E' possibile sfruttare ai fini pratici le proprietà "straordinarie" degli oggetti quantistici?

Se per fini pratici intendiamo cose che riguardano la vita di ogni giorno, come ad esempio elettrodomestici o dispositivi elettronici digitali (telefoni, computer, ecc.) allora si può dire che siamo già immersi in un mare di applicazioni della meccanica quantistica (MQ) visto che in qualche misura tutti questi apparati si basano su uno o più elementi caratteristici della fisica quantistica. Il forno a microonde funziona sulla base dei livelli energetici della molecola di acqua, che hanno precisi valori quantizzati (e non potete scaldare qualcosa che non contenga almeno un po' di acqua). I processori che si trovano in computer e telefoni cellulari sono costruiti con semiconduttori e la differenza tra questi materiali ed i metalli si deve in ultima analisi alla cosiddetta esclusione di Pauli, secondo la quale due o più elettroni non possono mai avere un'identica funzione d'onda. Sempre sul versante dei materiali innovativi, citiamo quelli per la costruzione di pannelli solari fotovoltaici che permettono di convertire l'energia della radiazione elettromagnetica in energia elettrica.

Esistono però applicazioni molto recenti, meno consuete, e in un certo senso "genuinamente quantistiche". Con questo mi riferisco ad applicazioni che sostanzialmente non sarebbero possibili se non sfruttassimo proprio quelle proprietà “straordinarie”. In altre parole, anche usando al meglio la scienza pre-quantistica non riusciremmo a realizzare quelle stesse applicazioni, non nello stesso modo.

Un esempio interessante mi sembra quello della **crittografia quantistica**, per la quale esistono già dei dispositivi a livello commerciale. La crittografia veniva usata già dal 400 a.c. per inviare messaggi cifrati, che potevano essere decifrati solo se il destinatario possedeva la chiave usata dal mittente per codificare il messaggio. Spesso si usa un alfabeto “parallelo”, diverso, che solo mittente e destinatario conoscono. Al tempo degli Spartani il messaggio viaggiava su striscia di pelle e la chiave era un bastoncino, oggigiorno i messaggi viaggiano via cavo o via radio e le chiavi crittografiche sono stringhe di bit, sequenze di 0 e 1. Più lunga è la stringa più sicuro è la cifratura, poichè per decifrare i messaggi è necessario prima trovare i fattori primi in cui si scompone la chiave. Diciamo che con numeri a 1024 bit adesso ci potremmo sentire ragionevolmente sicuri, ma se un intruso fosse proprio intenzionato a decifrare un messaggio in particolare (pensate a grossi trasferimenti di denaro o a questioni militari) allora si potrebbe mettere in ascolto su un canale ed impiegare tutte le risorse di calcolo che ha per fattorizzare il più in fretta possibile una specifica chiave che gli interessa... Diciamo che non c'è proprio una sicurezza assoluta. Ma se la chiave fosse distribuita su un canale quantistico, ossia un supporto dove le informazioni sono codificate nella funzione d'onda di fotoni o elettroni, le cose cambierebbero. Abbiamo sentito che non è possibile fare misure, in questo caso leggere dei dati, su un sistema quantistico senza far collassare (o contrarre) la sua funziona d'onda. E' lo stesso meccanismo che abbiamo visto nel filmato del Dr. Quantum quando l'occhio cerca di vedere da quale fenditura passa l'elettrone. La “misura: fenditura destra o sinistra” distrugge la funzione d'onda che dava luogo all'interferenza e la modifica in modo che sullo schermo si vedano solo due segnali in corrispondenza delle fenditure.

Nel caso della crittografia quantistica quando lo spione cerca di leggere la chiave sul “cavo quantistico” senza che mittente e destinatario se ne accorgano, modifica inevitabilmente la funzione d'onda e quindi c'è il modo di scoprirlo. La MQ offre una via intrinsecamente sicura per crittare i dati.

Notare che, pur riferendosi in modo essenziale a fotoni o atomi, alcune di queste applicazioni non sono propriamente “microscopiche”, ma si riescono a proiettare su distanze anche molto elevate. Ci sono già esperiementi di comunicazione quantistica su 144 km di distanza in aria aperta tra due isole Canarie e l'ipotesi progettuale di comunicare a livello quantistico nello spazio con satelliti.

Quindi c'è ancora spazio per miglioramenti, derivanti dalla meccanica quantistica, nei sistemi che usiamo tutti i giorni per comunicare, lavorare, ecc.

Non solo, per quanto suoni poco familiare i sistemi di elaborazione attuali si scontrano con il fatto che alcuni problemi sono ancora irrisolvibili, o meglio si potrebbero risolvere su tempi praticamente infiniti (l'età dell'universo...). Riprendiamo il discorso di prima sulla
la fattorizzazione di grandi numeri in numeri primi più piccoli, il problema matematico che rappresenta l'essenza della crittografia usata oggi in tutto il mondo. Un esempio che sembra banale, ma non lo è. Per dare alcuni numeri...

- 1 055 664 361 = 24151 × 43711 “facile”

- RSA-640 (193 cifre decimali) =
3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609 =

1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579 ×

1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

circa 5 mesi su un cluster di 80 processori a 2.2 GHz.

- RSA-2048 (617 cifre decimali) **???**

In matematica si classificano i problemi in base al loro grado di complessità, cioè in base a quante e quali risorse sono necessarie per risolverli. Una delle classi più importanti è quella NP, problemi la cui soluzione può essere verificata facilmente ma la cui soluzione “da zero” non si può trovare altrettanto facilmente. Facile in questo contesto indica che è fattibile con risorse di tempo e di spazio che crescono come una potenza del numero di dati in input, n. Quindi per un problema NP, come è quello della fattorizzazione di un numero di n cifre, servono ovviamente risorse limitate per verificare se il prodotto dei due numeri – la soluzione – fornisce il numero di partenza, ma se abbiamo in mano solo questo numero grande e vogliamo trovare un fattore primo dobbiamo utilizzare tempo e memoria che scalano esponenzialmente con n. Si arriva rapidamente all'età dell'universo!
Tuttavia, qualche anno fa (1994) Peter Shor ha messo a punto un algoritmo genuinamente quantistico, che risolve tale problema NP in tempi "umani"(mettendo tra l'altro a repentaglio gli attuali sistemi crittografici classici "sicuri"). Gli algoritmi quantistici sono procedure che risolvono problemi usando espressamente la matematica, o meglio la logica, della MQ. In particolare l'algortimo di Shor poggia sulla possibilità di elaborare simultaneamente, o parallelamente, tutta l'informazione che può essere contenuta in una sovrapposizione lineare di funzioni d'onda, come quella che arriva allo schermo del “nostro” interferometro. Questo è possibile solo se l'ampiezza E la fase delle onde viene elaborata senza perdite indesiderate. Si parla di **computazione quantistica e informazione quantistica**. Quest'ultima deve essere memorizzata ed elaborata in memorie e porte logiche quantistiche, ossia sistemi fisici che siano in grado di mantenere e/o trasformare una vera e propria funzione d'onda fino all'atto finale della misura in cui si legge il risultato. Come nell'informatica “classica” abbiamo bit che assumono valori 0 oppure 1, così nel caso quantistico parliamo di qubit che sono rappresentati da funzioni d'onda in cui ci sono contemporaneamente 0 E 1 nella sovrapposizione lineare. In un registro quantistico a n qubit si possono rappresentare in linea di principio 2^n numeri simultaneamente.

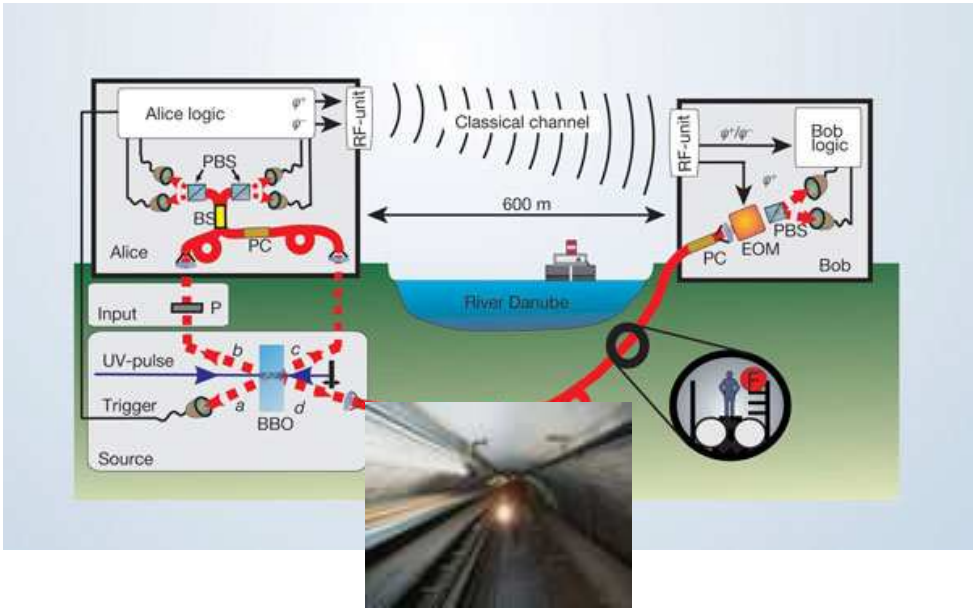
Non è sufficiente però riutilizzare gli algoritmi classici che si usano sugli attuali computer, per quanto potenti, ma bisogna concepire algoritmi ottimizzati per gestire questo parallelismo, come in quello di Shor per la fattorizzazione. Per implentare una logica quantistica dobbiamo poter gestire adeguatamente le sovrapposizioni, l'entanglement, l'interferenza, ecc. La tecnologia che oggi sembra offrire maggiori prospettive per la computazione quantisica è quella degli ioni intrappolati in trappole elettromagnetiche e raffreddati a temperature bassissime. In tal caso lo 0 è rappresentato dall'atomo nel suo stato fondamentale ad energia più bassa e 1 da uno stato ad energia più alta quantizzata secondo la MQ. Esistono però proposte alternative nel campo dell'ottica o della fisica dello stato solido. A differenza della crittografia, per il momento abbiamo solo dei prototipi funzionanti ma non ancora impiegati per problemi veri e propri. L'industria informatica però crede in questo campo e, assieme al mondo accademico, sta finanziando parecchie ricerche. L'idea di un computer di questo tipo, costruito in un laboratorio in condizioni controllate, ci suggerisce che probabilmente in futuro non accantoneremo i computer “classici” che rimarranno assolutamente validi per tutta una serie di compiti quotidiani. Ai computer quantistici verranno riservati dei compiti speciali ed importanti, non gestibili altrimenti e a cui verranno destinate le risorse di calcolo quantistico necessarie presso università, centri di ricerca, ecc.
Non mancano però le idee più “visionarie”, come quello di Seth Lloyd, uno dei fisici che più si è occupati di computazione quantistica. Nel suo libro “Programmare l'Universo”, concepisce appunto l'intero universo come un computer quantico nel quale è in esecuzione un programma cosmico che produce ciò che vediamo attorno a noi, inclusi forse noi stessi. Una volta che avremo compreso completamente le leggi della fisica, saremo anche in grado di replicare lo stesso dispositivo “Universo” su scala più piccola. Insomma, il “portatile” concettualmente più potente è costituito da un blocco di qualche kg di materia in cui gli atomi immagazinano l'informazione e le interazioni le elaborano. (figura da S. Lloyd, Nature **406**. 1047 (2000)).
Una provocazione: è davvero pensabile di comprendere completamente le leggi della fisica?

Figure 1 The ultimate laptop. The ‘ultimate laptop’ is a computer with a mass of 1 kg and a volume of 1 l, operating at the fundamental limits of speed and memory capacity fixed by physics. The ultimate laptop performs $2mc^2/\pi\hbar = 5.4258 \times 10^{50}$ logical operations per second on $\sim 10^{31}$ bits. Although its computational machinery is in fact in a highly specified physical state with zero entropy, while it performs a computation that uses all its resources of energy and memory space it appears to an outside observer to be in a thermal state at $\sim 10^{9}$ degrees Kelvin. The ultimate laptop looks like a small piece of the Big Bang.

Beh, a parte queste idee “visionarie”, se i prototipi di computer quantistici da laboratorio dovranno essere messi a punto per funzionare “sul serio”, migliorando sempre di più le prestazioni e la stabilità, si potrebbe pensare che nel futuro ci siano più sfide per l'ingegneria di alto livello che non per la fisica in quanto tale...

L'una e l'altra cosa. Certamente le ricerche applicative avranno bisogno di raffinamenti sempre maggiori sul piano operativo più che su quello concettuale, ma alcune questioni fisiche di fondo che abbiamo sentito nella prima parte, specialmente quelle sulla località e la completezza della MQ nel pensiero einsteiniano, sono ancora lì in attesa di essere "risolte". Penso che ci troviamo in una di quelle epoche in cui l'indagine sperimentale, in questo caso da un punto di vista prettamente fisico, stia portando alla manifestazioni di effetti nuovi e sorprendenti. Prendendo proprio spunto

dall'esperimento concettuale con cui Einstein, Podolsky e Rosen (nella formulazione di Bohm) argomentano l'incompletezza della teoria quantistica, qualche anno fa Bennett e collaboratori all'IBM hanno ideato un protocollo di **teletrasporto quantistico** che poi negli ultimi anni è stato realizzato "in laboratorio", da diversi gruppi tra cui uno di Roma. Le virgolette si riferiscono al fatto che in un caso recente il laboratorio era un apparato sotto il letto del Danubio a Vienna ed il canale di teletrasporto una fibra ottica di centinaia di metri di lunghezza. E adesso si pensa ad un teletrasporto su scala geografica (centinaia di km) o anche spaziale. (figura da Ursin et al., Nature **430**, 849 (2004)).



Descriviamo in breve l'esperimento: il mittente (Alice) possiede un oggetto dallo stato incognito (diciamo la funzione d'onda del fotone) da inviare al destinatario (Bob) ed i due hanno ciascuno un “capo” di una coppia di particelle entangled come nell'esperimento EPR. Alice compie una misura speciale che coinvolge la funzione d'onda delle sue due particelle. Dato che una di queste è entangled con quella di Bob l'effetto della misura si ripercuote, per così dire, all'altro capo con una fedeltà tale (frutto delle correlazioni quantistiche) che Bob si ritrova con una copia della particella che aveva Alice. Più precisamente, c'è un elemento di non causalità o di aleatorietà nella misura di Alice, che non può conoscere il risultato visto che il messaggio da teletrasportare è incognito. Una volta fatta la misura però comunica a Bob, su un canale classico, il valore ottenuto ed egli, in modo automatico, applica un'operazione condizionata al risultato e si ritrova “tra le mani” lo stato teletrasportato. Notare che, essendo l'ultimo canale classico, il principio di relatività non viene violato perché nessuna informazione può viaggiare più rapidamente della luce.

D: Hai detto teletrasporto, come quello dei film o dei romanzi di fantascienza?

R: Non proprio, almeno per ora. Se avete notato in quello che ho detto, ed in tutti gli esperimenti realizzati, si tratta di teletrasportare uno stato (alias di funzione d'onda) di un oggetto. Nel contesto della comunicazione quantistica parliamo di chiave crittografica o di un messaggio. Ma nel canale quantistico di teletrasporto il destinatario ha già un suo “substrato” su cui poi viene teletrasportato lo stato che ci interessa. Non abbiamo parlato di teletrasportare materia o energia, come in Star Trek!
Però è stato usato, provocatoriamente, lo stesso termine poiché nella visione più radicale della fisica quantistica il concetto di stato è molto vasto. L'esserci o il non esserci possono essere considerati due stati possibili di un fotone o di un elettrone, di un atomo, una molecola e su su fino a oggetti

macroscopici. Se è concepibile ideare e realizzare un teletrasporto di stati, perché non dovrebbe essere possibile estendere il teletrasportarto alla materia di cui siamo fatti? Il dibattito se abbia senso fisico o meno considerare l'entanglement con il vuoto (il non esserci) è appassionante e tuttora in corso. E dalle diatribe del secolo scorso tra i giganti della Fisica sappiamo che la meccanica quantistica non ha ancora finito di sorprenderci...