Computer Quantistici

Alessandra Di Pierro - Oliver Morsch

Come tutte le grandi scoperte, il computer quantistico nasce da un'idea visionaria. Nel caso specifico, l'idea fu avanzata dal premio Nobel Richard P. Feynman che in uno dei suoi più famosi articoli lo suggerì come una possibile soluzione al problema: `Can physics be simulated by a universal computer?'. In questo articolo, racconteremo l'evoluzione della ricerca teorica e sperimentale in quell'area che oggi è nota come `computazione quantistica', dall'idea di Feynman ai nostri giorni, descrivendo i risultati ottenuti sia nell'ambito della realizzazione fisica del computer quantistico, sia riguardo ad aspetti più prettamente informatici relativi alla teoria della calcolabilità e degli algoritmi e complessità.

Keywords: Quantum Physics; Quantum computation; Quantum algorithms

1. Introduzione

Quando Charles Babbage intorno al 1830 ebbe l'idea di un dispositivo meccanico in grado di eseguire compiti generici non ristretti a puri calcoli matematici, il progresso tecnologico non aveva ancora messo a disposizione gli strumenti specifici necessari per realizzare il suo prototipo. Valvole e transistor arrivarono solo cent'anni dopo per permettere la costruzione del calcolatore programmabile che tanto aveva in comune con la Macchina Analitica di Babbage.

Ritornando ai nostri giorni, il computer è innegabilmente un'icona dell'era in cui viviamo, imprescindibile per le sue capacità e in continua evoluzione diventando ogni anno più veloce, più piccolo e più economico secondo un processo di crescita che sembra non avere limiti.

In una situazione così diversa dai tempi di Babbage dobbiamo tuttavia di nuovo supporre che le tecniche attualmente esistenti, seppur avanzatissime per le nostre conoscenze attuali, non siano sufficienti a realizzare quella nuova rivoluzione nei sistemi di computazione prospettata dalla *computazione quantistica*.

Come vedremo in questo articolo, la realizzazione di un computer quantistico avrebbe conseguenze pratiche di portata enorme. Un computer quantistico avrebbe infatti una velocità di calcolo che supera di ordini di grandezza quella realizzabile con i computer tradizionali; questo renderebbe possibile la soluzione di molti problemi che i computer odierni non possono risolvere in modo effettivo, come ad esempio la fattorizzazione di numeri grandi, la cui rilevanza nella crittografia è ben nota. Vedremo anche che l'interesse in questa nuova forma di computazione va ben oltre le applicazioni pratiche.

2. Teoria della computazione quantistica

Il computer quantistico non è semplicemente il prossimo passo nel processo evolutivo dei computer ma anche e, soprattutto, il rappresentante di un paradigma di computazione non classico il cui studio ha dato origine ad un nuovo settore della ricerca teorica in informatica e fisica che va sotto il nome di computazione quantistica. Ad iniziare questa linea di ricerca fu Richard Feynman che per primo si rese conto di un problema fondamentale dei computer classici: non sono in grado di simulare la realtà quantistica. Nel suo famoso articolo `Simulating Physics with Computers' [8], Feynman descrive il problema con estrema semplicità concludendo che solo con un computer quantistico sarebbe stata possibile una simulazione efficiente. Il punto cruciale è che i sistemi fisici quantistici esibiscono un comportamento probabilistico che non corrisponde a quello implementabile sui computer classici.

La computazione classica probabilistica acquistò enorme importanza in informatica soprattutto negli anni `70 del secolo scorso, dopo l'introduzione ad opera di Solovay e Strassen di un algoritmo randomizzato per determinare se un numero intero è primo o no. L'algoritmo, che usa un generatore di numeri casuali, dà una risposta corretta solo con una certa probabilità. Questo fu il primo algoritmo efficiente per risolvere il problema della primalità, per il quale in quegli anni non si conoscevano ancora soluzioni deterministiche[1].

Un algoritmo *probabilistico* usa la casualità (tipicamente il lancio di una moneta) per rappresentare l'incertezza di proseguire una computazione lungo una direzione o un'altra tra le tante possibili. Il modo in cui le scelte fatte ad ogni passo di computazione si combinano per determinare la probabilità del risultato finale è dettato dalla teoria classica della probabilità; in particolare la regola di Bayes stabilisce che la probabilità di un evento che si può verificare in due o più modi distinti è la somma delle probabilità di ciascun modo considerato

[1] *Un algoritmo deterministico che effettua il test di primalità in tempo polinomiale fu poi introdotto nel 2002 da Agrawal, Kayal e Saxena, tre ricercatori dell'Indian Institute of Technology, Kanpur*

separatamente. L'albero in Figura 1a esemplifica una computazione probabilistica con risultato ½ R + ½ B, dove R rappresenta il risultato raggiunto negli stati rossi 5 e 7 mentre B quello raggiunto negli stati blu 4 e 6.

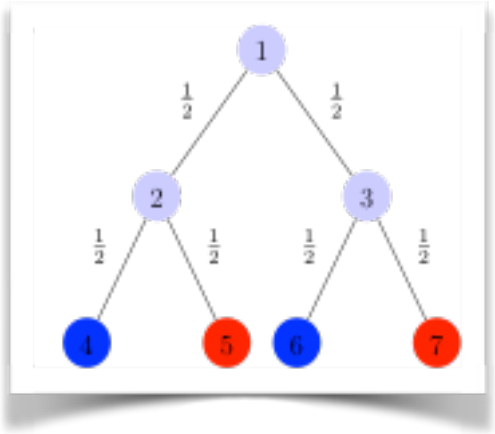


Figura 1a
Una computazione probabilistica in cui ogni cammino di esecuzione ha probabilità 1/4; poiché ciascuno dei due risultati viene raggiunto da due cammini diversi, entrambi i risultati si ottengono con la stessa probabilità 1/4+1/4=1/2.

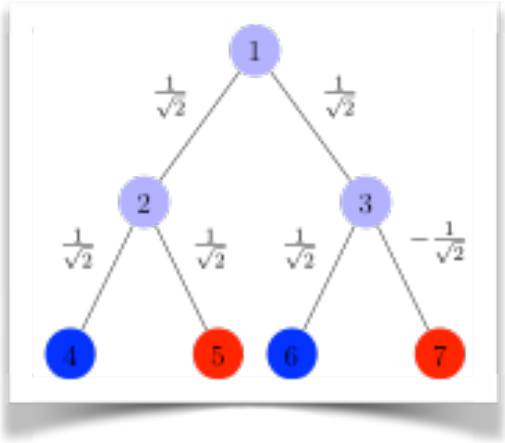


Figura 1b
Una computazione quantistica in cui il risultato blu ha ampiezza di probabilità 1/2+1/2, mentre il risultato rosso ha ampiezza di probabilità 1/2-1/2, da cui si ricava la probabilità 1 per il risultato blue e 0 per il risultato rosso.

L'elemento che rende la computazione quantistica nello stesso tempo più generale (essa comprende la computazione probabilistica come una particolare istanza) e distinta (essa consente nuovi modi di calcolo che non hanno alcuna controparte classica) deriva dalla considerazione di *numeri complessi* al posto dei numeri reali usati nella computazione probabilistica classica. Tali numeri, che al contrario delle probabilità possono essere anche negativi, stabiliscono *ampiezze di probabilità*; da queste si può ottenere la probabilità in senso classico di un certo evento (o cammino di esecuzione), calcolandone il quadrato del modulo. La regola di Bayes viene ora sostituita da un'altra regola che stabilisce come combinare ampiezze di probabilità e che, in onore del famoso fisico promotore della computazione quantistica, è chiamata in [14] regola di Feynman: l'ampiezza di probabilità di un evento che si può verificare in due o più modi distinguibili è la somma delle ampiezze di probabilità di ciascun modo considerato separatamente.

La conseguenza di questa sostituzione è che i diversi percorsi di una computazione possono ora *interferire* distruttivamente gli uni con gli altri. Questo si verifica per esempio quando le ampiezze associate ai due percorsi hanno

modulo uguale ma segno opposto. Una tale situazione è esemplificata dalla computazione quantistica rappresentata in Figura 1b, dove i due numeri complessi corrispondenti alle ampiezze di probabilità per le due derivazioni del risultato rosso (cioè $1/\sqrt{2}\times 1/\sqrt{2}$ e $1/\sqrt{2}\times(-1/\sqrt{2})$) si annullano dando probabilità zero a questo risultato.

Possiamo dunque aspettarci che la nozione di probabilità quantistica abbia grande influenza sul modo di costruire e sulle possibilità computazionali degli algoritmi quantistici. Proprio per l'uso del nuovo concetto di probabilità, questi algoritmi si possono descrivere come algoritmi randomizzati con un generatore quantistico di probabilità al posto del generatore di numeri `pseudo-casuali' tipicamente usato in quelli classici. Usando la fisica quantistica, la generazione di numeri `genuinamente random' si può ottenere oggi mediante un semplice dispositivo quantistico che opera su fotoni (particelle di luce) mediante specchi semi-argentati (*beam-splitter*) e *detector*. Dispositivi di questa natura (e loro varianti) sono stati realizzati e messi sul mercato dalla ditta IDQ (http://www.idquantique.com) e attualmente possono essere acquistati online a prezzi che variano dai 1000 ai 2500 euro.

Da un punto di vista più propriamente teorico degli algoritmi eseguibili su un computer quantistico, questo dispositivo implementa un'operazione chiamata operazione di *Hadamard* (e indicata con H) che compare in tutti gli algoritmi quantistici rappresentandone, come risulterà chiaro in seguito, un elemento imprescindibile.

2.1 Computazione quantistica e multiverso

Capire il funzionamento di un computer classico è relativamente semplice: esso è un sistema fisico che obbedisce alle leggi della fisica classica, cioè le leggi che regolano la nostra esistenza nell'universo macroscopico in cui viviamo e che ci sono quindi familiari. Tuttavia, secondo una particolare interpretazione della teoria quantistica, queste leggi rappresentano solo una particolare istanza o approssimazione della realtà fisica nella quale siamo immersi e che va al di là dell'universo contingente di cui abbiamo esperienza diretta. Tale interpretazione fu proposta nel 1957 da un fisico dell'Università di Princeton, Hugh Everett III, ed è oggi nota col nome di *interpretazione a molti mondi*. Essa spiega i fenomeni quantistici osservati sperimentalmente sulla base dell'esistenza di un'infinità di universi che coesistono mantenendo ciascuno la propria individualità. La sovrapposizione, dunque, altro non è che la visione completa di un oggetto in tutti i suoi possibili stati in tutti gli universi che compongono la realtà fisica o, con un termine coniato da David Deutsch (uno dei promotori della computazione quantistica e grande sostenitore dell'interpretazione di Everett), il *multiverso*.

Nel suo libro `The Fabric of Reality' [6], Deutsch ci spiega tutte le implicazioni di una tale visione del mondo e come la teoria classica della computazione, che possiamo identificare con la teoria delle Macchine di Turing, si può considerare un'approssimazione della teoria quantistica della computazione, proprio come la fisica classica è un'approssimazione della fisica quantistica. L'approssimazione classica della teoria della computazione è comunque sufficiente a descrivere quello che i computer oggi disponibili sono in grado di fare. Quello che essi non sono in grado di fare dipende dal fatto che, nel definire il loro funzionamento e modi di calcolo, si trascura la possibile interazione con gli altri universi. Quest'ultima si rivela negli esperimenti fisici come interferenza quantistica e dà

luogo a comportamenti osservabili ben lontani dalla nostra comune esperienza di vita quotidiana. Analogamente, un computer quantistico potrebbe sfruttare l'interazione tra le diverse computazioni parallele che avvengono nel multiverso per effettuare operazioni che nessun computer classico sarebbe in grado di svolgere.

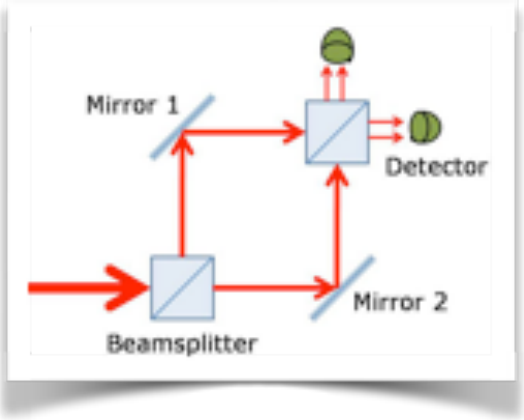
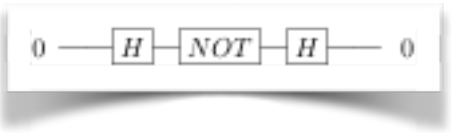


Figura 2a
Un esperimento che rivela l'interferenza quantistica: un singolo fotone passa attraverso uno specchio semi-argentato (beam splitter) che ne cambia la direzione da orizzontale a una sovrapposizione di orizzontale e verticale. Dopo aver attraversato nuovamente il beam splitter il fotone viene rilevato solo dal detector sulla direzione orizzontale

Figura 2b
Circuito quantistico che esegue una computazione equivalente all'esperimento del fotone e del beam splitter.



La corrispondenza tra sistema fisico e computazione quantistica è molto forte. Per rendersene conto basta pensare a un esperimento come ad un processo di calcolo (e viceversa). Si prenda ad esempio il famoso esperimento raffigurato in Figura 2a e consistente in un fotone che viene lanciato contro uno specchio semi-opaco o *beam splitter*. L'effetto del *beam splitter* è quello di creare uno stato in cui il fotone potrà essere rilevato con il 50% delle probabilità nella direzione iniziale e con il 50% nella direzione opposta, cioè il fotone si troverà in metà degli universi a viaggiare in un verso (direzione orizzontale nella figura) e nell'altra metà nel verso opposto (direzione verticale nella figura). Come già accennato, l'effetto del *beam splitter* è quello dell'applicazione dell'operazione di Hadamard allo stato computazionale rappresentato dal fotone. Questo è rappresentato nel circuito in Figura 2b dal qubit 0 in input, il quale viene sottoposto alla componente del circuito che implementa l'operazione H. La presenza dei due specchi in Figura 2a esprime il fatto che il fotone deve poter rimbalzare in tutti gli universi in cui si viene a trovare per effetto del *beam splitter*. L'effetto dello specchio è dunque di invertire la direzione del fotone, rimandandolo indietro verso il *beam splitter*. L'azione dello specchio corrisponde quindi ad applicare un'operazione di NOT allo stato del qubit ottenuto dopo l'applicazione di H (cfr. Figura 2b). Dopo aver incontrato lo specchio, il fotone ritorna quindi al *beam splitter* e a questo punto si osserva che i due *detector* posti nella due direzioni segnalano la presenza del fotone solo nella direzione orizzontale: il *beam splitter* ha agito ora come `*beam joiner*' riportando la direzione del fotone ad essere solo quella

iniziale. Analogamente, la seconda applicazione di H nel circuito di Figura 2b riporta la computazione nello stato di partenza realizzando di fatto una computazione analoga all'esperimento in Figura 2a (ed equivalente a quella rappresentata nell'albero in Figura 1b). Il risultato inaspettato dell'annullamento del secondo risultato creato da Hadamard (o il fatto di non rilevare la presenza del fotone nella direzione verticale creatasi dopo l'impatto con il *beam splitter*) è l'evidenza dell'interazione avvenuta tra le controparti dello stato del fotone (visto come oggetto multiversale) nei due universi corrispondenti alla direzione verticale e a quella orizzontale: esse hanno interferito distruttivamente le une sulle altre riportando il fotone ad assumere la stessa direzione iniziale, cioè quella orizzontale, in tutti gli universi. La computazione corrispondente, d'altra parte, è un modo non classico per calcolare la funzione identità.

2.2 Problemi computazionali

La sfida tra computer quantistici e computer classici si svolge sul piano della complessità computazionale, cioè la teoria che si occupa di stabilire le risorse (tipicamente tempo o spazio) necessarie per risolvere un dato problema mediante un dato algoritmo.

Molti problemi che si presentano nella vita reale possono essere formulati in modo astratto come problemi di ricerca: si cerca tra tutti i possibili candidati quello che soddisfa un certo criterio che lo caratterizza come soluzione al problema dato [4]. In questa formulazione, un metodo, o algoritmo, per risolvere un problema computazionale è migliore di un altro se è in grado di esplorare l'intero spazio di ricerca in modo più *efficiente* dell'altro. Per misurare l'efficienza di un algoritmo si guarda alla crescita asintotica del tempo impiegato (ad es. numero di passi dell'algoritmo) in funzione della dimensione n dell'input (ad es. numero di variabili utilizzate, numero di bit necessari a codificare ogni istanza del problema, ecc.). La teoria della complessità identifica un algoritmo efficiente con uno per cui tale funzione è polinomiale in n, come ad esempio le funzioni n, n^2, n^3, ecc. La classe di tutti i problemi per cui esiste un algoritmo efficiente è notoriamente la classe **P** (= Polynomial-time). In pratica, dopo l'avvento degli algoritmi randomizzati, la classe che identifica i problemi con soluzione efficiente è più realisticamente identificabile con **BPP** (*Bounded-error Probabilistic Polynomial-time*), cioè la classe dei problemi che possono essere risolti da algoritmi probabilistici in tempo polinomiale e con una probabilità di errore minore di un 1/3. Risolvere un problema di ricerca in modo efficiente è quindi un compito non banale se si tiene conto del fatto che tipicamente, per un input espresso su n bit, lo spazio di ricerca contiene un numero di candidati dell'ordine di 2^n; di conseguenza, un semplice algoritmo che fa la ricerca esaustiva in questo spazio avrà necessariamente una complessità limitata superiormente da una funzione esponenziale in n. Questo significa, per esempio, che se le nostre istanze si potessero codificare con n=64 bit, la ricerca esaustiva di tutte le possibili soluzioni potrebbe richiedere fino a 18.446.744.073.709.551.615 test!

Classicamente, la possibilità di progettare algoritmi efficienti dipende da quanto il problema si presta ad una strutturazione conveniente dello spazio delle possibili soluzioni; ad esempio, se quest'ultime si possono disporre ai nodi di un albero binario secondo un criterio discriminante tra soluzioni e non, allora la ricerca procederà velocemente potendo scartare ad ogni passo una metà dei candidati superstiti. In molti casi, tuttavia, l'unico criterio di ricerca risulta quello di controllare i candidati uno per uno, con conseguente necessità di esplorare, nel

peggiore dei casi, l'intero spazio di ricerca. Questa categoria di problemi computazionali è chiamata in teoria della complessità la classe dei problemi **NP-completi** o *difficili*. Esponenti ben noti di questa classe sono il problema del commesso viaggiatore (TSP), il problema della soddisfacibilità (SAT) e il problema dello zaino (Knapsac problem). **NP** sta per *Nondeterministic Polynomial-time*, nome scelto per indicare che una soluzione ad ogni problema di ricerca si può sempre trovare in tempo polinomiale purchè si usi un algoritmo non deterministico, cioè un algoritmo ideale che sfrutta la potenza di un numero indeterminato di macchine parallele per cercare la soluzione e che una volta trovata può verificarla in modo efficiente. L'aggettivo "completi" si riferisce alla proprietà di questi problemi di poter rappresentare qualsiasi problema in NP in modo che ogni soluzione per un problema NP-completo può essere adattata in modo efficiente per risolvere un qualsiasi problema in NP (ma non viceversa). Le relazioni tra queste classi di complessità classiche sono rappresentate nel diagramma A.

La computazione quantistica e, in particolare, l'introduzione di un algoritmo quantistico che risolve in modo efficiente un problema classicamente in NP ha modificato questo scenario rendendo necessaria l'introduzione di una nuova classe di complessità, cioè la classe **BQP**, che descriveremo nel seguito insieme al più famoso algoritmo che la rappresenta, cioè appunto l'algoritmo di Shor per la fattorizzazione di un numero. La collocazione della nuova classe all'interno dello scenario classico può essere approssimativamente raffigurata come nel diagramma B, anche se la relazione tra BQP e NP non è attualmente nota.

La domanda cruciale che da decenni impegna gli algoritmisti e che ancora non ha trovato risposta è: esistono algoritmi efficienti per i problemi **NP-completi** oppure è vero che **P≠ NP**?

La computazione quantistica non è servita finora a dare una risposta a questa domanda. Infatti, sebbene l'algoritmo di Shor riduca drasticamente il tempo di esecuzione richiesto dal più potente computer classico oggi esistente per risolvere il problema della fattorizzazione, questo problema non rappresenta la complessità di tutti i problemi in NP (non è un problema NP-completo) e risolverlo efficientemente non fornisce nessuna evidenza al fatto che NP possa collassare a P. Un altro esempio dove il computer quantistico avrebbe un vantaggio sugli odierni processori è la simulazione del comportamento degli atomi e delle molecole. Tuttavia, ancora una volta, questi risultati non hanno conseguenze sulla famosa questione **P≠ NP**? e, in generale, nonostante gli innumerevoli progressi nello studio della computazione quantistica, non esiste al momento alcuna evidenza che la potenza di calcolo del computer quantistico potrà essere dirimente nello sforzo di risolverla.

Se quindi nei prossimi decenni gli studi di fisici e informatici porteranno alla realizzazione del computer quantistico e dell'informatica quantistica, le ricadute saranno innanzitutto di natura pratica, provocando cambiamenti rivoluzionari almeno nei campi della crittografia, della nanotecnologia e della medicina.

Se invece falliranno, le conseguenze saranno ancora più interessanti sotto molti punti di vista; ad esempio questo potrebbe evidenziare errori in una teoria, quella quantistica, la cui validità è rimasta senza rivali per ormai un secolo, perché "*... not only can physics determine what computers can do, but what computers can do, in turn, will define the ultimate nature of physical laws*" (Rolf Landauer [11]).

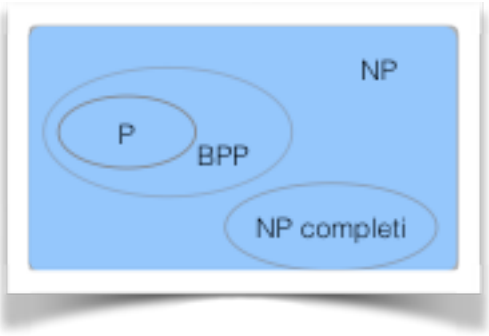


Diagramma A

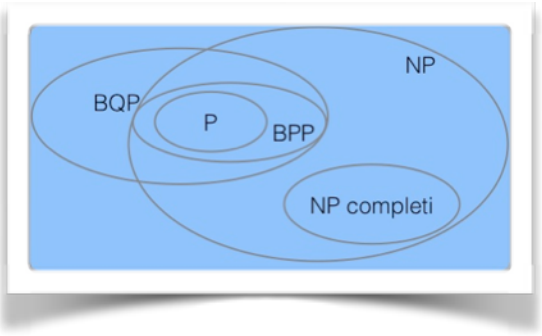


Diagramma B

2.3 Il qubit

L'abilità di manipolare ampiezze di probabilità è un aspetto nuovo che non può essere catturato con il semplice lancio di una moneta. Poiché un bit di informazione non è sufficiente a rappresentare questa nuova abilità, Benjamin Schumacher, fisico teorico e studioso della teoria dell'informazione quantistica al Kenyon College (Ohio) inventò una nuova parola, *qubit*, per indicare l'unità di informazione che rispetta la regola di Feynman al posto della regola di Bayes della teoria classica della probabilità. Il qubit corrisponde al più semplice tra tutti i sistemi fisici quantistici. Per capire la natura di questa entità e la differenza con la sua istanza classica, il bit, dobbiamo fare riferimento alle leggi che regolano il comportamento e l'evoluzione di un sistema fisico reale e di conseguenza l'elaborazione dell'informazione in esso contenuta. Dal punto di vista computazionale i postulati della meccanica quantistica ci permettono di allargare il campo d'azione di un calcolatore ad uno spazio che oltre alle dimensioni classiche corrispondenti alle sequenze binarie (registri di bit) ne include anche tutte le infinite combinazioni (principio di sovrapposizione degli stati) con le loro interazioni non classiche (fenomeno dell'interferenza) e gli effetti sui risultati finali (principio di misurazione).

Sovrapposizione

Le architetture basate sui microchip standard dei computer odierni rispettano rigorosamente la dicotomia del bit classico, cioè il loro funzionamento dipende in modo essenziale dalla codifica binaria dell'informazione (un bit può solo essere 0 oppure 1). La potenziale superiorità di un computer quantistico in quanto a capacità di calcolo viene dal fatto che esso opera su informazione codificata in qubit, cioè oggetti che possono assumere un'infinità di stati oltre agli stati 0 e 1 del bit. Infatti, i postulati della meccanica quantistica identificano il qubit con un vettore v nello spazio complesso bidimensionale C^2 (spazio di Hilbert), cioè con un oggetto

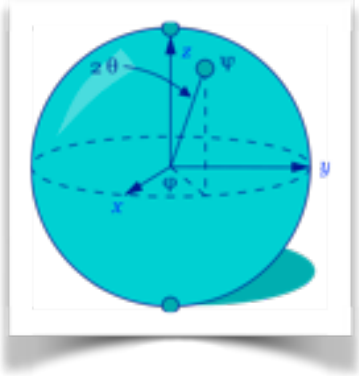


Figura 3
Sfera di Bloch. Il punto ψ sulla sfera rappresenta lo stato α0+β1 di un qubit. Le sue coordinate sferiche (φ, 2θ) sono codificate nelle ampiezze α e β (e viceversa).

della forma v=α0+β1, dove gli scalari α e β sono numeri complessi che esprimono la percentuale di probabilità che lo stato risulti essere effettivamente 0 e 1, rispettivamente. Questi stati intermedi del qubit, che implicano una coesistenza degli stati classici 0 e 1 in determinate proporzioni, vengono chiamati *sovrapposizioni* di stati e possono essere interpretati come situazioni di incertezza sullo stato *interno* del qubit sul cui valore non abbiamo garanzie assolute ma solo una probabilità che questo possa essere 0 oppure 1. Sull'interpretazione del principio di sovrapposizione non c'è tuttavia una tesi universalmente accettata come valida. Come verrà chiarito in seguito, il problema è strettamente legato al problema della misurazione sul quale il dibattito, iniziato alla nascita della teoria quantistica, continua a dividere i fisici teorici assumendo inevitabilmente risvolti filosofici che non affronteremo in questa sede.

Una rappresentazione del qubit che aiuta ad avere un'intuizione visiva di questa entità è la sua identificazione con i punti sulla superficie di una sfera unitaria nello spazio reale a tre dimensioni, nota come la sfera di Bloch (Figura 3) dal nome del fisico svizzero Felix Bloch che stabilì tale corrispondenza.

I punti corrispondenti al polo nord e al polo sud sono tipicamente associati ai due stati corrispondenti agli stati classici[2] 0 e 1, ma oltre a questi ogni altro punto della superficie sferica rappresenta un possibile stato del qubit [9,15]. Questa rappresentazione permette di visualizzare qualsiasi operazione su un qubit come una rotazione di un punto sulla sfera di Bloch. Così come una rotazione può essere applicata al contrario per riportare il punto nella sua posizione originale, un'operazione sul qubit può essere invertita in modo da riportare il qubit dallo stato finale nello stato iniziale, annullando di fatto il suo effetto. Questa *reversibilità* computazionale caratterizza la computazione quantistica e riflette il modo in cui un sistema fisico evolve nel tempo secondo i postulati della meccanica quantistica.

Il problema della misurazione quantistica

Nell'esperimento del *beam-splitte*r rappresentato in Figura 2a, la presenza del *detector* corrisponde ad una misurazione dello stato finale del qubit sottoposto alla computazione in Figura 2b. L'effetto che sperimentalmente si osserva dopo la misurazione di uno stato quantistico è un effetto distruttivo sulla *coerenza* del sistema che fa *collassare* una sovrapposizione in uno stato classico.

Il concetto di sistema coerente si riferisce all'interazione del sistema con un'entità esterna, come ad esempio uno strumento di misura, che determina una fuoriuscita (di parte) dell'informazione contenuta in esso. Questo processo, noto come decoerenza, determina inevitabilmente per le leggi della meccanica quantistica un cambiamento del sistema stesso e, come sarà chiarito in seguito, rappresenta uno dei più grossi ostacoli per l'implementazione pratica della computazione quantistica e la realizzazione di un computer quantistico *general-purpose*.

Il collasso di uno stato quantistico per effetto di una misurazione rappresenta un fenomeno la cui spiegazione diede luogo ad accesi dibattiti sin dalla nascita della teoria quantistica negli anni `20 del secolo scorso, facendo emergere soluzioni

---

[2] *Questa è la base standard dello spazio degli stati di un qubit, ma una qualsiasi coppia di punti antipodali sulla sfera sarebbe una scelta altrettanto adeguata.*

varie e contrastanti ancora oggi in discussione[3]. John von Neumann introdusse il primo trattamento assiomatico rigoroso della meccanica quantistica nel 1955, intervenendo in maniera decisiva sul problema della misurazione e fornendo una spiegazione ai vari paradossi che erano stati introdotti per sostenere l'inadeguatezza della teoria quantistica. Secondo la formalizzazione di von Neumann il processo di misurazione avviene in due fasi. Nella prima fase l'operatore che rappresenta l'osservabile (cioè la proprietà del sistema che si intende misurare) viene applicato allo stato del sistema. In una seconda fase avviene la ``riduzione di stato'', cioè il passaggio dallo stato di sovrapposizione coerente allo stato corrispondente ad uno dei risultati osservabili (corrispondenti agli autovettori dell'operatore lineare che rappresenta l'osservabile). Questa riduzione è nondeterministica e conseguentemente non c'è modo di prevedere quale dei risultati sarà ottenuto prima che il processo di misurazione abbia termine. In altre parole, per un osservabile non è mai possibile stabilire in maniera definita il valore che verrà misurato. La meccanica quantistica fornisce tuttavia delle informazioni statistiche sui possibili risultati di una misurazione secondo quella che è nota come l'*interpretazione statistica di Born*[4]. Attraverso misurazioni fatte su copie del sistema opportunamente preparate, è possibile stabilire la distribuzione probabilistica dei risultati. Il significato di probabilità di un risultato va inteso secondo l'interpretazione data in teoria delle probabilità come frequenza relativa: la probabilità di un risultato è il rapporto tra il numero delle volte che l'esperimento ha successo (cioè si ottiene quel risultato) e il numero totale degli esperimenti fatti, purché si ripeta l'esperimento un numero sufficientemente grande di volte.

2.4 Deutsch, parallelismo e interferenza

Il principio di sovrapposizione implica un enorme potenziale di capacità di calcolo. In particolare, la possibilità di identificare lo stato di una computazione con uno tra gli infiniti vettori dello spazio di Hilbert, cioè con una sovrapposizione qualsiasi di due stati classici, permette di codificare in un qubit molta più informazione di quella che può essere memorizzata in un singolo bit: tutti i numeri complessi nel primo caso, al posto dei soli 0 e 1 nel secondo. È dunque lecito pensare che, dal momento che operare sullo stato di un qubit corrisponde a operare contemporaneamente sia su 0 che su 1, la quantità di passi necessari per effettuare una computazione si possa ridurre notevolmente, tanto più quanto più grande è il numero n di qubit utilizzati: lavorare con n qubit significa in pratica considerare uno spazio di computazione infinito di dimensioni 2^n. In termini di complessità algoritmica questo significa passare da una complessità asintoticamente esponenziale ad una polinomiale in n. Sfruttare le potenzialità offerte dal parallelismo quantistico non è tuttavia immediato perché operare contemporaneamente su tutti i possibili input non produce direttamente tutti i possibili output ma solo una sovrapposizione di essi; sarà poi necessario effettuare una misurazione e quindi la selezione probabilistica di uno solo dei

---

[3] *Per un approfondimento su questo dibattito si può consultare il testo Quantum Theory and Measurement, Wheeler and Zurek, Princeton University Press, 1983, che contiene articoli originali e commenti sul problema della misurazione.*

[4] *Max Born, fisico e matematico tedesco, fu tra i fondatori della teoria quantistica e premio Nobel per la fisica nel 1954.*

possibili risultati. Il parallelismo deve essere quindi sfruttato in modo adeguato nella costruzione di algoritmi quantistici che siano più efficienti di quelli classici.

Un algoritmo che usa il parallelismo quantistico si può vedere come un insieme di computazioni classiche che si svolgono in parallelo su una molteplicità di input, tipicamente tutte le possibili configurazioni iniziali per un dato problema. Tuttavia, questo è solo un passo preliminare verso la costruzione di un algoritmo quantistico. Il passo successivo è identificare il processo di computazione vera e propria che interessa lo stato in sovrapposizione cioè quello che avviene quando il sistema si trova in uno stato di coerenza.

Perché una computazione quantistica possa aver luogo è infatti necessario che il sistema sia coerente. Il modo in cui essa avviene dipende dal tipo di problema che si intende risolvere. I risultati che si sono ottenuti fino ad ora dimostrano che l'unica tecnica algoritmica in grado di abbattere la complessità esponenziale di alcuni problemi considerati classicamente in NP è quella che sfrutta il parallelismo combinato con l'interferenza quantistica. Questa tecnica altro non è che la traduzione in termini computazionali dell'esperimento del fotone e del *beam splitter*

(cfr. Paragrafo 2.1). Verso la metà degli anni '80 del secolo scorso quando ancora non c'erano evidenze su come il parallelismo quantistico potesse essere usato per ottenere un vantaggio computazionale, David Deutsch descrisse un problema che, nonostante la sua semplicità, risultava intrattabile con un computer classico. Deutsch è uno dei pionieri della computazione quantistica e fu probabilmente il primo a mettere in atto l'idea di Feynman descrivendo in [5] un insieme di circuiti universale per la computazione quantistica[5]. L'algoritmo da lui ideato, noto appunto come l'algoritmo di Deutsch[6], introduce una tecnica che verrà poi sviluppata in quella che oggi è nota come la Trasformata di Fourier Quantistica ed è l'ingrediente fondamentale di tutti gli algoritmi quantistici ad oggi conosciuti che esibiscono un vantaggio esponenziale rispetto agli omologhi classici.

Il problema di Deutsch si può descrivere come quello di stabilire se una data funzione booleana f: {0,1} {0,1} darà lo stesso risultato su ogni input oppure risultati distinti su input distinti. La funzione f ci viene data attraverso un oracolo, cioè una scatola nera di cui non conosciamo il funzionamento interno ma che possiamo solo interrogare sui possibili input.

Chiaramente il problema, generalizzato a funzioni booleane di n bit, si può formulare come un problema di ricerca su uno spazio di dimensione 2^n e risulta

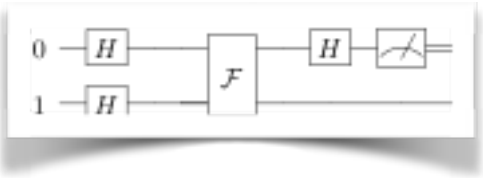


Figura 4
Un circuito quantistico che realizza l'algoritmo di Deutsch. Le linee singole rappresentano qubit, mentre la doppia linea dopo la misurazione rappresenta un bit classico (il risultato).

[5] *A.C. Yaho dimostrò nel 1993 che questi circuiti potevano simulare la macchina di Turing quantistica universale a qualsiasi grado di accuratezza.*

[6] *L'algoritmo fu poi migliorato nel 1998 da Richard Cleve, Artur Ekert, Chiara Macchiavello e Michele Mosca.*

classicamente un problema NP: sarà necessario nel caso più sfortunato un numero di interrogazioni esponenziale in n per poter stabilire con certezza che tipo di funzione è f. Il circuito in Figura 4 è la soluzione proposta da Deutsch che invece risolve il problema con una sola invocazione dell'oracolo. Il circuito opera su due qubit di cui il primo viene preparato nello stato 0 mentre il secondo, destinato a contenere il risultato, viene preparato in una opportuna sovrapposizione di stati ottenuta applicando H allo stato classico 1. L'operazione di Hadamard (*beam splitte*r) applicata a 0 produrrà una sovrapposizione di tutti gli input cosi che un'invocazione dell'oracolo produrrà una sovrapposizione di tutti i risultati (parallelismo). A questo punto entra in gioco l'interferenza realizzata mediante una nuova applicazione di H (*beam joiner*). Per effetto di quest'ultima l'informazione su f si ritroverà nell'output codificata nella fase relativa dello stato finale. Sarà ora sufficiente misurare il primo registro per ottenere la risposta al problema con probabilità 1: se il risultato sarà 1 allora la funzione è certamente costante, se invece sarà 0 allora vorrà dire che sicuramente $f(0) \neq f(1)$.

2.5 Shor e la classe BQP

Quando nei primi anni '80 del secolo scorso, Richard Feynman suggeriva nelle sue lezioni all'università di Caltech (*California Institute of Technology*) l'idea del computer quantistico, Peter Shor, allora studente in matematica che seguiva il corso di meccanica quantistica tenuto da Feynman, fece oro di quelle lezioni e circa tredici anni dopo arrivò ad una scoperta sensazionale. Nel 1994 Shor ideò un algoritmo che, usando un computer quantistico, risolveva il problema di trovare i fattori primi di un numero intero molto grande in maniera efficiente. Questa scoperta portò un grosso cambiamento nel campo della complessità computazionale facendo diventare `facile' un problema che fino ad allora si riteneva di complessità NP. D'altra parte, l'algoritmo prevedeva dei passi di computazione quantistica e quindi non poteva essere considerato al pari degli algoritmi polinomiali classici.

Si introdusse quindi una nuova classe di complessità destinata a contenere tutti i problemi che possono essere risolti con un algoritmo polinomiale *su un computer quantistico* a meno di un errore che si verifica con probabilità minore di 1/3. Questa classe, chiamata **BQP** (*Bounded-error Quantum Polynomial-time*), include anche i problemi che sono classicamente risolvibili con algoritmi deterministici o probabilistici in tempo polinomiale, cioè P e BPP (cfr. diagramma B). Tuttavia non è ancora chiara la sua relazione con i problemi difficili, cioè NP-completi. Una risposta a questa domanda darebbe una risposta anche al problema di stabilire l'effettiva superiorità o meno della computazione quantistica rispetto a quella classica, oltre a risolvere la ben nota questione **P = NP**?

Ritornando all'idea di Shor, la sua tecnica per ottenere lo *speed-up* esponenziale rispetto ai migliori algoritmi classici finora implementati per il problema della fattorizzazione è ancora una volta basata sul parallelismo e l'interferenza quantistica. Rispetto al problema di Deutsch la differenza è nell'uso consistente di risultati matematici (in particolare di teoria dei numeri e aritmetica modulare) per la formulazione del problema. L'ingrediente matematico costituisce la parte classica dell'algoritmo e si può riassumere nel seguente fatto: se N è il numero da fattorizzare, x un numero casuale tra 1 e N-1 e r l'ordine di x modulo N (cioè $x^r=1 \bmod N$), allora basta calcolare il massimo comune divisore tra N e $x^{r/2}-1$ e tra N e $x^{r/2}+1$ per ottenere con alta probabilità due fattori primi di N. La parte

“difficile” dell’algoritmo è quindi ridotta al calcolo dell’ordine r. Per far questo l’algoritmo di Shor usa un circuito quantistico molto simile al circuito di Deutsch, dove però l’oracolo è sostituito da un’opportuna funzione definita in modo da produrre nell’output una sovrapposizione corrispondente alla Trasformata di Fourier Quantistica (TFQ, una generalizzazione di Hadamard) del valore cercato. Questo potrà quindi essere ottenuto mediante un’applicazione della trasformazione inversa.

Lavorando su una sovrapposizione di tutti i possibili input, e sfruttando l’interferenza creata dalle operazioni quantistiche H e TFQ, l’algoritmo permette di calcolare i fattori di N ad un costo dominato da quello di operazioni classiche come il calcolo del massimo comun divisore, mentre il più efficiente algoritmo classico ad oggi noto per lo stesso problema, il “*number filed sieve*”, o crivello del campo di numeri, ha complessità superpolinomiale.

Per avere un’idea di cosa significhi questo dal punto di vista pratico, si pensi che con questo algoritmo si può attualmente fattorizzare un numero di 193 cifre usando una rete di qualche centinaio di computer ad altissima prestazione impiegati esclusivamente a questo scopo; il risultato si ottiene dopo qualche mese di lavoro ininterrotto. Utilizzando lo stesso hardware, per fattorizzare un numero di 500 cifre dovremmo aspettare un tempo più lungo dell’età dell’universo. Se avessimo a disposizione un computer quantistico in grado di effettuare lo stesso numero di operazioni al secondo del supercalcolatore classico descritto prima, potremmo utilizzare l’algoritmo di Shor per ottenere la fattorizzazione di un numero di 193 cifre in appena 0.1 secondi e di un numero di 500 cifre in soli 2 secondi.

A chi importa un tale risultato? In primo luogo, Ron Rivest, Adi Shamir e Len Adleman vedrebbero cadere la congettura che garantisce la sicurezza dello schema crittografico a chiavi pubbliche alla base del loro famoso cifrario RSA (dalle loro iniziali). Nel 1978, quando questo cifrario venne pubblicato sulla famosa rivista "Communications of the ACM", sembrava infatti ragionevole assumere che la fattorizzazione di numeri interi molto grandi fosse un problema difficile. In effetti, sebbene abbia attratto l'interesse di numerosi crittoanalisti, l'RSA è rimasto sino ad oggi sostanzialmente inviolato. Se a questo si aggiunge una grandissima semplicità strutturale, si può capire perché questo metodo di cifratura abbia avuto così tanto successo. Per la sua semplicità l'RSA è ampiamente utilizzato nelle applicazioni pratiche (dalle transazioni finanziarie effettuate in Internet alla protezione della privacy e autenticità dell’email e alla maggior parte delle applicazioni di sicurezza dei dati digitali, informatici e telefonici), e numerose sono le sue realizzazioni in hardware presentate nel corso di questi anni.

Tutto ciò dovrà quindi essere pesantemente rivisto quando/se il computer quantistico sarà realizzato e messo in commercio.

2.6 Grover e la complessità della ricerca algoritmica

Nel 1996 Lov Kumar Grover, originario di Delhi e attualmente ricercatore ai Bell Labs in New Jersey, ideò un metodo quantistico per risolvere problemi di ricerca (notoriamente *difficili*, cioè NP-completi) che migliora di un fattore quadratico le prestazioni degli algoritmi classici fino ad oggi proposti per questi problemi. Il metodo consiste essenzialmente nella definizione di un operatore che ha come sub-routine un oracolo O in grado di stabilire se un certo candidato è soluzione

oppure no al problema dato. Combinato con altre appropriate operazioni, un'invocazione di O sulla sovrapposizione di tutti i possibili candidati determina un'amplificazione dell'ampiezza di probabilità associata alla soluzione, rendendo di conseguenza quest'ultima di gran lunga più probabile come risultato di una misurazione. Questa tecnica si può visualizzare come una serie di rotazioni (applicazioni dell'operatore di Grover) applicate successivamente al vettore iniziale preparato nella sovrapposizione di tutti i candidati soluzione. La sequenza di rotazioni ha l'effetto di avvicinare il più possibile il vettore iniziale al vettore soluzione.

L'algoritmo di Grover è stato dimostrato *ottimale*, cioè nessun algoritmo classico o quantistico potrebbe effettuare una ricerca esaustiva più velocemente dell'algoritmo di Grover. Malgrado il titolo in un certo senso fuorviante dell'articolo in cui Grover introduce la sua tecnica di ricerca quantistica ("A fast quantum mechanical algorithm for database search[7]"), l'algoritmo di Grover potrebbe risultare di scarso vantaggio per le ricerche in ambito puramente databasista, dove una base di dati viene tipicamente realizzata come oggetto *custom-built* mediante memorie di sola lettura. La costruzione di questi oggetti come memorie quantistiche (così come per quelle classiche) richiederebbe di per sè un numero di operazioni esponenziale nel numero dei dati e l'algoritmo di Grover potrebbe aumentare la velocità di ricerca di un fattore al più costante. Inoltre questo vantaggio verrebbe con alta probabilità annullato dalla complessità tecnologica di mantenere la coerenza dello stato di computazione quantistica.

Il grande vantaggio nel poter utilizzare l'algoritmo di Grover, cioè il vantaggio di avere a disposizione un computer quantistico, è invece legato alla impraticabilità dell'alternativa classica della ricerca esaustiva come unica tecnica per i problemi NP-completi. Un campo di applicazione tipico è la criptoanalisi e il problema di decifrare un testo crittografato. Come è noto gli algoritmi di cifratura usano una chiave la cui segretezza è l'unica garanzia per impedire ad una persona non autorizzata di carpire l'informazione contenuta nel testo cifrato. La lunghezza in bit di una chiave dipende dal particolare algoritmo utilizzato ma deve essere sempre fissata in modo da assicurare tale segretezza. Questo significa che non deve essere possibile svelarla mediante un cosiddetto *attacco di forza bruta*: una chiave di n bit avrà 2^n chiavi distinte e non conoscendo quale chiave sia stata usata bisognerà provarle tutte fino ad individuare la chiave giusta. Se un ipotetico nemico avesse a disposizione un computer quantistico il problema rimarrebbe per lui ancora difficile per il fatto che la sua complessità asintotica non è cambiata (rimane NP-completo anche in campo quantistico), ma i progettisti del sistema crittografico dovrebbero ricorrere a chiavi di dimensioni notevolmente maggiori per tener conto del fatto che la potenza di calcolo a disposizione del nemico è aumentata di un fattore quadratico. Per avere un'idea delle ricadute sul piano pratico del guadagno in termini di tempo di ricerca si pensi ad una chiave di lunghezza 10^{30} e si supponga di trovarsi di fronte ad un nemico classico estremamente potente con a dispozione un processore in grado di effettuare 100

[7] *Proceedings of 28th Annual ACM Symposium on Theory of Computing (STOC), pages 212-219, May 1996.*

milioni di test al secondo[8]. Si calcola facilmente che nonostante la sua potenza egli dovrà mettere in conto la necessità di effettuare al più un numero di chiamate dell'ordine di 10^{29} e quindi di impiegare circa 10^{21} secondi, un tempo cioè molto vicino all'età dell'universo. A un suo omologo quantistico con un processore della stessa velocità basterebbero invece 10^{7} secondi, cioè circa quattro mesi, perché il suo algoritmo di ricerca effettuerà nella peggiore delle ipotesi "solo" 10^{15} test.

3. Realizzazione sperimentale di un computer quantistico

3.1 Sovrapposizione quantistica e decoerenza

Le promesse e le possibili implicazioni di un computer quantistico, come abbiamo visto, sono tante. Vediamo ora fino a che punto è stato possibile creare un apparato "reale" in grado di eseguire computazioni quantistiche. Vista l'importanza in questo contesto di alcuni concetti della fisica quantistica, come il principio di sovrapposizione e la decoerenza, iniziamo con un breve riepilogo di quanto già introdotto sopra, con l'aiuto di un altro esperimento fisico leggermente diverso da quello del *beam splitter*.

La realizzazione di un computer quantistico richiede, innanzitutto, l'implementazione fisica del suo elemento chiave, il qubit. Per rendersi conto dell'importanza – e della difficoltà – di questo compito, guardiamo prima al suo equivalente classico, il bit. Esso rappresenta "0" oppure "1" nel sistema binario e può essere realizzato in tantissimi modi: meccanicamente, come pallina su un abaco; elettricamente, con un interruttore che fa passare una corrente elettrica oppure la blocca; e infine elettronicamente, con capacità e transistor, che nei computer moderni sono miniaturizzati fino a raggiungere delle dimensioni di molto meno di un millesimo di un millimetro, permettendo di metterne milioni o addirittura miliardi su una superficie di pochi centimetri quadri. Tuttavia, queste realizzazioni hanno una cosa in comune: seguono le leggi della fisica classica, secondo la quale un qualsiasi oggetto può trovarsi, in un determinato momento, soltanto in uno stato ben specifico. Nel caso del bit, questo vuol dire che esso – per esempio, lo stato logico di una capacità caratterizzato dalla presenza oppure assenza di cariche – può essere nello stato "0" oppure nello stato "1". Non è ammesso nessun altro stato del sistema

Come abbiamo accennato sopra, nella fisica quantistica invece questo non è più vero. Qui vale il principio della sovrapposizione, secondo il quale un oggetto fisico può esistere simultaneamente in due o più stati possibili (cioè, ammessi dalle leggi della fisica quantistica) del sistema. Per semplicità, illustriamo questo principio con un esempio che, secondo Richard Feynman, "porta dentro di sé il cuore della meccanica quantistica" (vedi Figura 5). Un elettrone (oppure un fotone o un'altra particella microscopica) si trova a sinistra di uno schermo con due aperture e si muove verso lo schermo. A destra dello schermo si trova un rivelatore – per esempio, una pellicola fotografica che è sensibile all'arrivo di elettroni. Ogni volta che un elettrone viene lanciato, dopo essere passato attraverso le aperture nel primo schermo, raggiungerà la pellicola e lascerà una traccia su di esso.

[8] *Nella realtà si usano chiavi di di almeno 128 bit per cifrari simmetrici e di 1024 bit per cifrari asimmetrici, anche se questi numeri vengono aggiornati continuamente per far fronte al rapido aumento della velocità degli odierni processori.*

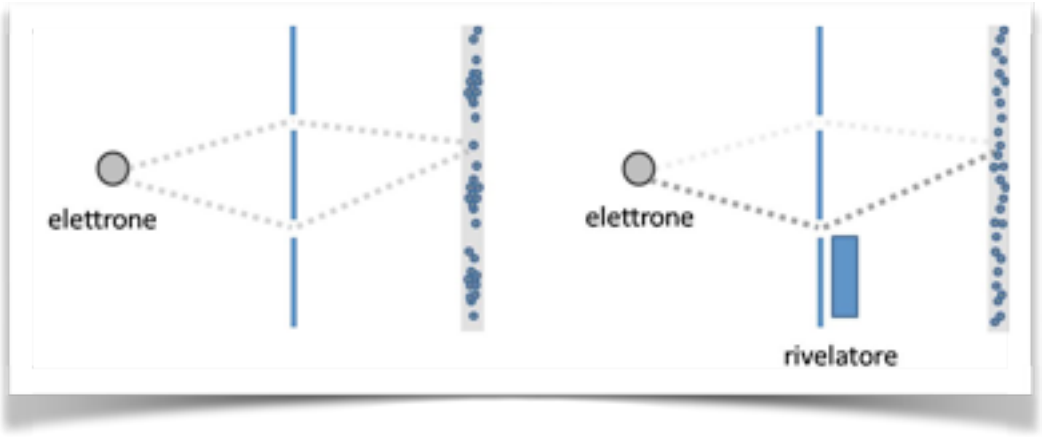


Figura 5
Interferenza quantistica di un elettrone che passa attraverso due aperture in uno schermo. A sinistra: L'interferenza dei due cammini (per l'apertura in alto e quella in basso) crea una variazione di intensità (cioè, della probabilità di trovare l'elettrone in quella posizione) sulla pellicola fotografica. A destra: Se un rivelatore di elettroni indica che l'elettrone è passato per l'apertura in basso, l'effetto di interferenza sparisce.

Il risultato sorprendente di un tale esperimento è che lanciando ripetutamente degli elettroni attraverso lo schermo in questo modo, sulla pellicola fotografica si formerà una struttura periodica molto simile a quella che si crea nell'interferenza di onde sull'acqua. L'interpretazione della fisica quantistica è che gli elettroni, infatti, si comportano come delle onde – e in più, un singolo elettrone in un tale esperimento percorre simultaneamente due cammini, uno che passa per l'apertura superiore e un altro che passa per quella inferiore. Durante il tragitto, quindi, l'elettrone si trova in una sovrapposizione di due stati. Il risultato del processo di interferenza che accade quando l'elettrone arriva alla pellicola e viene rilevato dipende, dunque, da quello che succede in entrambi i cammini.

Questa sovrapposizione, però, può essere compromessa se viene effettuata una misura in grado di rivelare per quale delle aperture l'elettrone è passato. In tal caso la coerenza tra i due cammini viene distrutta, e la struttura periodica sulla pellicola non si forma più.

Il principio illustrato sopra vale per qualsiasi sistema quantistico, e in particolare per un qubit. Per esempio, gli stati logici di un qubit possono essere rappresentati da due stati energetici di un atomo (più precisamente degli elettroni che orbitano intorno al nucleo dell'atomo). Le leggi della fisica quantistica permettono che l'atomo si trovi in una sovrapposizione dei due stati energetici. Una qualsiasi operazione logica – una porta NOT, per esempio – viene quindi effettuata su entrambi gli stati simultaneamente. Nello stesso modo, usando più atomi l'operazione viene effettuata su tutte le combinazioni degli stati 0 e 1 di ciascun atomo e quindi su un numero molto elevato di stati logici. Questo è il principio del parallelismo quantistico.

Come nell'esempio dell'elettrone che percorre allo stesso tempo due cammini diversi, anche nel caso di un qubit una misura fatta durante l'evoluzione

distrugge la coerenza e quindi la sovrapposizione dei due stati quantistici. Per "misura" qui si intende non soltanto una misura fatta volontariamente dall'operatore, ma anche una qualsiasi interazione con l'ambiente che provoca lo stesso effetto di una misura (si può anche interpretare come una "fuga di informazione" dal qubit verso l'esterno). Nell'esempio dell'atomo usato come qubit, una collisione con un altro atomo può provocare la decoerenza, cioè la perdita parziale o totale delle proprietà della sovrapposizione (per questo motivo in molti esperimenti le particelle usate vengono tenute sotto vuoto). Anche l'interazione tra l'atomo e un campo elettrico o magnetico esterno può provocare decoerenza. Appena questo accade, l'integrità del calcolo quantistico è compromessa e il risultato della computazione non è più affidabile.

3.2 I criteri di Di Vincenzo

Una condizione importantissima per realizzare un computer quantistico, dunque, è che il qubit mantenga la coerenza durante tutto il tempo necessario per effettuare un'operazione logica. Questa condizione si può esprimere con la seguente disugualianza: $t_{coh} >> t_{porta}$, dove t_{coh} è il tempo di coerenza del qubit e t_{porta} è il tempo impiegato per effettuare l'operazione di porta logica.

Alla condizione di coerenza si aggiungono altri criteri per la scelta di un sistema fisico adatto per implementare un computer quantistico, elencati nel 2000 da Davide Di Vincenzo [7]:

- Identificazione di qubit ben definiti. Questo criterio richiede che il sistema fisico scelto permetta di identificare delle entità ben distinte – per esempio, gli spin di nuclei atomici oppure singoli atomi preparati dentro un reticolo ottico (vedi sotto) – che possano svolgere il ruolo di qubit.
- Preparazione affidabile dello stato iniziale del computer quantistico. Evidentemente, deve essere possibile inizializzare il computer in uno stato ben noto, per esempio "00.....000", dal quale può partire l'algoritmo quantistico.
- Operazioni precise di porta quantistica. Bisogna poter controllare lo stato dei qubit in maniera accurata per implementare le varie porte quantistiche – rotazione di fase, gate CNOT – sia per singoli qubit che per coppie di qubit. Questo, in pratica, richiede sia un controllo preciso dei campi magnetici, impulsi laser ecc. sia un'ottima conoscenza delle proprietà fisiche del sistema.
- Possibilità di misurare in maniera accurata lo stato quantistico dei qubit. Al termine dell'algoritmo, è necessario "leggere" lo stato del sistema per conoscere l'esito della computazione.

Vedremo in seguito alcuni sistemi fisici che sono stati realizzati in laboratorio e che potrebbero soddisfare i criteri di Di Vincenzo. Questi sistemi si possono suddividere in due classi: sistemi *naturali*, quali atomi, molecole e fotoni, e sistemi *artificiali*, ovvero fatti dall'uomo, come le giunzioni di Josephson.

Visto il numero ormai molto elevato di sistemi sotto considerazione, nella maggior parte dei casi ci limiteremo a descrivere brevemente le loro caratteristiche essenziali. L'approccio basato sugli ioni intrappolati [12], invece,

verrà spiegato più in dettaglio per illustrare le difficoltà che si incontrano nella realizzazione di computer quantistici e per presentare il tipo di tecniche sviluppate per superare tali difficoltà.

3.3 Ioni intrappolati

Per molti anni il metodo degli ioni intrappolati è stato considerato come il candidato più promettente per realizzare un computer quantistico, e tuttora la ricerca sta andando avanti a pieno ritmo, anche se le aspettative sono state leggermente ridimensionate. Comunque, le tecniche sviluppate per controllare e manipolare gli stati quantistici di singoli ioni da sole rappresentano un importante progresso scientifico, e nel 2012 i fisici David Wineland e Serge Haroche sono stati onorati col premio Nobel per la fisica per le loro scoperte in questo campo.

La trappola di Paul

La storia della computazione quantistica con ioni intrappolati iniziò nel 1995, quando il fisico teorico austriaco Peter Zoller e il suo collega spagnolo Ignacio Cirac pubblicarono un articolo di ricerca di sole quattro pagine ma che diede inizio a un campo di ricerca che negli anni successivi avrebbe attratto centinaia di ricercatori. Nel loro articolo i due fisici proposero un approccio alla computazione quantistica nel quale si usano degli atomi carichi, anche noti come ioni, che vengono tenuti fermi nello spazio da campi elettrici. Gli stati quantistici necessari per realizzare dei qubit sono quelli degli elettroni dello ione, simili a quelli di un atomo neutro. Con fasci laser i singoli ioni possono poi essere controllati per eseguire delle porte quantistiche (vedi Figura 6).

La scelta di ioni come qubit sembra quasi naturale: grazie alla loro carica possono essere tenuti fermi e manipolati da campi elettrici e quindi non è necessario fisicamente “toccarli”, cosa che li disturberebbe e in ultima analisi distruggerebbe gli stati quantistici. Inoltre, scegliendo i livelli quantistici giusti dello ione si possono realizzare qubit con tempi di coerenza lunghissimi, fino a diversi secondi. C’è infine anche una considerazione pratica a favore di questa scelta e cioè che le tecniche per intrappolare particelle cariche sono state studiate per anni, e quindi si sa che in principio l’approccio deve funzionare.

Nel computer quantistico con ioni intrappolati, essi vengono tenuti fermi dentro una trappola di Paul. Una trappola di Paul è basata sul principio della “sella ruotante”: una pallina posata su una sella è intrappolata nella direzione longitudinale, nella quale la sella è rialzata, ma può facilmente scappare lateralmente. Se la sella viene montata su un palo ruotante, invece, ogni volta che la pallina inizia a scappare lateralmente, la posizione della sella è già cambiata ed a questo punto la pallina vede davanti a se la parte rialzata della sella. In questo modo, la pallina è effettivamente intrappolata in tutte le direzioni.

Un effetto analogo può essere usato per intrappolare delle particelle cariche in campi elettrici. Mentre una legge di James Clark Maxwell, lo scopritore delle leggi omonime dell’elettrodinamica, vieta l’intrappolamento stabile di una carica in un campo elettrico statico, è possibile creare delle trappole stabili usando campi oscillanti. L’equivalente di una sella nel caso di campi elettrici è un cosiddetto campo quadrupolare, formato per esempio dentro una configurazione di quattro elettrodi con segno alternato del potenziale. La “rotazione” della sella è provocata da una variazione periodica dei segni del potenziale, con il risultato che una carica posta in una tale trappola dinamica rimane ferma (a parte delle piccole oscillazioni

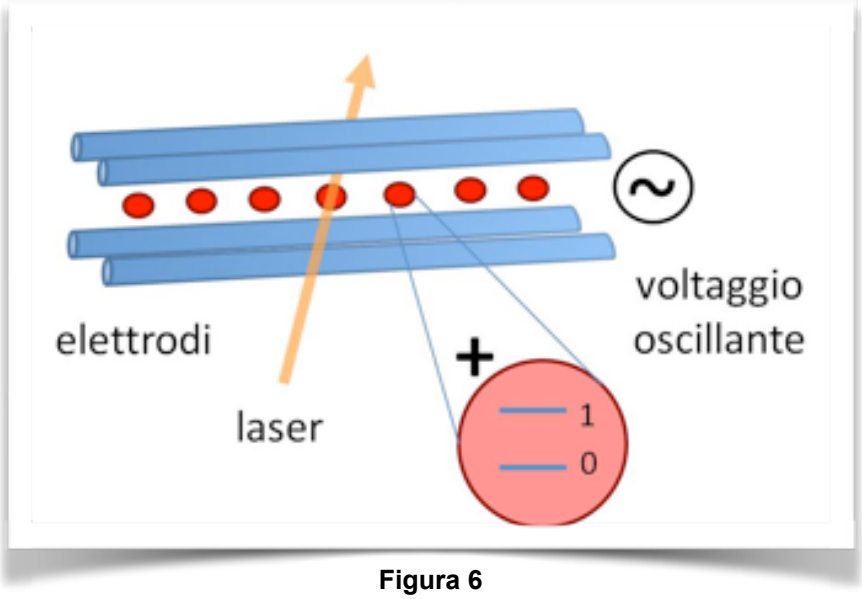


Figura 6
Una trappola di Paul (lineare) per intrappolare ioni. Il fascio laser può essere puntato su un singolo ione per controllarlo (per esempio, per effettuare una porta quantistica su un singolo qubit, rappresentato per i due livelli energetici 0 e 1).

note come micromoto). In questo modo si possono intrappolare e studiare piccoli oggetti come grani di polvere, ma anche elettroni o – appunto – ioni.

Una volta intrappolato in una trappola di Paul, uno ione non può essere usato subito come qubit per la computazione quantistica. Tipicamente gli ioni vengono intrappolati da un gas a temperatura ambiente, il che vuol dire che possiedono un'elevata energia cinetica e che una volta intrappolati oscilleranno dentro la trappola. Questo moto incontrollato rende difficile un controllo accurato dello ione, ed è quindi necessario ridurlo. Ridurre la velocità media di un gas, ovviamente, significa raffreddarlo

Tecniche di raffreddamento

Il raffreddamento viene effettuato tramite dei fasci laser. In un primo passo viene usato il "raffreddamento Doppler", così chiamato perché sfrutta l'effetto Doppler – quell'effetto che si conosce bene dall'apparente variazione in frequenza della sirena di un ambulanza che si avvicina oppure allontana. Per rallentare il moto degli ioni viene usato un effetto simile: un fascio laser che incide su un ione con una frequenza leggermente più bassa di quella risonante tra due stati quantistici dello stesso viene assorbito più facilmente da uno ione che si sta muovendo verso il fascio. In questo caso, lo ione "vede" una frequenza un po' più alta e quindi più vicina a risonanza. Vice versa, uno ione che si sta allontanando dal fascio laser vede una frequenza più bassa e quindi ancora più lontana dalla risonanza. Se ora teniamo conto del fatto che ogni volta che uno ione assorbe un fotone del fascio laser subisce un piccolo urto nella direzione opposta, vediamo subito che se illuminiamo lo ione da tutte le direzioni spaziali esso sentirà una forza rallentante dovunque si muova, come se si muovesse in un liquido viscoso (si parla anche di "melassa ottica").

Risultati ottenuti con ioni intrappolati

In questo modo, e usando altre tecniche simili e ancora più sofisticate, è possibile raffreddare uno ione fino a raggiungere lo stato quantistico più basso possibile. Partendo da un tale stato, già nel 1995 David Wineland riuscì a realizzare una porta CNOT con un singolo ione intrappolato (usando come primo qubit lo stato quantistico dell'elettrone e come secondo qubit quello del moto dello ione). Da allora numerosi gruppi di ricercatori hanno sviluppato delle tecniche sempre più avanzate. Nel 2003 all'università di Innsbruck in Austria fu realizzata una porta CNOT seguendo l'approccio di Zoller e Cirac del 1995. In quell'esperimento vennero usati due ioni dentro una trappola di Paul che si potevano indirizzare separatamente con due fasci laser. Da allora, i fisici sono riusciti anche ad implementare dei semplici algoritmi quantistici, come per esempio l'algoritmo di Deutsch. Per poter implementare algoritmi più complicati, ad esempio quello di Shor per numeri grandi, uno degli ostacoli principali è la scalabilità. Mentre fino ad una mezza dozzina di ioni possono essere intrappolati e manipolati dentro una trappola di Paul senza problemi, non è per niente banale aumentare questo numero fino a decine o centinaia di ioni. Un approccio studiato negli ultimi anni risolve questo problema usando delle trappole suddivise in vari segmenti, ciascuna dei quali contiene circa dieci ioni. Il calcolo quantistico può essere effettuato agendo su un segmento alla volta, con trasporto degli ioni tra i segmenti nelle varie fasi dell'algoritmo.

3.4 Atomi neutri in reticoli ottici

Come abbiamo visto, la realizzazione di un computer quantistico con ioni intrappolati ha come limitazione principale la scarsa scalabilità. Questa limitazione può essere superata in parte usando atomi neutri che vengono intrappolati dentro dei "cristalli di luce" creati da fasci laser sovrapposti che creano interferenza. Tali reticoli ottici intrappolano gli atomi sfruttando la forza della luce (nota come forza dipolare), e la scelta libera della geometria dei fasci laser permette di creare delle strutture spaziali a piacere, per esempio cristalli tridimensionali. In queste strutture possono essere intrappolati milioni di atomi che possono essere usati come qubit. Il problema principale, al momento attuale, sta nel realizzare porte quantistiche con due o più qubit. Per implementare tali porte è necessaria una interazione tra i qubit, che nel caso di ioni è data dall' interazione elettrostatica ma è assente per atomi neutri. Un approccio studiato negli ultimi anni usa stati altamente eccitati, noti anche come stati di Rydberg, per indurre un'interazione forte tra atomi adiacenti nel reticolo [16].

3.5 Qubit in superconduttori

I superconduttori sono dei materiali che conducono la corrente elettrica senza nessuna resistenza. Una corrente che scorre in un anello fatto di un superconduttore girerà dentro l'anello per sempre. La superconduttività fu scoperta dall'olandese Kammerlingh Onnes nel 1911 e spiegata teoricamente nel 1957 da tre scienziati americani che usarono il concetto del condensato di Bose-Einstein, nel quale delle particelle bosoniche si aggregano tutti nello stesso stato quantistico, benché gli elettroni che conducono la corrente elettrica siano dei fermioni che non possono condividere lo stesso stato quantistico. La teoria di Bardeen, Cooper e Schrieffer risolvette questo problema introducendo il concetto della coppia di Cooper – cioè, una coppia fatta da due elettroni (che sono

fermioni) che, insieme, si comportano come un bosone e quindi possono formare un condensato di Bose-Einstein insieme ad altre coppie di Cooper.

Anche se la corrente che scorre dentro un superconduttore è fatta da miliardi di elettroni (o meglio coppie di Cooper), la si può considerare come un singolo stato quantistico. Di conseguenza, tale corrente può anche esistere in uno stato di sovrapposizione di due o più stati quantistici - per esempio, in una sovrapposizione di correnti che scorrono allo stesso tempo in senso orario e antiorario dentro un anello superconduttore. Nello stesso modo una corrente che scorre avanti e indietro in un oscillatore può esistere in una sovrapposizione di stati quantistici dell'oscillatore. È lecito, quindi, pensare che i superconduttori possano essere dei candidati possibili per l'implementazione di un computer quantistico.

Vi sono alcuni vantaggi ovvii di un tale approccio rispetto all'uso di ioni o atomi come abbiamo visto fino ad ora. Innanzitutto, i superconduttori sono delle strutture fatte dall'uomo, e quindi è possibile adattare le loro proprietà alle esigenze del problema. Gli ioni e gli atomi, d'altro canto, sono dati dalla natura, e le loro caratteristiche non possono essere modificate. Inoltre, i circuiti di superconduttori possono essere fabbricati usando i processi ben noti che vengono già applicati alla produzione di circuiti integrati e microchip per computer classici.

Nonostante questi vantaggi non è affatto semplice usare i superconduttori per implementare qubit [13,18]. Un problema fondamentale è che gli stati quantistici di un oscillatore superconduttore sono equidistanti, cioè la differenza in energia tra uno stato e gli stati adiacenti è la stessa per tutti gli stati. Questo fa sì che diventi impossibile individuare due stati da usare come 0 e 1 del qubit. Esiste, però, un rimedio, la cosiddetta giunzione di Josephson. Tale giunzione consiste, sostanzialmente, in una lastra isolante molto sottile inserita tra due fili superconduttori (Figura 7). Nel mondo classico, per definizione un isolante non fa passare nessuna corrente. Nella fisica quantistica, invece, le coppie di Cooper di

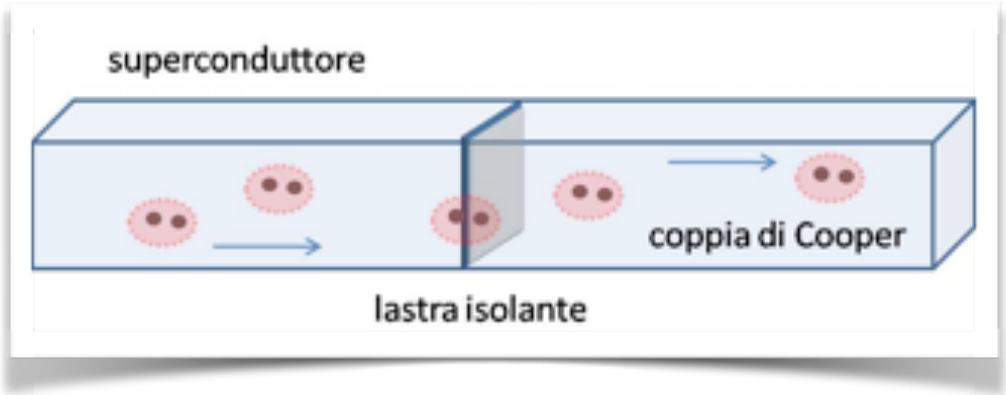


Figura 7
Schema di una giunzione di Josephson. Le coppie di Cooper possono attraversare la lastra isolante tramite il tunneling quantistico.

un superconduttore possono attraversare la barriera isolante tramite l'effetto tunnel. Una conseguenza di questo effetto è che si possono distinguere due livelli energetici del sistema, che a loro volta sono utilizzabili come qubit. Recentemente sono state sviluppate delle tecniche per una lettura efficace dello

stato di questi qubit, ed i tempi di coerenza sono stati allungati fino ad essere abbastanza lunghi da permettere l'esecuzione di alcune porte quantistiche.

3.6 Elettroni in quantum dots

I *quantum dots* sono delle strutture a semiconduttore in grado di confinare singoli elettroni in gabbie minuscole le cui dimensioni tipicamente sono inferiori a un micrometro. Dentro un tale *quantum dot*, l'energia di un elettrone è quantizzata, permettendo all'elettrone di muoversi soltanto in determinate "orbite". Per questo motivo i *quantum dots* vengono anche chiamati "atomi artificiali". Negli ultimi anni i ricercatori hanno investigato la possibilità di usare tali *quantum dots* come qubit. In particolare, lo spin di un elettrone si presta in maniera naturale alla realizzazione degli stati logici 0 e 1 di un qubit.

Per poter fare computazione quantistica con gli elettroni in *quantum dots*, bisogna dimostrare che è possibile implementare la porta CNOT oppure un'altra porta logica universale a due qubit oltre alla manipolazione di un singolo qubit. In esperimenti recenti questo è stato fatto, e sono stati misurati dei tempi di coerenza di alcuni microsecondi.

Una delle sfide più importanti nell'uso di quantum dots come qubit è la lettura dello stato finale della computazione. Per una lettura efficiente il quantum dot deve essere molto vicino al dispositivo di lettura; se invece è troppo vicino quest'ultimo può causare una decoerenza che interferisce con la computazione stessa.

3.7 Risonanza magnetica

Uno dei primi approcci sperimentali alla computazione quantistica è stata la risonanza magnetica (NMR). Questa tecnica [17], molto diffusa nella diagnostica, usa dei campi elettromagnetici per invertire la direzione dello spin del nucleo di un atomo dentro una molecola. La frequenza caratteristica per questa inversione dipende sia dallo spin stesso che anche dagli spin nucleari di altri atomi nella molecola (tramite accoppiamento mediato da elettroni). Mentre in diagnostica questa dipendenza viene sfruttata per distinguere diverse molecole, nell'ambito della computazione quantistica si può usare per eseguire porte quantistiche sia su un qubit che su due qubit. In questo modo nel 2001 è stato implementato l'algoritmo di Shor per fattorizzare il numero 15 usando molecole in cui i spin nucleari di 5 atomi di fluoro (simbolo chimico "F") e 2 due di carbonio (simbolo "C") fungevano da qubit (vedi Figura 8). Per fattorizzare numeri più grandi bisognerebbe aumentare di ordini di grandezza il numero di spin contenuti in una molecola, il che richiederebbe la sintesi controllata di molecole contenenti migliaia di atomi. Al momento attuale questa non sembra essere possibile, e per questo motivo la risonanza magnetica non viene più considerata una tecnica adatta per la realizzazione di computer quantistici.

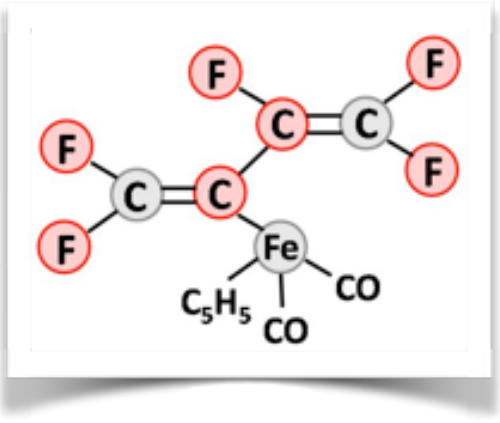


Figura 8
Molecola usata per implementare l'algoritmo di Shor. Gli atomi usati come qubits sono evidenziati in rosso.

3.8 Fotoni

Nella prima parte di questo articolo abbiamo parlato più volte di fotoni e del fatto che un *beam-splitter* può essere considerato un'implementazione di una porta Hadamard. Sembrerebbe, quindi, possibile usare fotoni per creare un computer quantistico. In linea di principio questo è vero, ma l'assenza di interazioni tra due o più fotoni rende complicata la realizzazione di porte a più qubit. Comunque, negli ultimi anni sono state sviluppate tecniche in grado di implementare tali porte tramite delle misure quantistiche e post-selezione [9].

4. Conclusioni

Nonostante considerevoli sforzi e notevoli progressi negli ultimi vent'anni, ad oggi non è ancora stato possibile costruire un computer quantistico in grado di fare cose "utili"- cioè, computazioni che non si possano eseguire sui più potenti computer oggi in commercio. La ditta canadese D-Wave da qualche anno sta sviluppando computer quantistici che si basano sulla tecnica del *quantum annealing*, ma al momento non è chiaro se il computer prodotto dalla D-Wave veramente esegua computazioni quantistiche e se, quindi, potrebbe superare le capacità di un computer classico[9].

In parallelo allo sviluppo di computer quantistici, più recentemente si è manifestato un altro filone di ricerca che si concentra sui cosiddetti simulatori quantistici. Nello spirito di Richard Feynman, che negli anni '80 del secolo scorso si chiedeva fino a che punto la fisica quantistica potesse essere simulata su dei computer classici, l'idea del simulatore quantistico è piuttosto semplice. Evitando di simulare un sistema quantistico su un computer, si crea nel laboratorio un sistema quantistico ben controllato in grado di simulare il fenomeno di interesse. A tutti gli effetti, quindi, un simulatore quantistico si può definire come computer quantistico "a singolo uso".

Scott Aaronson afferma nel suo libro [1] che fortunatamente oggi possiamo dire di aver fatto grandi passi avanti grazie a decenni di studio e di lavoro nel campo della computazione quantistica e dei fondamenti della teoria quantistica.

Tuttavia, visto che al momento non possiamo ancora contare su un computer quantistico per svolgere quei compiti che siamo soliti eseguire su un normale pc (e soprattutto per quelli che non possono essere svolti neanche dai più potenti computer oggi disponibili) una domanda che potrebbe venire spontanea al lettore è: ma allora ha un senso studiare la computazione quantistica?

Certamente la ricerca nel campo della computazione quantistica è puramente teorica e altamente speculativa; pur tuttavia la risposta al lettore è (in breve) `sì, ha senso'. Una risposta più dettagliata potrebbe elencare varie motivazioni, ma la più importante è che la ricerca teorica in generale (e quindi nel caso specifico dell'informatica e dell'informazione quantistica) contribuisce in modo fondamentale alla nostra comprensione dell'universo e ci permette di acquisire conoscenze che, indipendentemente dall'esistenza fisica del computer quantistico, rappresentano un arricchimento culturale e scientifico dell'umanità.

---

[9] *Si veda a tal proposito il recente articolo di Jeremy Hsu su IEEE Spectrum (http://spectrum.ieee.org/computing/hardware/dwaves-year-of-computing-dangerously) e il video del seminario di Matthias Troyer, fisico dell'ETH, su http://nitsche.mobi/2013/troyer/.*

Qualunque sarà il risultato degli sforzi rivolti alla costruzione del computer quantistico, il successo della computazione quantistica si può comunque affermare già da ora come il raggiungimento di un risultato non meno importante: l'aver messo in relazione molte questioni fondamentali della fisica e dell'informatica in uno sforzo scientifico comune.

Bibliografia

[1] Aaronson, S., *Quantum Computing since Democritus*, Cambridge University Press, 2013

[2] Bohr, N., Discussion with Einstein on Epistemological Problems in Atomic Physics, in Albert Einstein: Philosopher-Scientist, Cambridge University Press, 1949

[3] Das, A., Chakrabarti, B.K., *Colloquium*: *Quantum annealing and analog quantum computation,* Reviews of Modern Physics, vol. 80, p. 106, 2008

[4] Dasgupta, S., Papadimitriou, C., Vazirani, U., *Algorithms*, Mcgraw Hill Book Co., 2006

[5] Deutsch, D., Quantum Theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society of London, vol. 400, p. 97,1985

[6] Deutsch, D., *The Fabric of Reality*, Penguin Books, London, 1997

[7] Di Vincenzo, D.P., The Physical Implementation of Quantum Computation, Fortschritte der Physik, vol. 48, p. 771, 2000

[8] Feynman, R.P., *Simulating Physiscs with Computers*, International Journal of Theoretical Physics, vol.21, p. 467, 1982

[9] Kaye, P.R., Laflamme, R., Mosca, M., *An Introduction to Quantum Computing*, Oxford University Press, 2007

[10] Kok, P., Munro, W.J., Nemoto, W., Ralph, T.C., Dowling, J.P., Milburn, G.J., *Linear optical quantum computing with photonic qubits*, Reviews of Modern Physics, vol. 79, p. 135, 2007

[11] Landauer, R., Computation and Physics: Wheeler's Meaning Circuit, Foundations of Physics, vol. 16, 1985

[12] Leibfried, D., Blatt, R., Monroe, C., Wineland, D., *Quantum dynamics of single trapped ions,* Reviews of Modern Physics, vol. 75, p. 281, 2003

[13] Makhlin, Y., Schön, G., Shnirman, A., Quantum-state engineering with Josephson-junction devices, of Modern Physics, vol. 73, p. 357, 2001

[14] Milburn, G.J., *The Feynman Processor*, Perseus Books, 1998

[15] Nielsen, M.A., Chuang, I.L., Quantum Computation and Quantum Information, Cambridge University Press, 2000

[16] Saffman, M., Walker, T.G., Mølmer, K., *Quantum information with Rydberg atoms*, Reviews of Modern Physics, vol. 82, p. 2313, 2010

[17] Vandersypen, L.M., Chuang, I.L., NMR techniques for quantum control and computation, Reviews of Modern Physics, vol. 76, p. 1037, 2005

[18] Ze-Liang X., Ashhab, S., You, J.Q., Nori, F., Hybrid quantum circuits: Superconducting circuits interacting with other quantum systems, Reviews of Modern Physics, vol. 85, p. 623, 2013

Biografie

Alessandra Di Pierro ricopre il ruolo di Professore Associato presso il Dipartimento di Informatica dell'Università di Verona, dove insegna Informatica Quantistica nel corso di laurea magistrale in Ingegneria e Scienze Informatiche. La sua attività di ricerca si svolge nell'ambito della semantica e dell'analisi dei linguaggi probabilistici e in quello della computazione quantistica, dove recentemente si è rivolta allo studio del paradigma di computazione topologica.

Email: alessandra.dipierro@univr.it

Oliver Morsch Primo Ricercatore presso l'Istituto Nazionale di Ottica (INO-CNR) a Pisa. Dopo la laurea in fisica all'Università di Oxford (Inghilterra) nel 1995, ha conseguito il dottorato di ricerca, sempre a Oxford, nel 1999. La sua ricerca sperimentale si concentra sugli studi di atomi freddi, condensati di Bose-Einstein, controllo quantistico e atomi di Rydberg.

Email: morsch@df.unipi.it