che effettivamente hanno 10 milioni di dollari da buttare). Purtroppo ad oggi non ha ancora dimostrato di essere un "vero" quantum computer. Cioè non ha dimostrato di saper risolvere dei problemi in modo più efficiente degli analoghi algoritmi classici. Ha solo saputo dimostrare di fare simulated annealing più velocemente del simulated annealing classico, ma questo non vuole necessariamente dire che può risolvere problemi in modo più veloce di *altri* algoritmi classici. Attualmente c'è un forte dibattito molto divertente tra i costruttori della D-Wave e i principali scienziati che lavorano in quantum computation.

– In Europa?

L'Europa ha riconosciuto che la tecnologia quantistica, di cui il quantum computer è un aspetto, sarà fondamentale per lo sviluppo tecnologico del futuro. Infatti, sta partendo un'iniziativa di finanziamento molto rilevante nei confronti della tecnologia quantistica, la "quantum technologies flagship" che finanzierà un miliardo di euro nei prossimi anni per sviluppare queste tecnologie, incluso il quantum computer.

In Italia ci sono molti gruppi di ricerca che si occupano di questi temi. Oltre al nostro gruppo di Pavia, anche qui a Milano ci sono dei gruppi importanti (ad esempio il gruppo di Matteo Paris all'università statale) e molti altri in tutto il resto d'Italia.

– Quando avremo un quantum computer, allora?

Non lo so. È molto difficile prevedere gli sviluppi tecnologici senza rendersi completamente ridicoli. Negli anni 40 il direttore dell'IBM aveva previsto "I think there is a world market for maybe five computers." Se uno conta solo gli i-phone, ne sono stati prodotti, ad oggi, più di un miliardo.

– Tu di cosa ti sei occupato in questo ambito?

La mia ricerca non è direttamente collegata alla quantum computation, ma nel corso degli anni mi sono occupato anche di questo. In particolare menziono tre risultati a cui ho contribuito:

1. Quantum random access memory: la memoria quantistica ad accesso casuale. La RAM è parte integrante dell'architettura dei computer elettronici. Consiste in una serie di celle di memoria a cui si può accedere in modo indipendente e in maniera casuale. Io e i miei collaboratori avevamo sviluppato e brevettato una architettura per la versione quantistica della RAM.

2. Quantum private queries. È un protocollo crittografico per interrogare un database (ad esempio Google) senza che il proprietario del database possa scoprire quale domanda è stata posta. È anche uscito un articolo su 'Le Scienze' su questo protocollo, che abbiamo provato a vendere a Google. Non si sono dimostrati interessati all'acquisto perchè loro vogliono sapere cosa noi chiediamo a Google: il loro business model lo richiede.

3. Blind quantum computation. È un altro algoritmo crittografico che permette ad Alice di eseguire una computazione sul quantum computer di Bob senza che lui possa sapere che tipo di computazione lei sta eseguendo, nè il risultato ottenuto. Questo sarebbe impossibile usando un computer convenzionale.

– Perchè un fisico dovrebbe interessarsi al quantum computer? Sembra più una sfida tecnologica che concettuale.

No! Analizzare la fisica dal punto di vista dell'elaborazione dell'informazione quantistica si è rivelata essere una rivoluzione concettuale di grossa portata nella fisica moderna. Ad esempio, il prof. D'Ariano nel nostro gruppo di Pavia sta portando avanti un programma molto interessante di riformalizzazione di tutta la fisica a partire da principi fisici operativi e informazionali. Inoltre, le ultime idee sulla gravità quantistica esplorano quali tipi di operazioni quantistiche si possono effettuare con un buco nero in termini di elaborazione di informazione.

Quindi, ragionare in termini di elaborazione di informazione porta a nuovi risultati perfino nella fisica fondamentale, quanto di più lontano ci sia dalle applicazioni tecnologiche!

– Interessante, mi puoi sintetizzare cosa hai detto?

Ho parlato del quantum computer. Ho illustrato come esso sia

una generalizzazione dei computer convenzionali, dove i bit vengono sostituiti da qubit. Ho fatto vedere che in questo modo si ottiene un guadagno grazie agli effetti quantistici, quali la complementarità, di cui ho presentato una metafora e di cui ho illustrato la connessione con l'indeterminazione di Heisenberg. Ad esempio la complementarità è importante nell'algoritmo di Deutsch-Jozsa che sfrutta il fatto che posso calcolare una funzione con un input che è "contemporaneamente" sia "zero" che "uno". Infine ho concluso con un brevissimo excursus sullo stato attuale della ricerca in questo campo. Il messaggio che vorrei che il lettore conservasse di questa presentazione è che la tecnologia quantistica non è solo il futuro della tecnologia, ma riguarda anche una rivoluzione concettuale: un modo diverso di analizzare la natura, analizzando i sistemi fisici in base alla loro capacità di elaborare informazione.