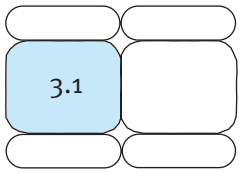
DAL COMPUTER CLASSICO A QUELLO QUANTISTICO: REALIZZABILITÀ E POTENZIALI APPLICAZIONI

Ernesto Hofmann

Gli odierni computer non sono altro che realizzazioni fisiche della macchina di Turing universale. Pur con delle sostanziali differenze, anche il più semplice PC può affrontare, seppur più lentamente, qualsivoglia problema risolubile da un supercomputer. Il computer quantistico è, invece, una macchina del tutto diversa, che, utilizzando i principi della meccanica quantistica potrebbe affrontare problemi che, anche in linea di principio, sarebbero insolubili per qualunque computer classico.



1. INTRODUZIONE

Qualche mese fa, su questa stessa rivista (Mondo Digitale n. 1, 2003, "Quantum Computing: sogno teorico o realtà imminente"), Emanuele Angeleri ha fornito un'affascinante descrizione del computer quantistico fornendo gli elementi fondamentali necessari per comprenderne il funzionamento.

Questo articolo può essere considerato un'ideale continuazione dell'analisi di Angeleri con l'obiettivo di approfondire alcuni aspetti più specifici, quali soprattutto le attuali tecnologie costruttive e alcune significative applicazioni.

Tutti hanno più o meno un'idea di come sia fatto, almeno esternamente, un computer. Dai grandi computer spesso apparsi in film famosi, come *2001 Odissea nello spazio*, ai *personal computer*, presenti ormai quasi in ogni casa, l'idea del computer si è sempre più diffusa nell'immaginario collettivo; e i computer, in tale immaginario, sembrano più o meno tutti simili, dimensioni a parte.

Ma se si potesse osservare un computer quantistico che cosa si vedrebbe? Certamente qualcosa di molto diverso da un computer tradizionale. Probabilmente si riconoscerebbero ancora uno schermo e una tastiera, ma il resto sarebbe molto differente.

Si vedrebbero dispositivi dalle forme inconsuete, come generatori di onde elettromagnetiche o di impulsi *laser* o, ancora, complessi dispositivi di raffreddamento. E i circuiti del computer quantistico, se di circuiti si può parlare, sarebbero anch'essi profondamente diversi. La maggior parte dei prototipi di circuiti quantistici, finora realizzati, sono aggregati di atomi o molecole, talora sospesi nel vuoto o immersi in sostanze liquide, e sottoposti a campi magnetici o a radiofrequenze.

Nulla di simile, quindi, a un tradizionale *chip* all'interno del quale circolano incessantemente microscopiche correnti. Ma la differenza è, in realtà, più profonda. Il computer quantistico non è un'evoluzione di quello classico ma una macchina del tutto diversa.

2. COME NASCE IL COMPUTER QUANTISTICO

Il computer classico è una macchina in grado di simulare la realtà con un certo grado di approssimazione. La modellazione aerodinamica, la progettazione di nuovi materiali, la bioinformatica consentono veri e propri esperimenti virtuali utili per comprendere i meccanismi della natura. La simulazione della realtà per mezzo del computer, dopo l'ipotesi teorica e l'esperimento, diventa il terzo pilastro della conoscenza scientifica.

Nel 1981, al *Massachusetts Institute of Technology* (MIT) si tenne un convegno che sarebbe stato il primo sul rapporto che esiste tra fisica e computazione. Richard Feynman, probabilmente il più grande fisico teorico del XX secolo, dopo Einstein, presentò una memoria dal titolo "Simulating Physics with Computers" [5]. Feynman non vedeva nulla di particolarmente eclatante nelle simulazioni approssimate della realtà fatte fino ad allora dai computer.

Era, invece, interessato alla possibilità di ottenere una simulazione esatta attraverso un computer che potesse fare le stesse cose che fa la natura.

Feynman già intuiva che la computazione non era solo una disciplina matematica ma anche fisica. La simulazione di un fenomeno sul computer classico richiede un mondo prevedibile in modo deterministico. Per esempio, in una partita a biliardo i movimenti delle palle obbediscono a leggi newtoniane ben note.

Per ogni causa (colpo) c'è un ben prevedibile effetto (traiettoria). Ci sono certamente limiti alla precisione della simulazione, ma questi limiti nascono dalla nostra ignoranza di ogni singolo elemento e possono, comunque, essere indefinitamente perfezionati.

Anche con un progressivo perfezionamento ingegneristico i circuiti elettronici operano, invece, sempre nello stesso modo e a fronte degli stessi dati in ingresso producono costantemente gli stessi risultati: 2 + 2 è sempre uguale a 4. Non ci sono incertezze nel comportamento di circuiti costituiti da miliardi di trilioni di atomi ed elettroni. "Ma un computer tradizionale fino a che punto può emulare il mondo quantistico?" si domandava Feynman, e aggiungeva: " ...non sono contento con le analisi fin qui fatte con la teoria classica perché la natura non è classica e se si vuole simulare la natura è meglio farlo quanto-meccanicamente, il che non sarà così facile".

3. COS'È IL MONDO QUANTISTICO

A chi non è capitato, guardando attraverso il vetro di una finestra, di vedere non solo il paesaggio esterno ma spesso anche la propria immagine, più o meno nitidamente?

E se si guardasse dall'altra parte forse si vedrebbe lo stesso paesaggio parzialmente riflesso. Questo fenomeno, troppo spesso osservato con indifferenza, è in realtà uno straordinario esempio alla portata di chiunque per entrare direttamente in contatto con il mondo quantistico.

La luce, si sa, è costituita di fotoni. Questi ultimi attraversano il vetro per mostrare il paesaggio; ma non è detto. Il mondo quantistico delle particelle elementari, come appunto i fotoni, non è un mondo di certezze ma di possibilità. Il fotone che colpisce il vetro può attraversarlo, ma può anche esserne riflesso: il fotone ha una certa probabilità di passare o meno attraverso il vetro. Il fenomeno è ancora più sottile e sfuggente per la logica aristotelica cui si è abituati: il fotone *passa e non passa*. È questo il senso di uno dei pilastri concettuali della meccanica quantistica: il *principio di sovrapposizione*. Se un'entità quantistica può assumere due valori o essere in due stati sarà in una sovrapposizione dei due, con una probabilità non nulla di essere nell'uno e nell'altro. In una sovrapposizione, a differenza di un miscuglio, non si può dire che un'entità si trovi realmente in uno stato o in un altro che però non si conoscono; la sovrapposizione contiene, invece, tutti i possibili casi, ma non equivale ad alcuno di essi.

A ogni particella si può poi associare un'onda, e ogni onda è una manifestazione di una particella. Max Born intuì per primo la natura di questa relazione: l'onda associata a una particella è un'onda di "probabilità", nel senso che indica quale sarà l'evoluzione possibile per quella particella. Lo stato di una particella non è più quello classico (posizione nel-

lo spazio e nel tempo e velocità). Lo stato di una particella è dato dalla sovrapposizione di tutti i suoi possibili stati futuri, ciascuno "pesato" con una probabilità. Si è lungamente riflettuto sul significato di una simile concettualizzazione: che cosa significa affermare che lo stato di una particella è un insieme di possibili stati? Il fotone che incide sul vetro passa o non passa? Un elettrone è qui o là? Nel mondo quantistico l'elettrone è sia qui sia là, ma con diverse probabilità di essere qui e là. Soltanto dopo una misura si può dire se sia qui. Tuttavia se si cerca di misurare una quantità di un sistema si fa collassare la funzione d'onda del sistema, e si ottiene un valore preciso per una quantità che prima era semplicemente una delle tante possibilità. È proprio l'osservazione che provoca la "scelta" di quel particolare valore fra tutti quelli possibili. Cosa causa il collasso di una funzione d'onda? La risposta a questa domanda è molto complessa ma nell'economia di questo articolo ci si può limitare, in maniera molto approssimativa, a rispondere che è l'*interferenza* tra il mondo quantistico e il mondo macroscopico.
Se, poi, a seguito di un certo fenomeno fisico, nascono due particelle esse saranno correlate tra loro come due gemelli omozigoti. In linea di principio, non si sa quali siano certe caratteristiche di una particella fino a quando non vengono misurate, e ciò vale ovviamente anche per l'altra. Ma se viene misurata una caratteristica di una particella immediatamente si determina l'analoga caratteristica dell'altra, dovunque essa si trovi nell'universo.
Detto così potrebbe sembrare quasi ovvio. Ma il fenomeno è molto più sottile. Occorre riflettere sul fatto che ciascuna particella è costantemente in una sovrapposizione di stati. Si potrebbe immaginare la situazione seguente. Due gemelli prima di uscire di casa si mettono un paio di calze; nel cassetto ce ne sono due paia: uno rosso e uno blu. Se si incontra un gemello e non si guarda sotto i suoi pantaloni le calze possono essere sia rosse sia blu: ma se si guarda sotto i pantaloni esse avranno un preciso colore e, quindi, si conoscerà anche il colore delle calze dell'altro gemello. Il mondo quantistico però non funziona in questo modo. Ciascun gemello sembra indossare entrambe le paia di calze e solo quando si va a verificare si costringe il gemello a sceglierne un paio: ciò immediatamente determina il colore delle calze dell'altro gemello. È il principio dell'*entanglement*, ossia della correlazione quantistica.
Si vedrà più avanti che *sovrapposizione, entanglement e interferenza* sono i tre pilastri alla base del funzionamento del computer quantistico.

4. PERCHÉ FEYNMAN AVEVA RAGIONE

Si immagini, allora, di avere una decina di particelle dotate individualmente di *spin*. Lo spin è una tipica grandezza quantistica che rappresenta una particolare caratteristica delle particelle elementari. Queste ultime potrebbero essere immaginate, in maniera quanto mai semplificata, come trottoline che ruotano intorno a se stesse. Tale rotazione può avvenire in senso orario o antiorario e può, quindi, rappresentare un bit; per esempio 0 per spin orario e 1 per spin antiorario. Si cerchi allora di contare i possibili stati in cui possono trovarsi le particelle stesse. Se fossero tutte nello stato di spin orario si avrebbero 10 bit a zero, se invece fossero tutte con spin antiorario si avrebbero 10 bit tutti a 1. In realtà, sono possibili anche tutte le combinazioni intermedie e, quindi, si hanno complessivamente 1024 possibili combinazioni di bit, ossia 2^{10}. Se le particelle fossero 20 si avrebbe 2^{20}, ossia oltre un milione di combinazioni; e se fossero 40 si avrebbe 2^{40}, ossia mille miliardi di combinazioni.
Le cose sono però ben più complicate. Infatti, la nostra semplice analisi ha considerato solo la possibilità che le particelle possano essere dotate di spin orario o antiorario.
Invece, secondo la meccanica quantistica lo spin può essere in uno stato di sovrapposizione, ossia in una qualsivoglia combinazione delle due direzioni, per esempio il 30% orario e il 70% antiorario. L'intero sistema è, quindi, un aggregato incredibilmente complesso di sovrapposizioni di tutte le possibili combinazioni di spin di ciascuna particella. L'evoluzione di un simile sistema, descritta da una complessa funzione d'onda probabilistica, è un problema non trattabile neppure oggi da qualsivoglia supercomputer.

Ecco allora l'idea di Feynman.
Cosa accadrebbe se la simulazione del sistema non fosse condotta su di un computer classico ma su di un computer che funzionasse anch'esso secondo le leggi della meccanica quantistica? I circuiti e i bit di memoria di quest'ultimo non sarebbero vincolati a una dualità di valori 0 e 1 ma potrebbero anch'essi operare in una sovrapposizione di stati 0 e 1.
Feynman, in realtà, nel 1981, non andò molto al di là di questa intuizione. Ma nello stesso convegno un altro fisico, Paul Benioff, presentava un modello di computer quantistico basato su di un'ipotetica macchina di Turing che funzionava eseguendo una sequenza di operazioni effettuate secondo le leggi della meccanica quantistica [1].
Il modello di Benioff era anch'esso molto approssimativo nei dettagli costruttivi, ma era sufficientemente solido dal punto di vista concettuale, tanto che tre anni dopo lo stesso Feynman ne presentava una propria versione semplificata e migliorata (senza peraltro citare il contributo di Benioff). Comunque anche il nuovo modello di Feynman restava ancora un astratto strumento concettuale. La differenza tra i modelli di Benioff/Feynman e un reale computer quantistico era abbastanza simile a quella che c'è tra una macchina di Turing e un personal computer.
La vera svolta, ancora concettuale, doveva avvenire solo un anno dopo con la pubblicazione di un nuovo articolo, di David Deutsch [3].
Come il computer di Benioff anche quello di Deutsch era basato su di una macchina di Turing: il programma era memorizzato insieme ai dati sul nastro. Il processore avrebbe eseguito il programma utilizzando operazioni di tipo quantistico. Tali operazioni, come in un computer classico, avrebbero agito sui bit del nastro. Poco veniva detto su come tale computer potesse essere realizzato praticamente, perché, in realtà, l'obiettivo era quello di esaminare la struttura concettuale di una simile macchina. Il grande passo avanti era costituito dalla dimostrazione dell'universalità di un simile modello. Deutsch mostrava come fosse possibile costruire una struttura logica in grado di eseguire qualunque tipo di calcolo. Il principio base di ogni computer classico è che ogni funzione che può essere calcolabile può essere calcolata da una macchina di Turing. Ma ora, secondo Deutsch, esisteva un computer universale in grado di effettuare qualunque tipo di calcolo che qualsivoglia entità fisica fosse in grado di attuare. La computazione non era più un ramo della sola matematica ma diventava una manifestazione delle leggi della fisica.
E poiché il mondo quantistico è intrinsecamente parallelo è possibile fare di conto in maniera completamente diversa rispetto alle tecniche tradizionali.
Si immagini, diceva Deutsch, di avere una funzione in grado di predire l'andamento del mercato azionario. Si immagini anche che occorra valutare tale funzione per soli due valori, 0 e 1, ossia $f(0)$ e $f(1)$. La funzione può, comunque, essere molto complicata e, quindi, si può anche immaginare che a un computer classico occorrano 24 h per calcolare la funzione stessa: quindi 48 h per verificare se $f(0) = f(1)$. Se però, utilizzando il parallelismo quantistico, fosse possibile calcolare contemporaneamente $f(0)$ e $f(1)$ si potrebbe sapere se $f(0) = f(1)$ in 24 h e, quindi, in tempo utile per investire con successo.

5. UNA NUOVA STRUTTURA FISICA

Si immagini di avere un atomo che abbia un solo elettrone nell'ultima orbita occupata. Questo elettrone può essere spostato, ossia "eccitato", in un'orbita più esterna illuminandolo con una luce di una determinata frequenza e durata.
L'elettrone fa così un salto quantico in uno stato di energia più elevata. Se tale stato è sufficientemente stabile lo si potrà utilizzare, insieme allo stato di energia più basso, per rappresentare rispettivamente i numeri 0 e 1.
Se un atomo "eccitato" viene colpito da un ulteriore impulso di luce, simile al precedente, l'elettrone ritorna nello stato di energia più bassa rilasciando un fotone.
Ma cosa accade se la durata del primo impulso di luce dura la metà del tempo necessario per commutare lo stato dell'elettrone? La risposta è sorprendente per la logica cui si è abituati: l'elettrone si troverà simultaneamente in entrambe le orbite. L'elettrone sarà allora in una "sovrapposizione" dei due stati, fondamentale ed eccitato.

Utilizzando in tal modo un atomo si può memorizzare un'unità di informazione, ossia un bit. Nel 1995, Ben Schumacher coniò il termine "qubit" (*quantum bit*) per denotare tale entità. Un bit digitale se viene misurato può essere solo 0 o 1, con certezza, mentre un bit analogico può assumere qualsivoglia valore tra 0 e 1. Un qubit è, invece, una "sovrapposizione" di 0 e 1 e può essere definito dalla notazione matematica a $|0> + b|1>$, intendendo con ciò che se misurato esso potrà valere 0 con probabilità $|a|^2$ e 1 con probabilità $|b|^2$, essendo *a* e *b* numeri complessi.
Non si vuole, per semplicità, approfondire la natura matematica degli stati rappresentati dal simbolo |>, ma è bene comunque ricordare che tale simbolo sta a rappresentare un vettore, per sua natura orientato. Lo stato $|1> - |0>$ è diverso dallo stato $|1> + |0>$, come si può vedere dalla figura 1. Lo stato di un qubit $a|0> + b|1>$ può essere rappresentato da un vettore che raggiunge un qualunque punto di una circonferenza. Nel disegno *a* e *b* sono numeri reali; se fossero numeri complessi (come in realtà sono) il disegno dovrebbe essere in tre dimensioni, ossia una sfera.
Da qui in avanti, per semplicità, non si useranno più le ampiezze di probabilità *a* e *b* assumendole eguali a $1/\sqrt{2}$ e ritenendo, quindi, i due stati $|0>$ e $|1>$ equiprobabili. Se due qubit vengono indipendentemente posti nella sovrapposizione $|0> + |1>$ si scriverà $(|0> + |1>)(|0> + |1>)$ ossia $|00> + |01> + |10> + |11>$. Si vede così che due qubit possono rappresentare "contemporaneamente" 4 valori, mentre 3 qubit ne rappresentano 8, $|00>$, $|001>$, ...$|111>$.
Ma come si possono modificare i valori memorizzati? In altri termini che tipo di operatori si possono utilizzare per modificare il contenuto di uno o più qubit? La domanda è, in realtà, ancora più generale.
In ambiente quantistico si è già visto come sia possibile invertire il contenuto di un qubit. L'impulso di luce di durata opportuna equivale a tutti gli effetti a un operatore NOT. Ma si è anche visto che illuminando l'atomo per metà tempo (rispetto a quello necessario per commutare lo stato dell'elettrone) si ottiene una sovrapposizione di stati. Detto in altri termini, se il bit era $|0>$ esso diventa $|0> + |1>$. Se a questo punto

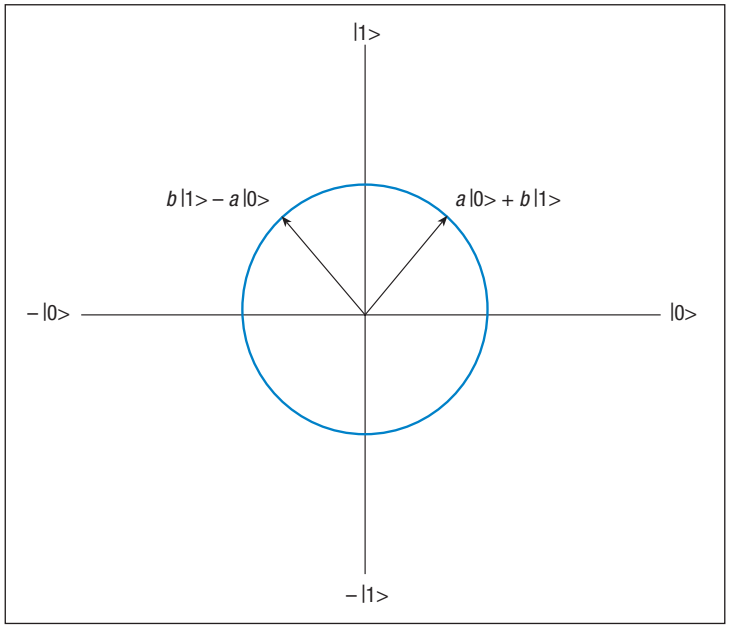


FIGURA 1

Lo stato di un qubit a $|0> + b|1>$ *può essere rappresentato da un vettore che raggiunge qualsivoglia punto di una circonferenza se le ampiezze a e b sono numeri reali e se la somma dei loro quadrati è uguale a* 1

riceverà un uguale impulso di luce passerà allo stato $|1>$. Un impulso completo equivale, quindi, all'operatore NOT. Ma uno di durata metà a cosa equivale? All'operatore radice quadrata di NOT. Infatti, due impulsi di questo tipo danno luogo a un:

$$\text{NOT} = \sqrt{\text{NOT}} \times \sqrt{\text{NOT}}$$

Oltre all'operatore $\sqrt{\text{NOT}}$ esistono in meccanica quantistica altri tipi di operatori, che possono essere applicati alle grandezze $|0>$ e $|1>$, e alle loro combinazioni $|0> + |1>$, $|0> - |1>$, .., per trasformarle opportunamente.
Uno di questi, che per semplicità non verrà esaminato matematicamente, è la cosiddetta trasformazione di Hadamard. Nell'attuale letteratura, l'operatore $\sqrt{\text{NOT}}$ viene indicato con *X* e l'operatore di Hadamard con *H*.
L'effetto di *X*, come si è visto, è $X\ |0> \tau \neq (|0> + |1>)$; e $X\ (|0> + |1> \tau \neq |1>$; mentre $X\ |1> \tau (|1> - |0>)$; $X\ (|1> - |0>) | \tau \neq \neq - |0>$.
L'effetto di *H* è $H\ |0> \neq \tau \neq (|0> + |1>)$; e $H\ (|0> + |1>)\ \tau \neq |0>$; mentre $H\ |1> \neq \tau \neq (|0> - |1>)$ e $H\ (|0> - |1>)\ \tau \neq \neq |1>$.
Ora si è finalmente in grado di esaminare il circuito quantistico proposto da Deutsch co-

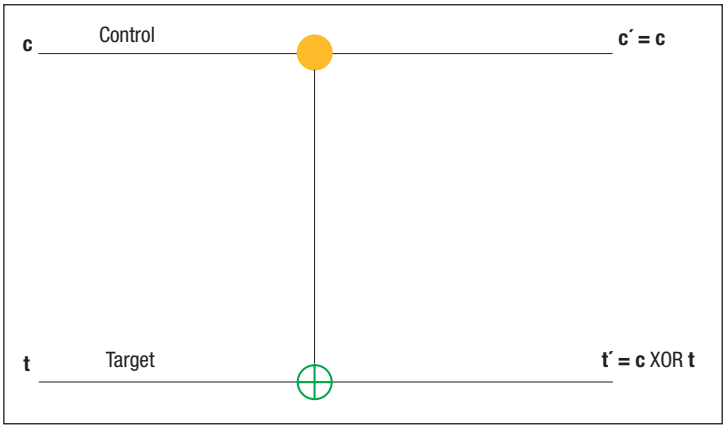


FIGURA 2
Nel circuito di OR esclusivo (XOR) si può vedere che il valore di c resta inalterato mentre il valore di t viene invertito se c è uguale a 1

me circuito universale per la costruzione di un intero computer quantistico.
Nell'articolo di Deutsch *c* è il control input, mentre *t* è il target input. Dalla figura 2 si può comprendere il significato dei due input.
Il circuito stesso prende il nome di *controlled not gate* e può essere schematizzato come segue:
Se $c = |0> + |1>$ e $t = |0>$ il risultato finale sarà $|00> + |11>$ e non $c = |0> + |1>$ e $t = |0> + |1>$.
Ciò vuol dire che se si misurerà *c* e si otterrà 0 anche *t* sarà a 0; viceversa se misurando *c* si otterrà 1 *t* sarà anch'esso a 1. Questo perché il valore 0 di *c* non fa commutare *t*, mentre il valore 1 lo fa commutare.
Ecco che finalmente entra in gioco il principio dell'entanglement visto precedentemente.
Se due qubit sono entrambi nella sovrapposizione di 0 e 1 vengono definiti entangled se il risultato della misurazione di uno di essi è sempre correlato al risultato della misura dell'altro qubit.
L'entanglement, insieme alla sovrapposizione, è la chiave di volta dell'intero funzionamento del computer quantistico. Senza l'entanglement, infatti, come si potrebbero correlare i risultati ottenuti con i valori in ingresso? Per comprendere più facilmente questo fondamentale concetto si può ricorrere a una semplice metafora. Si immagini di avere un insieme di domande, quali per esempio la moltiplicazione di diverse coppie di numeri molto grandi, e di distribuire tali moltiplicazioni tra più persone. Ciascuna di queste trascriverà il proprio risultato su di un foglietto che porrà in una scatola. La scatola in questo esempio rappresenta il registro di qubit in uscita. Estrarre di volta in volta dalla scatola un risultato equivale a far "collassare" il registro dei qubit a un valore preciso dopo una misura. Ma il risultato ottenuto a quale domanda, ossia a quale moltiplicazione, corrisponde se sul foglietto è scritto solo il risultato? Nel computer quantistico è proprio il meccanismo dell'entanglement che consente di associare i singoli risultati alle rispettive domande. Allo stesso tempo il principio dell'interferenza fa in modo che se viene estratto un foglietto con un risultato vengono contemporaneamente distrutti tutti gli altri.
Con i tre fondamentali meccanismi della sovrapposizione, dell'entanglement e dell'interferenza è possibile costruire un'intera logica circuitale quantistica, almeno a livello concettuale, con la quale si può mettere in luce la straordinaria capacità di calcolo di un computer quantistico.
Deutsch nel suo articolo si proponeva di calcolare in tempo utile una particolare funzione per due soli valori $f(0)$ e $f(1)$ per verificare se $f(0) = f(1)$.
Nel riquadro viene riportata in maniera semplificata una dimostrazione data da Artur Ekert.
A questo punto sorgono quasi spontaneamente due domande:
- quali classi di problemi può affrontare un computer quantistico ?
- come può essere fisicamente costruito un computer quantistico?

6. QUALI CLASSI DI PROBLEMI PUÒ AFFRONTARE IL COMPUTER QUANTISTICO

Da quanto detto finora, si può già intuire che il computer quantistico non è il computer tipico per navigare in Internet o per inviare la posta elettronica. A cosa può servire allora?
Si è già osservato che, secondo il dogma fondamentale della computazione, nell'ambito del calcolo non esiste alcuna macchina concettualmente più potente della macchina di Turing.
Dal punto dei vista della computabilità un algoritmo è caratterizzato anche dal numero di operazioni e dalla quantità di memoria richieste per un input di dimensioni *x*. Questa caratterizzazione dell'algoritmo determina quella che viene definita la complessità del-

l'algoritmo stesso. Tra i problemi considerati complessi ci sono certamente quelli che crescono come la potenza di un numero. La funzione $y = x^2$ cresce molto rapidamente. Per valori di x molto elevati occorre eseguire moltiplicazioni sempre più laboriose.
Se la potenza cresce ulteriormente, per esempio $y = x^4$ o $y = x^5$ la difficoltà aumenta ancora. Simili problemi, definiti polinomiali, sono oggi alla portata dei computer classici. Ma esistono problemi che crescono molto più rapidamente di quelli polinomiali. I problemi di tipo esponenziale aumentano di complessità più rapidamente di quelli polinomiali: e^x cresce molto più rapidamente di x^3, x^5, x^7,.. per valori crescenti di x.
La distinzione oggi più utilizzata è quella tra problemi che possono essere risolti in modo polinomiale (*P*), e considerati *trattabili*, e quelli che, invece, non possono essere risolti in modo polinomiale, e che vengono generalmente considerati *intrattabili*, e che possono a loro volta far parte di classi diverse. Tra queste ultime la prima è la cosiddetta classe NP. Semplificando, i problemi di tipo NP non possono, in generale, essere risolti da algoritmi deterministici di tipo polinomiale, e sono, quindi, in linea di principio intrattabili. NP, infatti, sta a significare *non-deterministic polynomial time*. Non deterministico significa che a un dato passo dell'algoritmo non si può stabilire in maniera univoca quale possa essere il passo successivo. Un pò come nel gioco degli scacchi: data una mossa dell'avversario non c'è al momento un algoritmo che possa, a priori, determinare deterministicamente, in tempo ragionevole, quale debba essere la mossa successiva.
Esistono ulteriori problemi, definiti NP-completi, che fanno parte di NP ma sono raggruppabili in gruppi tali che se si risolve un problema in tempo polinomiale allora tutto il gruppo è solubile.
Tra questi problemi rientra il celebre problema del commesso viaggiatore che debba visitare un certo numero di città, ciascuna una volta sola e senza tornare mai indietro, attraverso un percorso che abbia la lunghezza minima.
Per riassumere quanto detto finora si può dire che gli algoritmi possono essere classificati come:

- P: polinomiali: (per esempio, la moltiplicazione)
- NP: polinomiali non deterministici: (per esempio, la fattorizzazione)
- NP-completi: sottoclassi di NP tali che se uno della classe è trattabile lo sono tutti: (per esempio, il problema del commesso viaggiatore)

Sebbene le classi di tipo NP non siano le più complesse esse contengono comunque alcuni tra i problemi, al momento, di maggior interesse. Tra questi il problema della fattorizzazione di un numero è intimamente connesso con la possibilità di decrittare un sistema di crittografia, come per esempio il sistema RSA129 che utilizza chiavi costituite da 129 cifre. È stato valutato che, se per fattorizzare un numero di 129 cifre nel 1994 sono stati necessari 5000 MIPS-anni (MIPS: milioni di istruzioni al secondo), per fattorizzarne uno di 200 cifre occorrerebbero quasi 3 miliardi di MIPS-anni.
Ed è proprio nell'area di simili problemi che entra in gioco il computer quantistico.
Si è recentemente scoperto, per esempio, che proprio la fattorizzazione in fattori primi di numeri molto grandi può essere affrontata con successo da un ideale computer quantistico, che usi quindi sovrapposizione ed entanglement, con un metodo, detto algoritmo di Shor, ideato da Peter Shor nel 1994[1]. L'algoritmo di Shor è matematicamente abbastanza semplice e richiede un hardware quantistico abbastanza modesto, almeno per piccoli numeri.
Ed è interessante riflettere su quanto ha detto proprio Deutsch in merito. "... *vorrei lanciare una sfida a coloro che sono ancora attaccati alla concezione classica: spiegare come funziona l'algoritmo di Shor. Non si tratta soltanto di dimostrare che è valido – a tal fine basta semplicemente risolvere alcune equazioni – ma di fornire una vera spiegazione. Quando l'algoritmo di Shor fattorizza un numero utilizzando una quantità di risorse computazionali pari a circa* 10^{500} *volte quelle apparentemente presenti, dov'è il numero fattorizzato? Il numero degli atomi presenti in tutto l'universo visibile è all'incirca* 10^{80}, *un numero estremamen-*

[1] Bone S, Castro M: *A Brief History of Quantum Computing*. http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3

te piccolo in confronto a 10^{500}. *Quindi, se l'universo visibile esaurisse la realtà fisica in tutta la sua estensione, questa non conterebbe che una piccola frazione delle risorse necessarie per fattorizzare un numero tanto grande.Chi l'ha fattorizzato allora? Come, e dove, è stata effettuata la computazione*?.." [3]
Senza voler ulteriormente approfondire il tema si può osservare che il computer quantistico potrebbe, forse, essere in grado di trasformare i problemi di tipo NP in problemi di tipo P. Se così fosse ci si troverebbe di fronte a una scoperta straordinaria.
Ma come sarà possibile costruire fisicamente un computer quantistico?

7. COME COSTRUIRE UN COMPUTER QUANTISTICO

Nel 1994, si tenne a Boulder (Colorado), nel laboratorio del *National Institute of Standards&Technology* (NIST) un convegno internazionale sulla fisica atomica.
Nel corso del convegno Artur Ekert, che aveva più volte collaborato con Deutsch, sostenne che era giunto il momento di lanciare la rivoluzione del computer quantistico. Quest'ultimo avrebbe avuto bisogno di molteplici circuiti quantistici in grado di operare in sinergia. Perché non cominciare allora a costruire almeno un "controlled NOT quantum gate"?
Si è visto prima come un singolo atomo che venga eccitato o meno possa funzionare concettualmente come un NOT (o anche come un $\sqrt{\text{NOT}}$).
C'è da aggiungere che già da molti anni si era riusciti, grazie soprattutto alle ricerche di Hans Dehmelt (vincitore per questo del premio Nobel per la Fisica nel 1989) a isolare in una camera a vuoto un singolo ione, ossia un atomo con una piccola carica elettrica, dovuta per esempio al fatto di aver "strappato" all'atomo un elettrone.
Utilizzando con grande maestria campi elettrici e magnetici era possibile isolare un unico ione e muoverlo all'interno di un opportuno dispositivo in grado di mantenere uno stato di vuoto pressoché assoluto, quasi come se fosse una mosca all'interno di una bottiglia.
Bombardando lo ione da ogni direzione con impulsi laser lo si può sospendere praticamente in un punto. I ricercatori Cirac e Zoller (dell'università di Innsbruck) intuirono che un simile ione potesse funzionare come un *quantum gate*[2]. Si immagini che lo ione abbia un solo elettrone nell'orbita più esterna. Se tale elettrone è nello stato energetico più basso si avrà uno 0, se sarà in uno stato energetico più alto si avrà un 1.
Basterà un opportuno impulso laser per far commutare lo ione da uno stato a un altro.
Si immagini ora di costruire, come se fosse un filo di perle, una catena di ioni adiacenti; catena mantenuta stabile da opportuni campi elettromagnetici. Le singole cariche degli ioni tenderanno a respingerli reciprocamente mentre i campi elettromagnetici tenderanno a mantenerli raggruppati.
Si potrebbe immaginare il tutto come un insieme di minipendoli affiancati l'uno all'altro (Figura 3).
È bene riflettere su di un aspetto importante. Il movimento orizzontale dei minipendoli non è simile a quello di pendoli reali perché a livello atomico il movimento dei singoli ioni è quantizzato anch'esso. Ciò vuol dire che i minipendoli non potranno vibrare con qualunque tipo di frequenza ma solo nell'ambito di precise frequenze intervallate l'una dall'altra in maniera discreta, ossia non continua.
Le conseguenze sono molto interessanti. In-

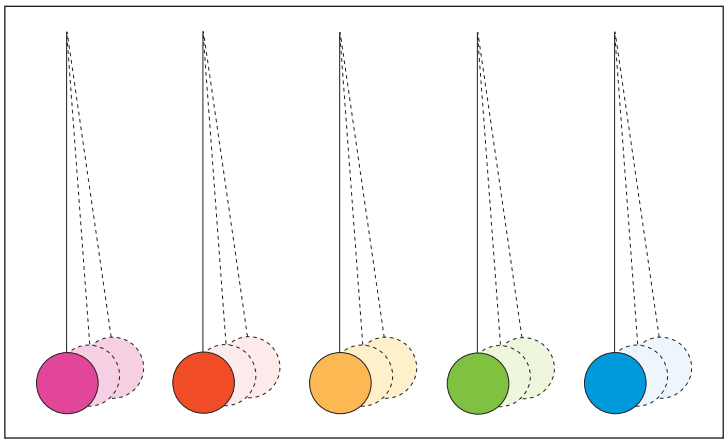


FIGURA 3
Un gruppo di ioni che oscillano: come pendoli essi possono oscillare all'unisono

[2] Cirac J, e al.: Quantum gates and Quantum Computation with Trapped Ions. (cap 4.3) in Bouwmeester D, Ekert A, An Zeilinger: The Physics of Quantum Computation [2].

fatti, tutto ciò che può assumere due stati ben distinti tra loro può essere considerato un bit - in questo caso un qubit - di informazione.
Il risultato complessivo di Cirac e Zoller è che diventa possibile costruire un registro quantistico con due tipi distinti di informazioni memorizzabili: il livello energetico dell'elettrone e la vibrazione orizzontale dello ione. Ciò che Cirac e Zoller avevano individuato era un metodo per ottenere operazioni quantistiche attraverso le interazioni dei qubit.
Si supponga, per esempio, che uno degli ioni sia in uno stato eccitato (1) e che stia vibrando con la frequenza base (0). Il dispositivo così realizzato è un miniregistro quantistico che contiene l'informazione 10. Con un opportuno impulso laser l'elettrone può essere fatto ritornare nello stato base mentre allo stesso tempo lo ione può essere fatto vibrare con frequenza 1. Il risultato sarà che 10 diventerà 01. Utilizzando opportunamente ulteriori impulsi il bit 1 può essere fatto viaggiare da ione a ione come se la catena di ioni fosse un vero e proprio bus di trasferimento.
Ma la cosa più importante è che il modo con il quale uno ione risponde a un impulso laser può dipendere dalla vibrazione delle catene di ioni.
Cirac e Zoller mostrarono come lo stato 01 potesse diventare 00, 10, 11. In conclusione, furono in grado di costruire un "controlled NOT gate".
Il dispositivo di Cirac e Zoller era basato su di una catena di ioni affiancati. Ma già nel 1995 due ricercatori del NIST, David Wineland e Christopher Monroe, riuscirono a costruire il primo vero "two-bit controlled NOT gate" utilizzando un solo ione di berillio (Be+)[3].
Isolarono uno ione di Be+ con un solo elettrone nell'orbita più esterna e, invece di utilizzare l'eccitazione di tale elettrone in un'orbita più esterna, sfruttarono i livelli di energia "iperfine" che dipendono dall'allineamento tra lo spin dell'elettrone e quello del nucleo dello ione.
Usando i due stati di energia iperfine (spin allineati o disallineati) e due stati dipendenti dai modi di vibrazione dello ione ottennero due qubit correlati.

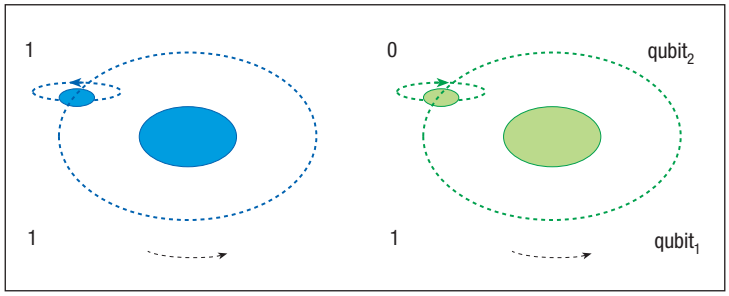


FIGURA 4
Un esempio di controlled NOT gate

Applicando opportuni impulsi laser furono in grado di dimostrare il funzionamento dello ione come "controlled NOT gate" (Figura 4).
Tra i due esperimenti di Cirac-Zoller e Wineland-Monroe ci sono però sostanziali differenze. Cirac e Zoller furono in grado di mantenere lo stato di sovrapposizione quantistica per almeno un decimo di secondo, ossia un tempo molto lungo su scala atomica.
Il gate di Wineland-Monroe era almeno cento volte meno stabile. Ma il problema era, in realtà, un altro. Per effettuare realmente dei calcoli occorre poter operare con moltissimi ioni. Wineland e Monroe sono stati in grado di arrivare a far cooperare 4 ioni, ma per eseguire i calcoli necessari alla scomposizione in fattori di un numero di molte cifre occorrono migliaia di qubit.
Il limite di *scaling*, ossia di capacità di crescita dimensionale, della tecnologia *ìon-trap* sembra in questo momento intorno ai 50 qubit. E soprattutto non si sa se un programma quantistico possa essere eseguito per il tempo necessario senza incorrere nel fenomeno della *decoerenza*. Uno dei problemi più complessi da risolvere è quello di impedire che l'interferenza dei vari calcoli si rifletta sul mondo macroscopico. Infatti, se un gruppo di atomi o di molecole è sottoposto a un fenomeno di interferenza e interagisce al tempo stesso con l'ambiente macroscopico non è più possibile rilevare l'interferenza con misure che riguardano solo gli atomi del gruppo originario che così cessa di effettuare un'attività di calcolo quantistico utile.
Una nuova interessante soluzione è sembrata arrivare nel 1997 con una tecnologia denominata NMR (*Risonanza Nucleare Magnetica*).
L'idea, in questo caso, è di utilizzare non ato-

[3] Monroe C, et al.: *Demonstration of a Fundamental Quantum Logic Gate* :http://qubit.nist.gov/

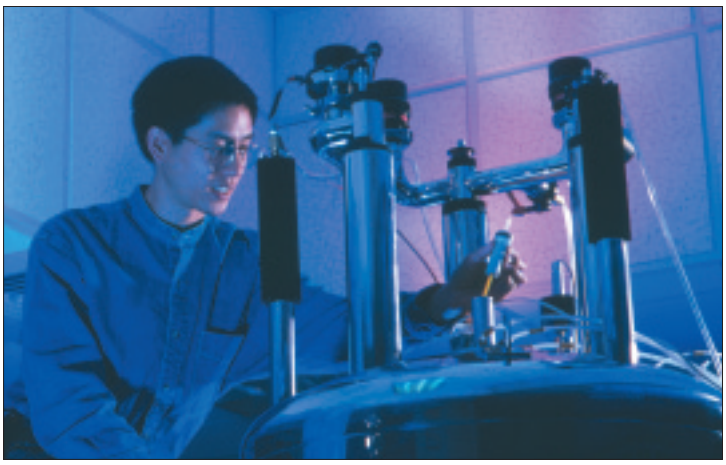


FIGURA 5
Isaac Chuang carica le molecole a 7-qubit nel dispositivo a risonanza nucleare magnetica

mi ma intere molecole. Una molecola di per sé è già una catena di atomi. Ma gli elettroni degli atomi non sono le sole entità che possono essere utilizzate come qubit. La risonanza nucleare magnetica dipende dal fatto che anche i nuclei possono essere utilizzati come gli elettroni. I nuclei sono aggregati di protoni e neutroni, ambedue dotati di spin. Tali spin si bilanciano più o meno tra loro. Ma se un nucleo è costituito di un numero dispari di protoni e neutroni potrà restare uno spin netto a 0 o a 1. Si è scoperto che tali spin possono essere usati anch'essi come qubit. Immersi in un campo magnetico i vari atomi di un nucleo (idrogeno, carbonio,..) rispondono ciascuno a un preciso impulso laser. Anche lo stesso atomo potrà rispondere in maniera diversa a seconda della sua posizione nella molecola. Per poter creare un circuito quantistico i nuclei devono anche essere in grado di interagire l'uno con l'altro attraverso i propri campi magnetici. Devono essere correlati (*entangled*). Che un nucleo possa commutare, o meno, il proprio stato a fronte di un impulso esterno può, quindi, dipendere dallo stato dei suoi vicini. Poiché gli atomi della molecola emettono anch'essi deboli segnali questi possono essere rilevati dall'esterno. Si immagini di avere una sostanza composta di molecole costituite di quattro atomi (*a*, *b*, *c*, *d*) che rappresentano quattro qubit. Tale sostanza viene diluita in un liquido che conterrà miliardi di trilioni di queste molecole. All'inizio i nuclei delle molecole punteranno in ogni direzione: un vero e proprio brodo di spin. Un intenso campo magnetico può però allinearne una piccolissima frazione che è pur sempre costituita di innumerevoli miliardi di molecole i cui nuclei saranno tutti allineati allo stesso modo, ossia 1111. Questo allineamento provoca un segnale complessivo che può essere letto da un operatore su di uno schermo. A questo punto, l'operatore può scegliere uno degli atomi - per esempio il secondo - e inviare un impulso che modificherà lo stato di tutti i secondi atomi di tali molecole. Ancora una volta, il segnale prodotto da tali molecole verrà letto sullo schermo come 1011.

La molecola può essere stata scelta in base al fatto, per esempio, che l'atomo *b* commuta solo se l'atomo *d* è a 1. Altrimenti l'impulso verrà ignorato.

Isaac Chuang (Figura 5), Gregory Breyta, Mark Sherwood e Costantino Yannoni, dei laboratori IBM di Almaden, insieme a Lieven M.K. Vandersypen e Matthias Steffen, della Stanford University, hanno presentato, nel 2001, i risultati di un loro esperimento relativo alla fattorizzazione del numero 15 con l'algoritmo di Shor[4]. Sono stati in grado di disegnare e costruire una nuova molecola con sette spin nucleari – cinque di fluoro e due di carbonio – in grado di interagire come qubit e di essere programmati per mezzo di una radiofrequenza. Il loro contenuto poteva essere quindi letto per mezzo di dispositivi tipici della tecnologia NMR.

Il calcolo è stato eseguito da 10^{18} molecole. Sebbene il calcolo possa sembrare banale la gestione contemporanea di 7 qubit costituisce alla data il calcolo quantistico più complesso finora eseguito.

Ma si ritiene che non sarà facile spingersi molto più oltre con la tecnologia NMR. Ogni volta che un nucleo viene aggiunto alla catena di molecole la voce elettromagnetica di ciascun qubit diventa più debole e difficile da sentire. Probabilmente non è possibile andare al di là di 50 qubit.

Sono state però sperimentate anche altre tecniche, come i cosiddetti *quantum dot* che sono piccole isole di materiale semiconduttore all'interno di un chip. Un tipico quantum-dot può essere costituito da poche centinaia

[4] Lieven M, e al.: *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*. Nature 414, pp. 883-887 (2001).

di atomi. Applicando opportuni campi elettrici attorno a queste isole è possibile controllare il numero di elettroni mobili all'interno delle isole stesse.
Si può fare in modo di intrappolare, all'interno di un'isola, un unico elettrone. Intrappolato in tal modo l'elettrone può occupare solo stati discreti (quantizzati) di energia. Ogni elettrone può, quindi, essere usato come un qubit. Le tecniche costruttive dei quantum dot sono diverse da quelle della fotolitografia tradizionale ma sono comunque accessibili, e recenti sviluppi hanno mostrato che è possibile costruire un notevole numero di quantum dot sullo stesso chip.
I qubit possono interagire attraverso fenomeni elettromagnetici o di *tunneling* quantistico, ed eseguire quindi operazioni logiche. Poiché gli elettroni possono avere lo spin orientato verso l'alto o verso il basso tale direzione può essere utilizzata come informazione di on-off, ossia ciascun dot può essere a uno o a zero a seconda dello stato di spin. Recentemente[5] alcuni ricercatori sono stati in grado di correlare due quantum dot, controllare quanti elettroni erano in ciascun dot e determinare lo stato di spin in ogni dot. A differenza di un computer classico nel quale la corrente circola attraverso i circuiti per trasferire le informazioni, nei computer basati su quantum dot il flusso delle informazioni è basato sulla manipolazione degli spin degli elettroni confinati nei dot.
Molti ritengono che di tutte le tecnologie quantistiche quella dei quantum dot sia la più promettente e, soprattutto, quella che ha la maggior capacità di *scalability*, fino a 1000 qubit e oltre.
Purtroppo il tempo di decoerenza è molto breve – dell'ordine del milionesimo di secondo – e i chip stessi per operare devono essere mantenuti a temperature prossime allo zero assoluto. Ma qualunque tecnologia dovesse affermarsi dovrà comunque risolvere il problema degli errori che possono nascere per qualunque disturbo dal mondo esterno il sistema quantistico possa avvertire. Come trattare tali errori è materia di ulteriore analisi che esula, tuttavia, dalle finalità di questo articolo.

8. QUALI PROSPETTIVE

Non è possibile al momento attuale formulare previsioni sull'effettiva capacità tecnica di costruire un computer quantistico in grado, per esempio, di scomporre in fattori primi un numero di almeno 10 cifre. Ci sono almeno tre tipi di problemi che occorre risolvere.
Innanzitutto, il mantenimento dello stato di sovrapposizione quantistica dei vari elementi, e quindi un effettivo isolamento dei circuiti quantistici dal mondo macroscopico che li circonda.
In secondo luogo, la gestione degli errori che comunque si manifestano in un complesso circuitale così delicato.
Infine, la sapienza costruttiva necessaria per realizzare le funzioni di calcolo che attraverso sovrapposizione, entanglement e interferenza consentono di creare risposte dalle domande e di correlare le prime alle seconde.
La strada da percorrere è enormemente complessa e non è nemmeno certo che sia realmente percorribile. Ma anche se alla fine il computer quantistico si rivelasse grande come un edificio e richiedesse centinaia di specialisti per essere programmato e gestito, e costasse centinaia di milioni di euro, o ancor più, esso potrebbe rivelarsi un formidabile strumento di calcolo.
Dal punto di vista strategico o economico potrebbe consentire di decifrare qualunque chiave crittografica o di investigare in tempi brevissimi qualunque archivio.
Ma è soprattutto dal punto di vista conoscitivo che esso consentirebbe di entrare realmente in un mondo, quello della meccanica quantistica, che oggi appare ancora quasi incomprensibile anche se viene utilizzato per le più complesse teorie della fisica.
Anche un piccolo computer quantistico, permettendo, di manipolare concretamente fenomeni come la sovrapposizione o l'entanglement, farebbe apparire la meccanica quantistica molto meno surreale di quanto non appaia oggi.
Il computer quantistico permetterebbe, infine, di capire meglio non solo la realtà del mondo subatomico ma anche il significato più profondo di ciò che è realmente la computazione e il suo ruolo nel mondo.

[5] Jeong H, e al.: *The Kondo Effect in an Artificial Quantum Dot Molecule*. Science 21 Sept. 2001.

La dimostrazione matematica di Ekert

Viene qui riportata la spiegazione matematica (semplificata) data da Ekert per spiegare il ragionamento di Deutsch.
Nel ragionamento di Deutsch il controlled Not gate è stato lievemente modificato nel cosiddetto F-controlled NOT gate (Figura).
In questo circuito si vuole calcolare il valore di una funzione utilizzando (nel rettangolo F) operazioni quantistiche. Poiché le operazioni quantistiche devono essere reversibili l'output comparirà nella linea inferiore.
Si immagini allora che il circuito utilizzato per risolvere il problema di Deutsch sia il seguente (Figura):
Il qubit superiore (qubit$_1$) resta così intatto mentre la risposta è nel qubit inferiore (qubit$_2$). La correlazione avviene attraverso il meccanismo dell'entanglement: eseguendo una misura viene distrutto lo stato di sovrapposizione e restano solo una risposta e un domanda strettamente correlate.
Nella linea in basso (2), prima dell'operatore di Hadamard, la funzione *F* avrà creato una sovrapposizione:

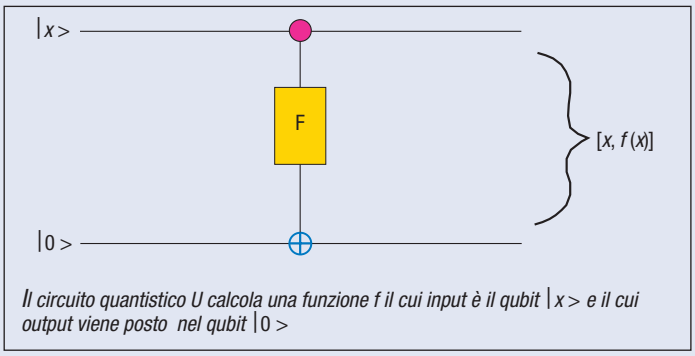
$|0, f(0)> + |1, f(1)>$

Si considerino ora i quattro casi possibili:

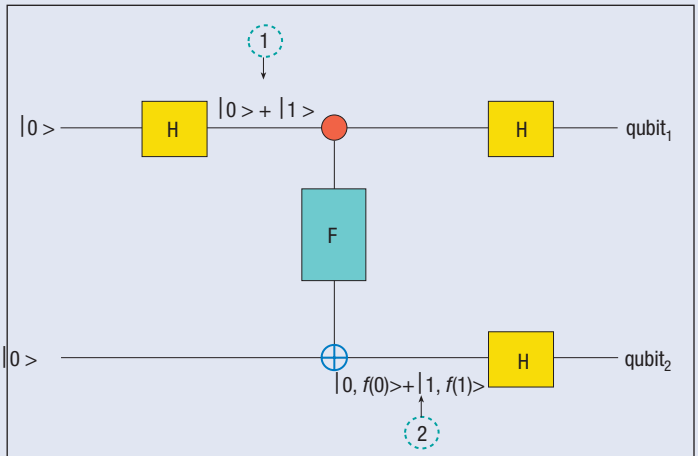
a. $f(0) = f(1) = 0$
b. $f(0) = f(1) = 1$
c. $f(0) = 0, f(1) = 1$
d. $f(0) = 1, f(1) = 0$

Nel punto (2) si avranno, quindi, le quattro seguenti possibilità:

a.	$(\|0> + \|1>)(\|0>)$	$(q_1)(q_2)$
b.	$(\|0> + \|1>)(\|1>)$	$(q_1)(q_2)$
c.	$\|0>\|0> + \|1>\|1>$	$q_1q_2 + q_1q_2$
d.	$\|0>\|1> + \|1>\|0>$	$q_1q_2 + q_1q_2$



Il circuito quantistico U calcola una funzione f il cui input è il qubit $|x>$ e il cui output viene posto nel qubit $|0>$



Le sezioni circuitali denominate H sono trasformazioni di Hadamard mentre la sezione F, quella principale, è preposta al calcolo della funzione f(x), che prende il ingresso il valore del qubit$_1$ e crea in uscita il qubit$_2$

Nei primi due casi il primo qubit è $(|0> + |1>)$ indipendentemente dal contenuto del secondo. In tal caso *F* è indifferente al valore in ingresso e quindi non c'è entanglement tra qubit$_1$ e qubit$_2$. Ma quando i valori sono differenti i bit diventano correlati (entangled) e il valore del primo qubit dipende dal valore del secondo. Nel terzo caso sono identici, nel quarto opposti.
La domandava che Deutsch poneva era: è possibile in un solo colpo sapere se $f(0)$ e $f(1)$ coincidono?
Per rispondere a questa domanda si facciano passare i qubit 1 e 2 attraverso due ulteriori operatori di Hadamard.
Nel qubit$_2$ si otterrà:

		q_1q_2 q_1q_2 q_1q_2 q_1q_2
$(\|0> + \|1>)(\|0> + \|1>)$	=	$\|0>\|0> + \|0>\|1> + \|1>\|0> + \|1>\|1>$
$(\|0> + \|1>)(\|0> - \|1>)$	=	$\|0>\|0> - \|0>\|1> + \|1>\|0> - \|1>\|1>$
$\|0>(\|0> + \|1>) + \|1>(\|0> - \|1>)$	=	$\|0>\|0> + \|0>\|1> + \|1>\|0> - \|1>\|1>$
$\|1>(\|0> + \|1>) + \|0>(\|0> - \|1>)$	=	$\|0>\|0> - \|0>\|1> + \|1>\|0> + \|1>\|1>$

Se ora si misura il qubit$_2$ si otterrà 0 o 1.
Se si otterrà 0 si potranno eliminare la seconda e la quarta colonna e si avrà:

$(|0> + |1>)|0>$
$(|0> + |1>)|0>$
$(|0> + |1>)|0>$
$(|0> + |1>)|0>$

(*segue a p. 60*)

Questo risultato non dice nulla essendo gli stati indistinguibili.
Ma se misurando il secondo qubit si ottiene 1 allora si avrà:

$$
\begin{array}{cc}
q_1 & q_2 \\
(|0>+|1>)|1> & \\
-(|0>+|1>)|1> & \\
(|0>-|1>)|1> & \\
(|1>-|0>)|1> &
\end{array}
$$

Facendo passare il qubit1 attraverso un operatore di Hadamard si otterrà:

$$
\begin{array}{l}
|0>|1> \\
-|0>|1> \\
|1>|1> \\
-|1>|1>
\end{array}
$$

Se ora si misura il qubit1 si avrà ancora 0 (primi due casi) o 1 (secondi due casi).
Ci sono, quindi, due valori ben distinti che correlano ai casi *a*, *b* (valori identici) e *c*, *d* (valori opposti).
Si può, quindi, concludere che se il qubit$_2$ vale 1 allora ha senso guardare il qubit$_1$ e se questo è uguale a 0 allora $f(1)$ è uguale a $f(0)$.
La risposta finale viene data quindi dalla lettura del qubit1 che però era stato lasciato intatto dalla funzione di calcolo *F*.
Ma ciò avviene soltanto a causa della retroazione che l'entanglement crea tra qubit$_1$ e qubit$_2$ dopo le operazioni quantistiche in *F*.
Ciò ha veramente qualcosa di magico ed è proprio qui che Deutsch ha indicato per la prima volta le straordinarie possibilità del calcolo quantistico.

Bibliografia

[1] Benioff P.: The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model. *J. Stat. Phys.*, Vol. 22, 1980, p. 563-591.

[2] Bouwmeester D., Ekert A., Zeilinger An.: *The Physics of Quantum Computation*. Springer,2000.

[3] Deutsch D.: *La trama della realtà*. Biblioteca Einaudi, 1997.

[4] Feynman R.: *Lectures on Computation*. Addison Wesley, 1996.

[5] Feynman R.: *Simulating Physics with Computers reprint*. In: Feynman Lectures on Computation. Addison Wesley, 1996.

[6] Lindley D.: *La luna di Einstein*. Longanesi 1998.

[7] Nielsen M., Chuang I.: *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[8] Penrose R.: *La mente nuova dell'imperatore*. Rizzoli, 1992.

[9] Turton R.: The Quantum Dot. Freeman, *Spectrum*, 1995.

Ernesto Hofmann è laureato in fisica presso l'Università di Roma. È entrato in IBM nel 1968 nel Servizio di Calcolo Scientifico. Nel 1973 è diventato manager del Servizio di Supporto Tecnico del Centro di Calcolo dell'IBM di Roma. Dal 1984 è Senior Consultant IBM. È autore di molteplici pubblicazioni sia di carattere tecnico sia divulgative, nonché di svariati articoli e interviste. Dal 2001, collabora con l'Università Bocconi nell'ambito di un progetto comune Bocconi-IBM.