La Computazione Quantistica

Nature isn't classical dammit, and if you want to make a simulation of Nature you better make it quantum mechanical, and by golly it's a wonderful problem because it doesn't look so easy

R. Feynman

Luigi Martina

Dipartimento di Matematica & Fisica "Ennio De Giorgi" - Università del Salento
Istituto Nazionale di Fisica Nucleare, Sez. di Lecce, Lecce, Italy

Informazione Quantistica: sembra la formula stregonesca di un qualche personaggio poco affidabile. In realtà è un *corpus* di attività scientifiche che sta ricevendo sempre più attenzione, soprattutto da parte dei governi che aspirano ad ottenere la supremazia quantistica, come chiave di quella politica. Qui cercheremo di indicare le sue basi scientifiche e le sue possibili prospettive.

Fisica e Informazione

Lo studio dei fenomeni naturali si inquadra in un modello teorico chiamato Meccanica Quantistica (MQ) che, per quanto poco intuitiva per gli esseri umani, risponde molto efficacemente alle domande relative al comportamento dei sistemi fisici. Lo fa molto meglio (in senso tecnico) della più intuitiva Meccanica Classica e, nelle sue varie estensioni, include anche il comportamento della radiazione (la luce) e delle forze fondamentali della natura ad esclusione, finora, della teoria della gravitazione. Quindi possiamo affermare con una certa confidenza che l'Universo sia in gran parte descritto dagli strumenti fornitici dalla MQ. Tra i concetti che dominano la nostra concezione del mondo moderno c'è sicuramente quello di `Informazione`. Abbiamo bisogno spasmodico di informazioni, al fine di prendere decisioni, preferire un tipo di studi ad un altro, decidere dove e come allocare del denaro ed altre risorse finanziarie e materiali, sapere se si vuole trascorrere del tempo libero o fare la guerra e via dicendo. Ma come ci giungono le informazioni? Esse devono essere catturate e trasformate opportunamente per permettere la loro trasmissione e diffusione. Per quanto l'informazione costituisca la base della valorizzazione dei beni immateriali, essa è codificata negli stati di certi sistemi fisici. La sua elaborazione, spesso intesa come calcolo, si esplica attraverso azioni di controllo ben precisi su degli opportuni sistemi materiali. Quindi essa corrisponde allo stato fisico di certi supporti materiali. Nemmeno essa quindi può sfuggire alla Fisica. In particolare, il celebre esempio del `diavoletto di Maxwell` ci ricorda che l'Informazione è associata al concetto di entropia e ad una qualche formulazione della seconda Legge della Termodinamica. In effetti, sappiamo che una quantificazione della qualità dell'Informazione trasmessa è descritta dall'`Entropia di`

`Shannon`, che ha indubbie relazioni matematiche con il concetto termodinamico introdotto da Boltzmann. Ancor più, il `Principio di Landauer` ci ricorda che in corrispondenza di un processo di cancellazione di informazione, si verifica una precisa crescita dell'entropia termodinamica ed una corrispondente dissipazione di calore nell'ambiente. In definitiva, per quanto affermato inizialmente sulla natura quantistica dell'Universo, dobbiamo porci nell'ottica di affrontare il calcolo e l'elaborazione delle informazioni utilizzando sistemi quanto-meccanici e tecniche coerenti con la MQ.

Retrospettiva

La MQ ha già prodotto nel mondo moderno una prima rivoluzione molto più incisiva di quelle sociali, costituendo la base teorica per lo sviluppo della globale civiltà delle comunicazioni.

Essa ha consentito invenzioni come il laser e il transistor, gli elementi costitutivi di base dei computer, e gli scienziati che costruiscono tali dispositivi seguono le regole della MQ. Ma molto più in generale la MQ ha fornito una chiave di lettura di gran parte dei fenomeni naturali: dalla struttura stellare alle origini della vita. Lo studio del comportamento dei semiconduttori, in particolare, ha prodotto i metodi e le tecniche per produrre quei dispositivi elettronici a risposta rapida, che consentono di memorizzare ed elaborare imponenti quantità di informazione, come mai in precedenza nella storia umana. Tuttavia, la codifica dell'informazione avviene distinguendo valori alto/basso di corrente, o di potenziale elettrico. Cioé la codifica avviene sulla base di un alfabeto binario classico: 0 - 1, si - no, vero - falso, acceso - spento. Espressioni queste del concetto di **bit** come unità base dell'informazione. Questo codice di rappresentazione finito non può essere utilizzato per una ragione intrinseca in MQ: i possibili stati di un sistema fisico si possono sovrapporre linearmente con coefficienti complessi arbitrari. Non esiste più qualcosa del tipo la traiettoria di un corpo, ma si può parlare solo di posizioni più o meno probabili per esso. Tali probabilità si compongono secondo delle regole specifiche, differenti da quelle abituali, diciamo, quelle del gioco dei dadi. Questo aspetto è all'origine di lunghe discussioni, equivoci e incomprensioni, anche tra i fondatori della teoria stessa, tuttora in corso. Inoltre, i vari tentativi teorici di ricondurre questo problema a quello di un modello statistico classico (teoria delle variabili nascoste), ammettendo in definitiva che l'attuale formulazione della MQ sia incompleta, non ha portato i frutti desiderati. Anzi, escogitati opportuni test per dirimere la questione (disuguaglianza di Bell e simili), i dati sperimentali sostengono i postulati della MQ. Questi, a loro volta, implicano delle correlazioni non locali (spesso dette "*entanglement*") tra parti differenti di un sistema fisico, che non hanno alcun analogo classico. L'esistenza di queste correlazioni svolge allora un ruolo importante, quando il sistema fisico considerato funga anche da supporto alla memorizzazione e al trattamento dell'informazione. Per avere un'idea sommaria del concetto di *entanglement*, utilizziamo l'analogia con un libro. Se si tratta di un normale libro classico, per ogni pagina letta si impara una frazione del contenuto totale ed è necessario leggerle tutte singolarmente, per conoscerlo completamente. Supponiamo invece che esista un libro quantistico, le cui le pagine siano fortemente collegate tra loro: nelle singole pagine si trovano solo parole che formano frasi senza senso e, leggendole tutte una ad una, si saprà molto poco del contenuto totale. Bisogna quindi fare un'osservazione collettiva su più pagine contemporaneamente. Una caratteristica di questo tipo rende le informazioni contenute nei sistemi quantistici molto diverse da quelle elaborate dai normali computer digitali. Nel seguito di questo scritto si darà una definizione più tecnica e precisa del concetto.

D'altro canto, la poderosa progressione delle tecnologie informatiche in tutti i campi della nostra vita dipende in larga misura dalla capacità di miniaturizzare i circuiti elettronici. Attualmente la lunghezza della più piccola struttura circuitale riconoscibile raggiunge i 4 nanometri (circa 15 strati di atomi di silicio impilati). Ma a scale prossime a quelle atomiche, gli effetti quantistici cominciano a interferire nel funzionamento dei dispositivi elettronici. Quindi gli approcci progettuali attuali tendono a confliggere con i propri presupposti, quali la certezza della sequenzialità dei processi di calcolo. Ancora una volta siamo di fronte alla necessità di trovare una strada alternativa per elaborare l'informazione.

Naturalmente accanto ai problemi tecnologici si sovrappongono, come si dice, aspetti geopolitici: i detentori di tecnologie così spinte si riducono ad un numero di colossi industriali, nessuno in Europa, che si contano sulle dita di una mano. Non entreremo in queste questioni, ma il lettore dovrebbe tenerle presenti.

Prospettiva

Per affrontare le problematiche esposte sopra si sta proponendo un passaggio all'ambito dell'**Informazione Quantistica**; la scienza che si basa sull'idea di utilizzare dispositivi puramente quantistici per immagazzinare, manipolare e trasmettere informazioni [1],[2], [3]. Essa sintetizza i due campi della MQ e della teoria dell'Informazione, fornendo un punto di vista unificante, sia sul piano applicativo che teorico. L'Informazione quantistica studia la preparazione e il controllo degli stati quantistici dei sistemi fisici ai fini della trasmissione e della manipolazione dell'informazione. Comprende la computazione, la comunicazione e la crittografia quantistiche. Questo campo si basa su una ampia gamma di nuovi dispositivi, tenuto conto sia della varietà di osservabili fisici che possono essere usati per la computazione, sia dello sviluppo di tecniche raffinate di preservazione della fase relativa degli stati in sovrapposizione: la cosiddetta **coerenza** degli stati. Quindi non si misureranno solo correnti elettriche, ma stati di carica, di spin, di cammino, di eccitazione interna, di numeri di occupazione e altri osservabili. Non più solo elettroni, per esempio confinati in *quantum dots* [9], ma nuclei con tecniche di Risonanza Magnetica Nucleare (NMR) [3], [10], atomi in cavità elettromagnetiche [11], [12], catene di ioni [13], [14],[15], fotoni [16], fononi [17] e anioni [18]. Infatti, l'unità di informazione quantistica, il **qubit** può essere realizzato e trasportato fisicamente in molti modi diversi: può esserlo da un singolo atomo, o da un singolo elettrone, o da un singolo fotone. Oppure un qubit può essere realizzato utilizzando un sistema più complicato, come un circuito elettrico superconduttore, a bassa temperatura, nel quale si muovono molti elettroni [19]. L'area di ricerca dei supporti materiali richiesti ed il loro controllo è indicata genericamente come **tecnologie quantistiche**: per un quadro sinottico si veda Fig. 20 e [20, 21].

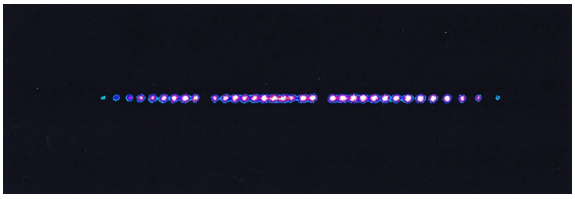


Figura 1: Immagine in fluorescenza di diversi ioni atomici di mercurio $^{199}Hg^{+}$ intrappolati. Gli ioni sono distanziati di $\approx 15\,\mu m$ e le due lacune sono isotopi differenti del mercurio, che non rispondono alla sorgente laser. (NIST)

Poiché la MQ è fondamentalmente probabilistica, la casualità e l'incertezza sono profondamente radicate nel calcolo e nell'informazione quantistici. Di conseguenza, gli algoritmi quantistici sono di natura casuale, nel senso che forniscono soluzioni solo con una una associata distribuzione di probabilità. Il compito di massimizzare le distribuzioni attorno alle soluzioni desiderate costituisce il compito fondamentale di un buon algoritmo quantistico. In prospettiva quindi siamo in presenza di una seconda rivoluzione quantistica, che riguarda fondamentalmente il controllo dei singoli sistemi quantistici in misura molto più marcata rispetto a prima [22].

In che senso un computer quantistico dovrebbe essere più potente

La frontiera dell'*entanglement*

Per un fisico come me, ciò che è entusiasmante dell'informatica quantistica è che abbiamo buone ragioni per credere che un computer quantistico sia in grado di simulare in modo efficiente qualsiasi processo che avviene in Natura. Vorremmo sondare più a fondo le proprietà di molecole complesse e dei materiali esotici, esplorare la fisica fondamentale simulando le proprietà delle particelle elementari o il comportamento quantistico di un buco nero, o l'evoluzione dell'universo subito dopo il Big Bang.

Non pensiamo che ciò non sia possibile grazie ai computer digitali classici, ma che essi (per quanto ne sappiamo) non possono simulare siste-

mi quantistici altamente correlati. Tali situazioni costituiscono la frontiera dell'*entanglement*. La nostra fiducia che l'esplorazione della frontiera dell'*entanglement* sarà gratificante si basa in gran parte su due principi:

1. la teoria della complessità quantistica: una tecnica per esprimere l'efficacia dell'informatica quantistica;
2. la teoria della correzione dell'errore quantistico: una tecnica per consentire ai computer quantistici di rimanere affidabili, proteggendoli dalla perdita di coerenza dei qubit, ed efficienti, anche se il numero degli stessi qubit e delle operazioni di controllo dovessero aumentare di diversi ordini di grandezza.

Complessità computazionale

Quando parliamo di complessità quantistica, ciò che ci viene in mente è la sconcertante mole di dati classici ordinari necessari per descrivere stati quantistici altamente correlati. Infatti, le correlazioni in un dato insieme di qubit sono espresse da una quantità di numeri complessi esponenzialmente crescente con la numerosità dell'insieme stesso. Tuttavia, per quanto questo suggerisca una inimmaginabile potenza di immagazzinamento ed elaborazione dell'informazione, non c'è garanzia di per sé che i computer quantistici siano più efficienti di quelli classici. In effetti, ci sono almeno tre buone ragioni per pensare che questo sia il caso.

- Conosciamo problemi che riteniamo siano difficili da affrontare per i computer classici, ma per i quali sono stati scoperti algoritmi quantistici che potrebbero risolverli molto più facilmente.

  L'esempio più noto consiste nel trovare i fattori primi di un grande intero composito N [4]. Discuteremo successivamente con maggiore dettaglio questo problema ma, in genere, si ritiene che la fattorizzazione sia classicamente difficile, perché non è stato trovato alcun algoritmo in grado di farlo per tutti i numeri interi in un tempo, o con una quantità di risorse computazionali, che crescano secondo una legge del tipo $O(b^k)$, essendo $b = \log_2 N$ i bit rappresentativi e k una certa costante positiva, che caratterizza i problemi di classe P . Non è stata dimostrata la non esistenza di tali algoritmi, quindi si sospetta che il problema non sia di classe P , mentre è chiaramente di classe NP , cioé ipotizzando

Complessità a confronto

La complessità computazionale è riferita a modelli digitali di calcolo comparabili con una macchina di Turing (TM): TM deterministica (DTM), TM quantistica (QTM) cioè che processa un algoritmo quantistico su una memoria quantistica, TM classica non deterministica (o probabilistica) (NTM), essa è anche detta Oracolo, non essendo sequenziale. Le classi di complessità sono definite dal tempo di esecuzione che una TM impiega per un certo calcolo in funzione delle dimensioni dell'input. P denota quei problemi che sono risolvibili in modo efficiente con un computer classico in un tempo crescente come la potenza intera del numero di bit in ingresso. P è un sottoinsieme di NP, che è la classe dei problemi le cui soluzioni sono verificabili in modo efficiente da un computer classico. Essi potrebbero essere risolti efficientemente da una NTM. I problemi NP-hard sono i problemi difficili almeno quanto il più generico problema NP. Quindi nemmeno una NTM potrebbe risolverli efficientemente. I BQP sono problemi che potrebbero essere risolti in un tempo polinomiale da una QTM. Poiché l'esito di un calcolo in questo ambito ha un carattere probabilistico, tali algoritmi vanno confrontati con i problemi BPP, cioé quelli risolubili con algoritmi probabilistici a tempo polinomiale con errore limitato, contenente problemi decisionali risolti da famiglie di circuiti uniformi randomizzati di dimensione polinomiale. QTM non sembra contenere interamente NP e NP-hard ed inoltre non si è dimostrata neanche la disuguaglianza BPP $\neq$ BQP . QMA denota i problemi verificabili efficientemente da un computer quantistico. I problemi QMA-hard sono i problemi difficili almeno quanto un qualsiasi problema in QMA.

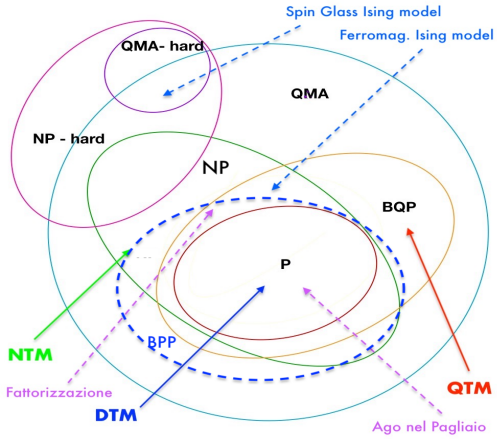


Figura 2: Diagramma delle Complessità Computazionale. Alcuni problemi celebri sono collocati nelle loro classi di complessità.

una soluzione la sua verifica è facile. Per una introduzione alla *Teoria della Complessità Computazionale* si può fare riferimento a [5]. Una sintesi estrema è contenuta nel riquadro "Complessità a confronto". In generale, gli algoritmi quantistici possono accelerare le procedure di calcolo. Il tipico esempio è costituito dal cosiddetto algoritmo di Grover [6] per la ricerca in un database disordinato, o problema dell'`Ago nel Pagliaio`. La sua implementazione sarà descritta con un certo dettaglio nel seguito, ma qui ci basti avere un'idea generale di quale sia il concetto di fondo. Ad esempio, si immagini una rubrica telefonica contenente N nomi disposti in ordine completamente casuale. Per trovare il numero di telefono di qualcuno con una probabilità del 50% un algoritmo classico (sia deterministico che probabilistico) dovrà accedere al database un minimo di $\frac{1}{2}N$ volte. Memorizzando il database su un sistema quantistico, che si trovi in una sovrapposizione di stati, si possono esaminare simultaneamente più nomi. Regolando adeguatamente le fasi relative dei qubit durante le varie operazioni, si ottiene una amplificazione di certe specifiche ampiezze di probabilità, mentre altre interferiscono in modo casuale quasi azzerandosi. Di conseguenza, si può dimostrare che il numero di telefono desiderato può essere ottenuto con $O(\sqrt{N})$ accessi al database. Il che rappresenta un certo guadagno in velocità rispetto alle $O(N)$ del metodo classico.

- Argomenti della teoria della complessità mostrano (sotto presupposti ragionevoli) che la misura di tutti i qubit in uno stato *entangled* avviene con una distribuzione di probabilità correlata, che non può essere campionata efficientemente con alcuna procedura classica [7] [8].

- Nessun algoritmo classico conosciuto può simulare un computer quantistico. Ciò rimane vero anche dopo molti decenni di sforzi da parte dei fisici indirizzati a trovare modi migliori per simulare i sistemi quantistici.

Per un fisico, l'ambito naturale in cui cercare problemi che siano classicamente difficili, ma in principio facili per un *quantum computer*, è simulare un sistema quantistico a molte particelle. Una serie di modelli di riferimento sono costituiti dai vetri di spin (Spin Glass Ising model, vedi Fig. 2), la cui classe di complessità è stata dimostrata essere NP-complete [24], [25]. Anche se B. Laughlin e D. Pines [26] sollevarono molte perplessità sulla possibilità teorica di risolvere le equazioni che descrivono molte particelle tra loro *entangled*, circa 40 anni dopo la proposta di Feynman [1] stiamo appena iniziando a raggiungere la fase in cui i computer quantistici possono fornire soluzioni utili a problemi quantistici complessi. Questo senza essere necessariamente riduzionisti ad ogni costo.

Scogli e Criteri

Il nocciolo del problema deriva da una caratteristica fondamentale del mondo quantistico a volte noto come `Principio di Indeterminazione di Heisenberg`: non possiamo osservare un sistema quantistico senza produrvi un disturbo incontrollabile. Allora, per archiviare ed elaborare informazioni in modo affidabile su un supporto quantistico, dobbiamo mantenere tale sistema quasi perfettamente isolato dal mondo esterno. Allo stesso tempo, però, vogliamo che i qubit

interagiscano fortemente tra loro, in modo da poter correlare le informazioni tra di essi. Inoltre, dobbiamo essere in grado di controllare il sistema dall'esterno ed eventualmente leggere i qubit, in modo da estrarre il risultato del nostro calcolo. Ci sono troppe condizioni in conflitto nel realizzare e utilizzare un sistema quantistico. La prospettiva tecnologica entro la quale l'Informazione quantistica si muove è definita dai cosiddetti criteri di Di Vincenzo [27], che costituiscono la principale linea guida per fisici e ingegneri che costruiscono computer quantistici. Essi sono:

1. Trovare qubit ben caratterizzati e scalabili. Molti dei sistemi quantistici che troviamo in natura non sono qubit, quindi dobbiamo trovare un modo per farli comportare come tali. Inoltre, dobbiamo mettere insieme molti di questi sistemi.

2. Determinare procedure di inizializzazione del qubit. Dobbiamo essere in grado di preparare ripetutamente lo stesso stato entro un margine di errore accettabile.

3. Garantire tempi di coerenza lunghi rispetto all'esecuzione del calcolo. I qubit perderanno le loro proprietà quantistiche dopo aver interagito con l'ambiente. Vorremmo che durino abbastanza a lungo da poter eseguire tutte le operazioni quantistiche richieste.

4. Realizzare l'insieme universale delle `Porte Logiche Quantistiche`. Dobbiamo eseguire operazioni arbitrarie sui qubit. Per fare ciò, sono necessarie sia porte a qubit singolo che porte a due qubit. Questo aspetto deve essere appropriatamente approfondito.

5. Avere la capacità e le procedure di misurazione dei singoli qubit. Per leggere il risultato di un algoritmo quantistico, dobbiamo misurare accuratamente lo stato finale di un insieme prescelto di qubit.

Oltre alla produzione di materiali e metodi di controllo appropriati, sarà cruciale il ricorso alla correzione degli errori quantistici [28], il che permetterà di aumentare anche il numero di qubit utilizzabili. L'idea base è che per proteggere un sistema quantistico da disturbi, l'informazione va codificata in uno stato altamente *entangled*. Questo stato *entangled* ha la proprietà che l'ambiente, interagendo con le parti del sistema, non sia in grado di leggere le informazioni correlate e quindi non può danneggiarle. Sfortunatamente, la correzione degli errori quantistici comporta costi generali significativi: scrivere le informazioni quantistiche protette in un libro altamente correlato richiede molti qubit fisici aggiuntivi, quindi è improbabile che computer quantistici affidabili che utilizzino la correzione degli errori quantistici siano disponibili a breve. Anche se dispositivi basati su circuiti superconduttori sono stati recentemente resi operativi rispettivamente da Google con 53 qubit [29] e con 127 da IBM [30], rimane comunque una scala limitata di possibili risorse computazionali. Questi sono i numeri con i quali ci si dovrà confrontare e possiamo considerare l'attuale stato dell'arte, che Preskill [31] ha battezzato *NISQ era*: epoca della Scala Quantistica Intermedia Rumorosa. Nonostante tutto, sembra che alcuni importanti test di efficienza (alcuni basati sullo studio di modelli di Ising in 3d) siano stati dimostrati [32], [33]. Questo sembra valere anche per i sistemi nanofotonici, come dimostra la Xanadu [34] nel lavoro [35].

Per approfondimenti dei vari aspetti sia della teoria dell'Informazione quantistica, che delle realizzazioni concrete di *quantum computers* si rimanda ai testi base, ormai dei classici, [36]-[41], oppure ai più recenti [42, 43].

Richiami di MQ

Quadro

La differenza più significativa tra la Fisica Classica e la MQ risiede nel fatto che quest'ultima permette di ottenere soltanto previsioni probabilistiche delle varie grandezze. Nonostante essa appaia controintuitiva, non solo fornisce una spiegazione plausibile e coerente dei fenomenti che avvengono a scala atomica, o subatomica, ma anche molte proprietà della fisica a scala macroscopica possono essere pienamente interpretate e comprese alla sua luce. Basti pensare a tutta la Fisica dei metalli e dei semiconduttori. È noto che fenomenologicamente le onde luminose, in certe condizioni, si comportano come particelle, mentre le particelle si comportano come

onde (dualità onda-particella). La MQ fornisce una descrizione matematica di tale dualità onda-particella e dell'interazione tra materia ed energia a livello di processi elementari microscopici. Essa descrive i sistemi fisici e la loro evoluzione temporale con l'ausilio di entità matematiche (funzioni d'onda, operatori di stato, etc.), che non necessariamente corrispondono a quantità fisicamente osservabili, ma che incapsulano le distribuzioni di probabilità relative agli esiti delle misure di ogni possibile grandezza osservabile sul sistema.

Dal punto di vista della MQ i singoli eventi non sono riproducibili. Tuttavia i risultati delle `Misurazioni` di uno stesso `Osservabile`, su una sequenza (idealmente infinita) di `Preparazioni` uguali dello stesso `Sistema`, hanno distribuzioni di frequenza limite ben definite. Ogni specifica `Preparazione` determina le distribuzioni di probabilità di tutti i possibili `Osservabili` del `Sistema`. Quindi uno `Stato` del dato `Sistema` è identificato con l'insieme di tutte le `Distribuzioni di Probabilità` degli esiti di ogni possibile `Misurazione`. Per tal motivo è impossibile dedurre lo `Stato` iniziale del sistema dal risultato di una `Misurazione`. Infine, esistono `Osservabili Incompatibili`. Il che equivale a dire che le distribuzioni di probabilità degli esiti di `Misurazioni` su `Osservabili` distinti sono in generale correlate. Questo postulato è privo di un analogo classico. Pertanto l'atto di acquisire informazioni su un sistema misurando l'`Osservabile` $\mathcal{A}$ disturba lo `Stato`, talché l'esito della `Misura` di un altro `Osservabile` $\mathcal{B}$ ne verrà influenzato in modo casuale. Infine, è un fatto che più stati si possano sommare linearmente con coefficienti complessi, che nel dar luogo alle nuove distribuzioni di probabilità intervengono in maniera quadratica. Per gli approfondimenti relativi a queste tematiche si vedano i manuali [44, 45, 46]. Alcune idee fondanti della MQ sono presentate nell'Appendice.

Qubit

Il qubit è il più semplice sistema quantistico, realizzato da un qualsiasi sistema fisico che abbia un osservabile dicotomico, cioé con uno spettro costituito da due valori reali non degeneri. Ad essi corrispondono due autostati ortogonali. Esempi fisici di qubit sono gli stati di polarizzazione dei fotoni, un atomo con due livelli energetici, lo spin dell'elettrone o quello del protone e simili sistemi che posseggono due stati ben distinti.

Matrici di Pauli.

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \; ; \; \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \; ; \; \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

In ossequio al bit classico, che assume i valori logici 0 e 1, esistono due vettori $\{|0\rangle, |1\rangle\}$, che costituiscono una base ortonormale nello spazio di Hilbert associato al qubit

$$\begin{aligned} \mathcal{H} \equiv \mathbb{C}^2 &= \{|\psi\rangle = a\,|0\rangle + b\,|1\rangle\}_{a,b\in\mathbb{C}} \\ &\quad \langle\psi\,|\psi\rangle = |a|^2 + |b|^2\,. \end{aligned} \tag{1}$$

Tale spazio è invariante rispetto alle trasformazioni unitarie

$$\begin{aligned} \mathbf{U}(\hat{\mathbf{n}},\theta) &= e^{-\imath\frac{\theta}{2}\hat{\mathbf{n}}\cdot\overrightarrow{\sigma}} \\ &= \mathbf{1}_2\cos\frac{\theta}{2} - \imath\hat{\mathbf{n}}\cdot\overrightarrow{\sigma}\sin\frac{\theta}{2}\;, \end{aligned} \tag{2}$$

espresse dalle matrici di Pauli $\{\sigma_0 = \mathbf{1}_2, \overrightarrow{\sigma}\} = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ (vedi riquadro). Gli operatori σ_i sono hermitiani e rappresentano `Osservabili Fisici` corrispondenti, per esempio allo stato di polarizzazione di spin/momenti magnetici elementari lungo tre direzioni ortogonali nello spazio [44, 45, 46]. Le componenti $1, 2, 3$ di questi `Osservabili` sono incompatibili tra loro che, come si è detto in precedenza, è una delle caratteristiche specifiche di MQ. Questo schema può essere generalizzato a qualsiasi sistema fisico, che ammetta tre osservabili dicotomici, che godono delle stesse proprietà delle matrici di Pauli. Nel quadro teorico della MQ, facendo eventualmente rifermento alla sintesi dei suoi postulati riportata in Appendice, lo stato fisico di un qubit è descritto da un operatore di stato hermitiano positivo a traccia 1 (per brevità, da qui in poi, si userà `stato` per indicare un operatore di stato)

$$\boldsymbol{\rho}(\overrightarrow{p}) = \tfrac{1}{2}(\mathbf{1} + \overrightarrow{p}\cdot\overrightarrow{\sigma})\,, \tag{3}$$

dove $\overrightarrow{p} \in \mathbb{R}^3$, $0 \leq \overrightarrow{p}^2 \leq 1$. Quindi tutti

gli stati sono in corrispondenza biunivoca con i punti contenuti in una sfera di raggio unitario, detta la **Sfera di Bloch**. Se un qubit è nello stato $\boldsymbol{\rho}$, le misure di una qualunque pertinente grandezza fisica $\mathcal{O}$ hanno come loro valor medio $\langle \mathcal{O} \rangle = tr \boldsymbol{\rho}\, \mathbf{O}$ (vedi la Regola di Born in Appendice), avendo denotato con $\mathbf{O}$ il corrispondente operatore osservabile hermitiano su $\mathcal{H}$. La proprietà cruciale degli stati, immediatamente verificabile, è che si possono sommare secondo la combinazione lineare convessa $\boldsymbol{\rho}\,(\lambda) = \lambda\ \boldsymbol{\rho}_1 + (1-\lambda)\,\boldsymbol{\rho}_2,\ 0 \leq \lambda \leq 1$. Questa formula connette tutti gli stati che si trovano sulla corda tra $\boldsymbol{\rho}_1$ e $\boldsymbol{\rho}_2$, rappresentati come punti nella Sfera di Bloch. È evidente che, in generale, ogni singolo stato può avere un numero infinito di queste rappresentazioni, ad eccezione di quelli che si trovano esattamente sulla superficie della Sfera di Bloch. Dall' espressione in (3) si deduce che gli stati puri sono `operatori di Proiezione`, cioé della forma

$$\boldsymbol{\rho} = |\psi\rangle\langle\psi|,\ \ |\psi\rangle \in \mathcal{H},\ \langle\psi\,|\psi\rangle = 1,$$

dove $|\psi\rangle$ è detto **vettore di stato**. A loro volta, essendo i vettori di stato elementi di $\mathcal{H}$, si possono sommare tra loro con coefficienti complessi come, per esempio, riportato in (1). Combinazioni lineari di vettori di stato sono dette `coerenti` e, una volta normalizzate a 1, corrispondono univocamente a nuovi stati puri $\boldsymbol{\rho}$ collocati sulla superficie della Sfera di Bloch. Da un punto di vista fisico gli stati puri rappresentano tutti e soli gli stati di un qubit isolato. Pertanto, ogni coppia di essi può essere connessa da una trasformazione unitaria, del tipo indicato in (2).

Invece, i punti interni alla Sfera rappresentano **Stati Misti**, cioé miscele statistiche classiche degli stati puri (non di vettori di stato, attenzione!). Come visto in precedenza, queste combinazioni, dette `incoerenti`, sono convesse e, in una opportuna scelta di base in $\mathcal{H}$, possono essere espresse con coefficienti reali positivi di somma 1.

I punti interni della Sfera di Bloch possono essere raggiunti da uno stato puro iniziale tramite trasformazioni non unitarie. Pertanto si è nella condizione di descrivere con un unico quadro teorico sia il qubit come sistema isolato, evoluzione unitaria, sia quando esso è parte di un sistema aperto, con evoluzione non unitaria, ma che preserva la traccia e la positività di $\boldsymbol{\rho}$ (si veda la sezione Decoerenza nel seguito). Questo si realizza, per esempio, quando il qubit è in interazione con un ambiente esterno, comunque modellato, che non si possa o non si voglia controllare.

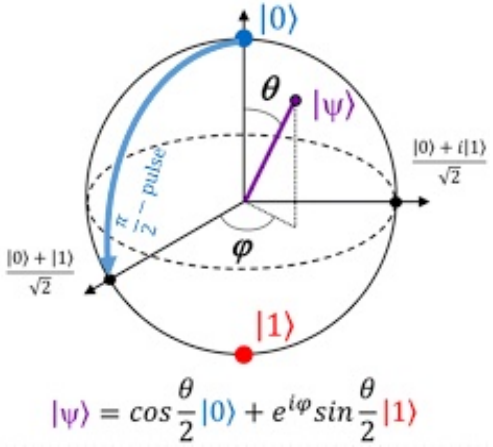


Figura 3: La sfera di Bloch.

Chiaramente le trasformazioni non unitarie fanno perdere, in generale, la correlazione di fase tra i coefficienti complessi dei vettori di base, nella quale è espresso il vettore di stato iniziale. Questo fenomeno è chiamato **Decoerenza** ed è il principale ostacolo alla computazione quantistica, che intende basarsi esattamente sul controllo dei vettori di stato e della loro evoluzione. Ricordiamo a tal proposito il criterio 3. di Di Vincenzo nella sezione precedente.

In conclusione il qubit costituisce un modello elementare, sia in sovrapposizione coerente di stati puri, che in quelli incoerenti degli stati misti in presenza di decoerenza e rumore.

Tuttavia è abbastanza chiaro che ben poco si possa fare con un solo qubit, quindi è necessario passare a `Sistemi Composti`, il cui modello minimale è quello del 2-qubit, descritto nello spazio di Hilbert

$$\begin{aligned} & \mathcal{H}_A \otimes \mathcal{H}_B \\ \equiv\ & Span\,\{\,|0_A\rangle,\,|1_A\rangle\} \otimes \{\,|0_B\rangle,\,|1_B\rangle\} \\ =\ & Span\,\{\,|0_A\,0_B\rangle,\,|0_A\,1_B\rangle,\,|1_A\,0_B\rangle,\,|1_A\,1_B\rangle\} \quad . \end{aligned}$$

Questa struttura della base suggerisce subito la notazione `computazionale`

$$\mathcal{H}_A \otimes \mathcal{H}_B \equiv Span\,\{\,|0\rangle,\,|1\rangle,\,|2\rangle,\,|3\rangle\}\,.$$

Ovviamente tale spazio ha dimensione $4 = 2^2$.

Ma se si mettono assieme 3 qubit il loro spazio è

$$\begin{aligned} & \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C = \left(\mathbb{C}^2\right)^{\otimes 3} \\ = \quad & Span\{\, |0_A\, 0_B\, 0_C\rangle,\, |0_A\, 0_B\, 1_C\rangle, \\ & |0_A\, 1_B\, 0_C\rangle, \ldots\} \end{aligned}$$

che è a $8 = 2^3$ dimensioni e così via all'aumentare del numero di qubit. Lo spazio di Hilbert di n qubit è $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes n}$ con dimensioni 2^n.

Si consideri, ora, un sistema bipartito AB in un particolare stato puro, specificato dal vettore di stato

$$|\psi\rangle_{AB} = a\,|0_A\, 1_B\rangle + b\,|1_A\, 0_B\rangle \tag{4}$$

con $|a|^2 + |b|^2 = 1$. Si supponga, inoltre, che un osservatore esegua una misura dell'osservabile locale σ_{3A}, che considera solo il qubit A rimanendo ininfluente sullo stato di B. I possibili esiti si verificano secondo la seguente distribuzione di probabilità $\mathcal{P}$ (si veda l'Appendice):

$$\left\{ \begin{array}{ccc} valore & \mathcal{P} & \texttt{Stato ridotto} \\ 0 & |a|^2 & |0_A\, 1_B\rangle, \\ 1 & |b|^2 & |1_A\, 0_B\rangle. \end{array} \right. \tag{5}$$

Dalla tabella deduciamo che l'esito della misura sul sottosistema A comporta immediatamente informazione sullo stato del sottosistema B. Lo stato considerato stabilisce una correlazione interna tra i sottosistemi A e B. Tale correlazione è il prototipo del concetto di *Entaglement*.

Entanglement

EPR

Nel 1935 Einstein, Podolski e Rosen considerarono un sistema analogo a quello descritto sopra per presentare un esperimento mentale, con lo scopo di dimostrare la non completezza della MQ come teoria della `Natura` [48]. La loro convinzione era che in qualsiasi teoria fisica completa ogni elemento di realtà dovesse essere rappresentato. Essi ritenevano che una condizione sufficiente affinché una proprietà fisica sia un elemento di realtà consista nella possibilità di prevederne con certezza il suo valore immediatamente prima della misurazione. Le precedenti misurazioni condotte dall'osservatore A gli consentono di prevedere con certezza quale possa essere il valore dell'osservabile locale σ_{3B} effettuata dal suo omologo osservatore B. Riuscendo A a prevedere il valore dell'osservabile adottato da B, esso deve corrispondere a un elemento della realtà, il quale a sua volta dovrebbe essere rappresentato in qualsiasi teoria fisica completa. In particolare, la riduzione (o collasso) dello stato puro (4) nello stato ridotto in (5) dovrebbe avvenire istantaneamente per tutto il sistema composto, indipendentemente dalla distanza relativa tra A e B. In tal modo verrebbe introdotta una *spooky action at a distance*, incompatibile con la `Relatività Speciale`, che invece impone una condizione di località: l'influenza di un corpo su un altro non può manifestarsi ad una velocità superiore a quella della luce. Tuttavia, la MQ dice semplicemente come calcolare le probabilità dei possibili risultati di un osservabile, quando esso viene misurato, e non include alcun altro elemento più fondamentale.

Bell & Co.

Quasi trent'anni dopo la pubblicazione dell'articolo EPR [48] è stato proposto un test, noto come disuguaglianza di Bell [49], utilizzabile per verificare sperimentalmente la validità dell'ipotesi di località di Einstein (o realismo locale) in MQ: se A e B sono sistemi quantistici spazialmente separati, un'azione eseguita sul sistema A non deve modificare la descrizione del sistema B. L'idea fruttuosa di Bell fu quella di testare la località di Einstein, tradotta nella cosiddetta "teoria delle variabili nascoste". Il test si basa sulla stima quantitativa delle correlazioni tra gli esiti delle misure effettuate, rispettivamente, dall'osservatore `Alice` su A e dall'osservatore `Bob` su B, i quali condividono un 2-qubit A-B. Un ausiliario preparatore `Caio` fornisce una sequenza, idealmente infinita, di copie del 2-qubit preparate sempre nello stesso stato.

Se i valori delle variabili nascoste fossero esattamente noti, allora i risultati di qualsiasi misurazione potrebbero essere previsti con certezza. Ma in realtà bisogna continuare a descriverli probabilisticamente, perché di fatto possiamo solo fissare il dominio delle variabili nascoste. In secondo luogo si presume che tali variabili siano locali, cioé ogni decisione di `Bob` sul tipo di misura da effettuare, non ha alcun effetto sulle variabili

nascoste che regolano le misure di `Alice`, purché tali osservatori siano causalmente disconnessi. Questo significa i due osservatori sono tanto lontani tra loro, che un segnale luminoso non potrà giungere dall'uno all'altro prima che entrambe le rispettive misure siano state eseguite.

Per ipotesi `Alice` può decidere di misurare casualmente uno dei due osservabili $\mathbf{Q}$ o $\mathbf{R}$ e, analogamente, `Bob` può misurare $\mathbf{S}$ o $\mathbf{T}$, essendo $\{\pm 1\}$ lo spettro di ognuno degli osservabili. Allora, sotto le ipotesi della teoria delle variabili nascoste, si può dimostrare la disuguaglianza di (tipo) Bell

$$\begin{aligned} \Delta_{CHSH} &= \mathcal{E}(\mathbf{Q}\,\mathbf{S}) + \mathcal{E}(\mathbf{R}\,\mathbf{S}) \\ &+ \mathcal{E}(\mathbf{R}\,\mathbf{T}) - \mathcal{E}(\mathbf{Q}\,\mathbf{T}) \leq 2 \ , \end{aligned}$$

dove $\mathcal{E}$ rappresenta il valor medio rispetto all'ipotetica distribuzione di probabilità delle variabili nascoste, qualunque essa sia. Il pedice CHSH nella precedente relazione fa riferimento alle iniziali dei ricercatori J.F.Clauser, M.A.Horne, A.Shimony, R.A.Holt, che diedero la formulazione della disuguaglianza qui presentata [50].

Si supponga ora che il sistema considerato sia un 2-qubit con vettore di stato $|\psi_{AB}\rangle$ e segua la sola MQ, senza alcun riferimento a variabili nascoste. Gli osservabili presi in considerazione siano

$$\begin{aligned} \mathbf{Q} &= \overrightarrow{\sigma}_A \cdot \hat{\mathbf{q}}, \qquad \mathbf{R} = \overrightarrow{\sigma}_A \cdot \hat{\mathbf{r}}, \\ \mathbf{S} &= \overrightarrow{\sigma}_B \cdot \hat{\mathbf{s}}, \qquad \mathbf{T} = \overrightarrow{\sigma}_B \cdot \hat{\mathbf{t}}, \end{aligned}$$

dove i simboli con il cappuccio indicano versori nello spazio, lungo i quali si misurano le componenti di spin $\overrightarrow{\sigma}$. È immediato valutare la CHSH usando la MQ, specificamente la formula di Born (si veda l'Appendice). Per esempio, se detti versori sono coplanari e sono separati da angoli di 45^o e lo stato $|\psi\rangle_{AB}$ dell'equazione (4) è determinato dalle ampiezze $a = -b = 1/\sqrt{2}$, si ottiene $\Delta_{CHSH} = 2\sqrt{2} \geq 2$, che viola chiaramente la CHSH. Si scopre quindi che le correlazioni previste dalla MQ sono, in generale, incompatibili con le ipotesi di una teoria di variabili nascoste.

Nel 1982, Aspect e collaboratori [51] condussero un esperimento che dimostrava la violazione di CHSH e affrontando la questione della separazione causale tra le azioni di A e B. Per questo lavoro Aspect ha ricevuto il premio Nobel nel 2022 [52], assieme a J. Clauser e A. Zeilinger, anch'essi "per esperimenti con fotoni *entangled*, per stabilire la violazione delle disuguaglianze di Bell e per aprire la strada alla scienza dell'informazione quantistica".

Rimane da verificare che la teoria delle variabili nascoste non rientri in gioco controllando lo stato dei rivelatori, oppure la stessa tecnica decisionale delle osservazioni da effettuare. In ogni caso, si avrebbe una causa di inapplicabilità della condizione CHSH. Perciò la verifica sperimentale di tale disuguaglianza, o simili, è un'attiva area di ricerca. Per esempio, molto recentemente è stato pubblicato un articolo su Physical Review X [53], nel quale si riporta di un esperimento EPR con due condensati di Bose-Einstein spazialmente separati, ciascuno contenente circa 700 atomi di rubidio. L'*entanglement* tra i condensati si manifesta in forti correlazioni dei loro spin collettivi. Tali esperimenti mostrano che il conflitto tra la MQ e il realismo locale non scompare quando le dimensioni del sistema aumentano.

Da Enigma a Risorsa

Dopo il lavoro di Bell, l'*entanglement* quantistico divenne oggetto di studio intensivo da parte di coloro che erano interessati ai fondamenti della teoria quantistica. Ma a poco a poco si è evoluto un nuovo punto di vista: l'*entanglement* è anche una risorsa potenzialmente preziosa. Sfruttando gli stati quantistici *entangled*, possiamo svolgere compiti altrimenti difficili o impossibili. Questa caratteristica essenziale della MQ è vista oggi come una risorsa fisica, che può essere spesa per risolvere compiti di elaborazione delle informazioni in modi nuovi, ma anche per descrivere nei dettagli gli stati della teoria dei campi quantistici [54].

Il primo obiettivo è definire quando un sistema si trova in uno stato *entangled*. L'idea di base consiste nel comprendere quale informazione si riesca ad ottenere effettuando misure soltanto sul sottosistema A, ignorando quanto si verifichi in B. Da un punto di vista matematico, lo strumento che realizza questo concetto consiste nella **traccia parziale**. Considerando uno stato puro $\boldsymbol{\rho}_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, la sua traccia parziale rispetto a B

è lo stato di A fornito dalla relazione

$$\begin{aligned}\boldsymbol{\rho}_A &= tr_B\left(|\psi_{AB}\rangle\langle\psi_{AB}|\right)\\ &= \sum_{\pi\mu\nu} c^*_{\pi\nu}c_{\mu\nu}\,|\mu_A\rangle\langle\pi_A|,\end{aligned}$$

dove il vettore di stato

$$|\psi_{AB}\rangle = \sum_{\mu,\nu} c_{\mu\nu}\,|\mu_A\rangle\otimes|\nu_B\rangle$$

è stato sviluppato in una generica base di $\mathcal{H}_{AB}$. Questa decomposizione è utile quando si considerano osservabili locali solo di A, in quanto si dimostra che il valor medio di ogni osservabile $\mathbf{O}_{AB} = \mathbf{O}_A \otimes \mathbf{1}_B$ si scrive come

$$\langle \mathbf{O}_{AB}\rangle = tr\left(\mathbf{O}_A\,\boldsymbol{\rho}_A\right).$$

Questa relazione caratterizza tutti gli osservabili e le trasformazioni locali su A (analogamente su B). Per un generico sistema bipartito si dice che $\boldsymbol{\rho}_{AB}$ è uno **stato *entangled*** se

$$\boldsymbol{\rho}_{AB} \neq \sum_\mu p_\mu\,\boldsymbol{\rho}^\mu_A\otimes\boldsymbol{\rho}^\mu_B.$$

dove $\boldsymbol{\rho}^\mu_A$ e $\boldsymbol{\rho}^\mu_B$ sono stati puri per ogni μ. L'insieme complementare è costituito dagli **stati separabili**, per i quali effettivamente si verifica che

$$\boldsymbol{\rho}_{AB} = \sum_\mu p_\mu\,\boldsymbol{\rho}^\mu_A\otimes\boldsymbol{\rho}^\mu_B.$$

con $\boldsymbol{\rho}^\mu_A$ e $\boldsymbol{\rho}^\mu_B$ stati puri.

Un esempio di vettore di stato che rappresenta uno stato puro separabile è dato da

$$|\psi_{AB}\rangle = |1_A\,1_B\rangle\ .$$

Infatti si ha $\boldsymbol{\rho}_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}| = |1_A\rangle\langle 1_A|\otimes|1_B\rangle\langle 1_B|$. Differentemente, il vettore di stato

$$|\phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|0_A\,0_B\rangle + |1_A\,1_B\rangle\right) \qquad (6)$$

corrisponde ad uno stato puro *entangled* dato da

$$\begin{aligned}\boldsymbol{\rho}_{AB} &= |\phi^+_{AB}\rangle\langle\phi^+_{AB}|\\ &= \tfrac{1}{2}[\ |0_A\rangle\langle 0_A|\otimes|0_B\rangle\langle 0_B|\\ &\quad + |1_A\rangle\langle 1_A|\otimes|1_B\rangle\langle 1_B|\\ &\quad + |0_A\rangle\langle 1_A|\otimes|0_B\rangle\langle 1_B|\\ &\quad + |1_A\rangle\langle 0_A|\otimes|1_B\rangle\langle 0_B|]\ ,\end{aligned}$$

dove gli ultimi due termini in parentesi non sono proiettori, né esiste una diversa base in $\mathcal{H}_A\otimes\mathcal{H}_B$ che consenta di eliminare tale tipo di termini.

In generale, un vettore di stato che corrisponde ad uno stato puro bipartito separabile è un prodotto diretto di vettori di stato di $\mathcal{H}_A$ e $\mathcal{H}_B$, cioé $|\psi\rangle_{AB} = |\phi\rangle_A\otimes|\chi\rangle_B$. Corrispondentemente gli stati ridotti $\boldsymbol{\rho}_A = |\phi\rangle_A\langle\phi_A|$ e $\boldsymbol{\rho}_B = |\chi\rangle_B\langle\chi_B|$ sono sempre puri.

Ogni vettore di stato che non può essere espresso come prodotto tensoriale corrisponde ad uno stato *entangled* e, in tal caso, $\boldsymbol{\rho}_A$ e $\boldsymbol{\rho}_B$ sono stati misti. Non esistendo alcun analogo classico di questa situazione, sembra quasi che la peculiarità della MQ sia contenuta negli stati *entangled*. In particolare, si può dimostrare che la CHSH è violata da tutti gli stati *entangled*, mentre è soddisfatta da tutti gli stati separabili. Inoltre l'*entanglement* tra le due parti di un sistema non può essere creato agendo localmente, ma solo attraverso una effettiva interazione tra di esse. Per convenienza, conviene definire gli **stati puri massimalmente *entangled*** come

$$\boldsymbol{\rho}_{AB} = |\Psi\rangle\langle\Psi|,\ \ |\Psi\rangle = \frac{1}{\sqrt{d}}\sum_\mu |\mu_A\rangle\otimes|\mu_B\rangle$$

se accade che

$$tr_A\boldsymbol{\rho}_{AB} = \frac{\mathbf{1}_B}{d},\quad tr_B\boldsymbol{\rho}_{AB} = \frac{\mathbf{1}_A}{d}\ ,$$

essendo d la dimensione dei rispettivi spazi di Hilbert.

Una maniera equivalente di caratterizzare l'*entanglement* degli stati può essere fatta attraverso il concetto di `Numero di Schmidt`, oppure tramite il concetto di `Entropia di Entanglement` $S_A = -tr\left[\boldsymbol{\rho}_A\log\boldsymbol{\rho}_A\right]$, particolarmente utile in teoria dei campi, ma non tratteremo questi aspetti nella presente discussione (vedi [37]).

Non Super-Luminale

Il primo impulso che si potrebbe avere nel manipolare uno stato *entangled* sarebbe quello di utilizzare il carattere non locale delle sue correlazioni per inviare messaggi a velocità superluminale (idea aborrita da Einstein in primis).

Si supponga d'aver preparato una serie copie di un particolare stato puro massimalmente

entangled rappresentato dal vettore

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left[|\uparrow_{\hat{n}\,A}\uparrow_{\hat{n}'_B}\rangle + |\downarrow_{\hat{n}\,A}\downarrow_{\hat{n}'\,B}\rangle\right] \quad (7)$$

specificato dalle direzioni $\hat{n}, \hat{n}'$. Il vettore di stato (6) è chiaramente un caso particolare di (7). Come in precedenza si suppone che gli osservatori `Alice` e `Bob` che posseggono il sottosistema A e B, rispettivamente, siano causalmente disconnessi. Per inviare un messaggio ad `Alice`, `Bob` lo codifica misurando l'osservabile σ_{1B}, oppure σ_{3B}, su ogni qubit in suo possesso, inducendo una corrispondente preparazione del qubit A nella base $\{|\uparrow_{\hat{x}\,A}\rangle, |\downarrow_{\hat{x}\,A}\rangle\}$, oppure in $\{|\uparrow_{\hat{z}\,A}\rangle, |\downarrow_{\hat{z}\,A}\rangle\}$. Tuttavia, sebbene le due preparazioni siano sicuramente differenti, l'operatore di stato che effettivamente possiede `Alice` è $\boldsymbol{\rho}_A = \mathbf{1}_A/2$ Pertanto, non esiste alcuna misurazione che `Alice` possa effettuare per distinguere quale riduzione `Bob` abbia operato. Il messaggio è illeggibile, non c'è possibilità di comunicazioni superluminali. Solo nel caso in cui `Alice` e `Bob` effettuassero la misura lungo uno stesso asse, giungerebbero a una concordanza.

Analogamente, se `Bob` misurasse il suo insieme di qubit, scegliendo a caso una delle due direzioni dello spazio, diciamo x e y, e comunicasse ad `Alice` anche solo la successione dei valori da lui ottenuti, allora con misure su A `Alice` potrebbe distinguere quale degli osservabili sia stato effettivamente misurato. In ogni caso ci deve essere una comunicazione convenzionale, quindi non più veloce della luce.

Usare l' Entanglement

Informazioni e Cancellazioni

Lasciatoci alle spalle questo sogno fantascientifico, ci sono altri aspetti sorprendenti su cui far leva. Ad esempio, sappiamo che gli operatori di stato formano un insieme convesso e gli stati puri sono i punti estremi dell'insieme. Uno stato misto di un sistema A può essere preparato come un insieme di stati puri in molti modi diversi, tutti però sperimentalmente indistinguibili. D'altra parte, per ogni dato stato misto $\boldsymbol{\rho}_A$ si può trovare una sua `purificazione`, cioé un vettore di stato *entangled* $|\Phi_{AB}\rangle$ per un appropriato sistema bipartito A-B, tale che la traccia parziale di $|\Phi_{AB}\rangle\langle\Phi_{AB}|$ in B produca esattamente $\boldsymbol{\rho}_A$.

Inoltre, è possibile trovare un osservabile in B che riproduca, in corrispondenza di ogni esito, il corrispondente stato puro presente nella miscela rappresentata da $\boldsymbol{\rho}_A$. Infine, a seguito di un ulteriore cambiamento di base in B, si può ottenere una nuova rappresentazione degli stati puri che costituiscono $\boldsymbol{\rho}_A$ differenti dai precedenti. Questo risultato è noto come teorema di Gisin-Hughston-Jozsa-Wootters e costituisce la formulazione più generale della procedura detta della **cancellazione quantistica** [36, 37]. Risulta quindi che a seconda dell'informazione acquisita sul sistema B, viene cambiata anche la descrizione fisica dello stato di A.

Tutte queste proprietà dei sistemi bipartiti si possono sfruttare in applicazioni nell'ambito delle teleomunicazioni: il ***dense coding***, il **teletrasporto quantistico** e la **crittografia quantistica**.

Dense Coding

In primo luogo supponiamo che `Alice` possegga due bit di informazione, che desidera inviare a `Bob` in un modo particolarmente efficiente. In effetti, se `Alice` condividesse con `Bob` un 2-qubit in uno stato *entangled* puro, ad esempio rappresentato da (6), lei potrebbe spedirli con un solo qubit (*dense coding*). Sul qubit A, quello in possesso di `Alice`, si possono eseguire solo trasformazioni unitarie locali: per esempio tre rotazioni di π attorno a tre assi ortogonali tra loro, oltre alla rotazione identica. Esse possono cambiare il vettore di stato $|0_A\rangle$ in $|1_A\rangle$ e viceversa, con un eventuale fattore di fase. I corrispondenti stati del 2-qubit complessivo formano i quattro elementi di una base ortonormalizzata di stati massimalmente *entangled* (base di Bell) dello spazio di Hilbert. Dopo una simile preparazione, il qubit A viene inviato lungo un canale classico a `Bob`, il quale esegue una misura collettiva, per esempio di $(\vec{\sigma}_A + \vec{\sigma}_B)^2$ e di $\sigma_{A3} + \sigma_{B3}$ che commutano tra loro. Essa permettere di distinguere inequivocabilmente quale delle quattro trasformazioni sia stata eseguita. Questo equivale alla trasmissione di due bit classici. In conclusione, per comunicare più efficientemente i loro messaggi `Alice` e `Bob` hanno sfruttato un pre-esistente stato *entan-*

gled come una risorsa computazionale quantistica, per ottenere la trasmissione di due bit classici. Realizzazioni sperimentali pionieristiche sono riportate in [55].

Teletrasporto

Ci si chiede ora se sia possibile avere l'effetto inverso, cioé inviare due bit classici per trasmettere un qubit. Si supponga, come prima, che `Alice` e `Bob` posseggano ciascuno uno dei qubit che si trovano in uno stato *entangled* $|\psi_{AB}\rangle$, per semplicità (7). Inoltre, `Alice` è in possesso di un secondo qubit, che per convenienza si denota con $|\widetilde{\psi}_A\rangle$, del quale vuole trasmettere lo stato a `Bob` attraverso un canale di comunicazione classico. A questo scopo, in primo luogo ella provvede a produrre un nuovo stato *entangled* tra i qubit $|\psi_A\rangle$ e $|\widetilde{\psi}_A\rangle$ in suo possesso, facendoli opportunamente interagire. A questo stadio ci sono ben tre qubit in un unico stato *entangled*. Su quelli in suo possesso `Alice` esegue una misura locale, per esempio di σ_{A3}, separatamente su ciascuno dei due qubit. Questa doppia misura produce la coppia di esiti $(m, \tilde{m})$. Ora, su un canale classico `Alice` invia tali dati numerici a `Bob`, il quale possiede un opportuno protocollo di codifica: ad ogni coppia di valori ricevuti corrisponde una ben precisa trasformazione locale sul suo qubit $|\psi_B\rangle$, che gli consente di porlo esattamente nello stato originario definito da $|\widetilde{\psi}\rangle$.

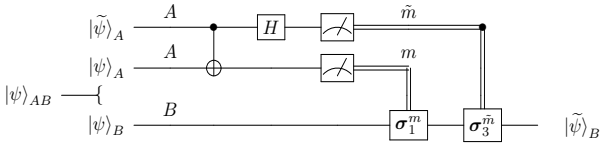


Figura 4: Il Teletrasporto attraverso una rappresentazione circuitale, che verrà discussa più dettagliatamente nel seguito. Gli elementi essenziali sono i due qubit entangled suddivisi tra B ed A, che ne possiede anche un terzo in uno stato specifico. Ogni qubit procede lungo un filo del circuito. Il simbolo che collega i due fili di A rappresenta una specifica forma di interazione tra i due qubit e che li pone in *entanglement*. Le altre operazioni unitarie locali sul singolo qubit vengono rappresentate con dei simboli a `scatola`. Infine le misure vengono rappresentate con un simbolo di `misuratore` e i canali di comunicazione classici con un doppio filo.

La procedura è stata ideata dal gruppo di McGill University [56] ed implementata sperimentalmente in molti modi [57, 59, 60]. In particolare la tecnologia fotonica dal gruppo di Roma [59] è diventata uno standard in questo ambito. Questo sorta di magia è spesso chiamata **Teletrasporto Quantistico**, ma in effetti il termine sembra piuttosto enfatico: 1) nulla di materiale viene trasportato, 2) ma solo informazione su un canale classico a velocità non superiore a quella della luce, 3) inoltre viene distrutto lo stato *entangled* originario per generare un solo qubit in B, quindi c'è un costo in questa operazione, 4) infine il qubit $|\widetilde{\psi}\rangle$ non viene copiato: in primo luogo l'originario viene distrutto dalla misura e solo dopo di ciò il nuovo qubit è prodotto. Queste ultime osservazioni sono conformi al cosiddetto `Teorema di No Cloning`.

Crittografia Quantistica

L'impossibilità di copiare stati quantistici, oltre all'effetto perturbativo di ogni misura su di essi, ha stimolato un'area piuttosto importante di applicazioni chiamata `Crittografia Quantistica`. Si è sviluppata così una grande area di ricerca, sia per quanto riguarda i protocolli di codifica che le tecniche di implementazione. Tra i più noti esempi vi è il protocollo di `distribuzione di`

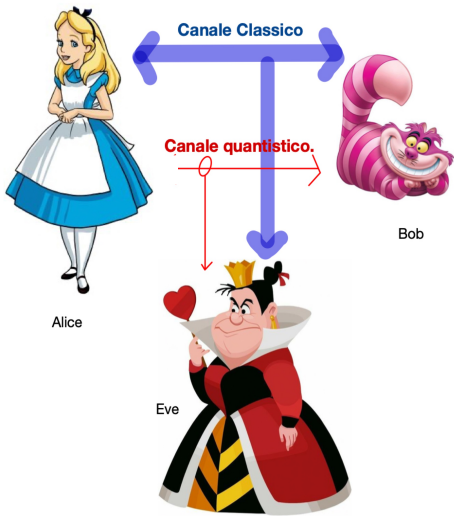


Figura 5: `Alice` e `Bob` possono accordarsi su una comune chiave crittografica sia su un canale classico che uno quantistico. In questo caso, il tentativo di spionaggio da parte di `Eve` incontra difficoltà legate allo stabilirsi di uno stato correlato con i qubit A e B.

chiavi quantistico (QKD) denominato BB84 dal nome dei suoi inventori [61] (Si veda l'articolo di Samuele Altilia, Michele Notarnicola e Stefano Olivares e quello di Taira Giordani, Alessia Suprano, Fabio Sciarrino in questo numero di **Ithaca**).

Lo scopo del protocollo è quello di stabilire una chiave segreta, cioé una sequenza casuale di bit, nota solo alle due parti Alice e Bob, che possono utilizzarla per eseguire lo scambio di messaggi criptati o rilevamento di eventuali manomissioni. Se non si dovessero rilevare problemi durante il tentativo di stabilire tale chiave, con alta probabilità essa si potrà ritenere segreta, anche se non c'è garanzia che si riesca a stabilire una chiave privata, nota a solo una delle parti.

Immaginiamo che Alice e Bob siano collegati da due canali pubblici: un canale classico bidirezionale e un canale quantistico unidirezionale. Il canale quantistico consente ad Alice di inviare a Bob una sequenza di singoli qubit. Per esempio, supponiamo che essi condividano una scorta di coppie *entangled* descritte dal vettore di stato $|\phi^+_{AB}\rangle$ di (6). Alice e Bob decidono di misurare σ_1 o σ_3 sui qubit in loro possesso con un criterio pseudo-casuale di probabilità $1/2$. Una volta eseguite le misurazioni, sia Alice che Bob annunciano sul canale classico quali osservabili abbiano misurato, ma non rivelano i risultati ottenuti. Per quei casi (circa la metà) in cui abbiano misurato i loro qubit lungo assi diversi, i loro risultati vengono scartati. Invece, nei casi in cui abbiano misurato lungo lo stesso asse, i loro risultati sono perfettamente correlati, ma mantenuti segreti. In questo modo stabiliscono una chiave condivisa, cioé una QKD.

Ci si chiede se questo protocollo sia davvero invulnerabile ad un subdolo attacco da parte di una terza parte Eve. In particolare, Eve potrebbe aver manomesso clandestinamente le coppie in qualche occasione nel passato. Il significa che le coppie che Alice e Bob possiedono potrebbero essere (a loro insaputa) non perfette, ma piuttosto *entangled* con i qubit in possesso di Eve. Se così fosse, Eve può attendere che Alice e Bob facciano i loro annunci pubblici e procedere a misurare i propri qubit, in modo tale da acquisire la massima informazione possibile dagli scambi tra i due. Di fatto il vettore di stato quantistico complessivo a tre con Eve è del tipo

$$\begin{aligned} |\Psi\rangle_{ABE} &= |00_{AB}\rangle\,|\phi_{0E}\rangle + |10_{AB}\rangle\,|\phi_{1E}\rangle \\ &+ |01_{AB}\rangle\,|\phi_{2E}\rangle + |11_{AB}\rangle\,|\phi_{3E}\rangle \end{aligned}$$

Si osservi, ora, che $|\phi^+_{AB}\rangle$ è autostato sia di $\sigma_1^A \otimes \sigma_1^B$ che di $\sigma_3^A \otimes \sigma_3^B$ con lo stesso autovalore 1, mentre si può verificare facilmente che $|\Psi\rangle_{ABE}$ a tre qubit non gode di questa proprietà. Quindi, con una misura di integrità di questo tipo il tentativo di spionaggio da parte di Eve può essere facilmente svelato.

Fin dalla sua concezione la QKD si è evoluta da una semplice curiosità teorica a un'industria prolifica all'avanguardia nelle tecnologie quantistiche. Oggigiorno si stanno costruendo reti QKD sia metropolitane [62], [63], [64], [65] che satellitari [66], [67], culminati nello sviluppo e nel lancio del satellite Micius dell'Accademia cinese delle Scienze, che ha dimostrato la realizzabilità collegamenti QKD intercontinentali [68].

I vari dispositivi e i protocolli offrono buone prestazioni in termini di stabilità e di tasso di qubit errati, ma ulteriori studi hanno evidenziato che una implementazione completamente sicura può essere ancora una sfida impegnativa.

Algoritmi Quantistici

Architettura di un Computer Quantistico

In tutti gli esempi precedentemente esposti si è potuto notare che ogni operazione a livello quantistico deve necessariamente essere accompagnato dall'uso di un canale classico di comunicazione. Questo tipo di struttura si deve riflettere nell'architettura di un computer quantistico, che assume una struttura ibrida nella quale i processori classici e quantistici funzionano in modalità *master/slave*. In questo caso, il codice classico effettua chiamate a un dispositivo esterno quantistico. Inoltre, il codice quantistico, scritto in un linguaggio adeguato, fornisce le istruzioni che devono essere eseguite dal processore quantistico. Una volta che le istruzioni inviate dal computer classico sono state eseguite nel processore quantistico, viene eseguita una misurazione e il risultato viene rinviato al processore classico. Tale processo può essere ripetuto più volte. Tale architettura viene chiamata QRAM [69].

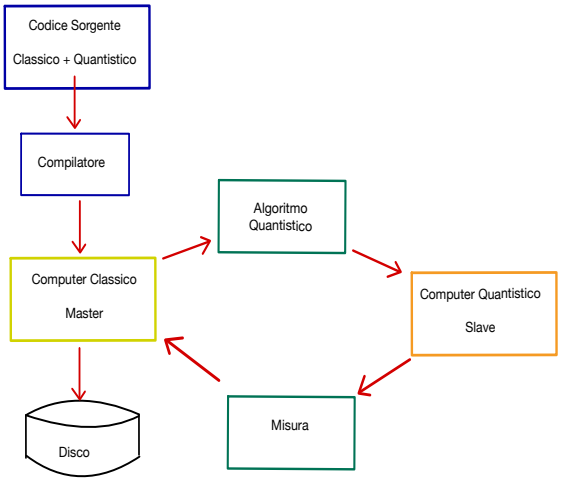


Figura 6: Architettura QRAM per un computer quantistico.

In questa architettura rimangono alcuni colli di bottiglia, quali l'eventualità di un possibile sovraccarico del trasferimento dati, fatto comune anche per i processori grafici e vettoriali. Oltre a queste limitazioni, il processore quantistico ne introduce potenzialmente altre: potrebbe, nello specifico, esserci un limite alla quantità di tempo a disposizione, durante la quale è possibile mantenere una sovrapposizione quantistica prima che si dissipi per interazioni con l'ambiente circostante. Questo è il già menzionato `tempo di decoerenza`, il quale rappresenta un vincolo senza analogo nella progettazione degli algoritmi classici.

Porte Logiche e Circuiti Quantistici

Passiamo ora ad analizzare le operazioni elementari di un computer quantistico. Come già discusso in precedenza, mentre un computer classico elabora bit, un computer quantistico elabora i qubit. Per l'elaborazione dei bit, un computer classico utilizza un insieme finito di porte logiche, cioè di funzioni booleane $f : \{0,1\}^n \to \{0,1\}^m$, dove n è il numero di bit in ingresso ed m quello dei bit in uscita. Ma nel caso quantistico questo non è un fatto scontato. In primo luogo, le porte logiche classiche sono tipicamente irreversibili (dissipative): a due ingressi corrisponde in genere una sola uscita, come ad esempio per la porta $AND : (a,b) \in \mathbb{Z}_2^2 \to a\,b \in \mathbb{Z}_2$. Ma nel manipolare più qubit non ci debbono essere dissipazioni, perderemmo rapidamente la coerenza degli stati. Solo manipolazioni reversibili sono quindi ammesse: cioé rappresentate da trasformazioni unitarie. Dal punto di vista classico la teoria booleana consente un calcolo reversibile a patto di utilizzare porte logiche con un numero uguale di ingressi e uscite, come ad esempio la porta NOT : $x \leftrightarrow \bar{x}$, oppure quella di Toffoli: $(x,\, y,\, z) \leftrightarrow (x,\, y,\, z \oplus x\; y)$, avendo indicato con $\oplus$ la somma tra interi mod 2. Si può dimostrare che, facendo uso della porta di Toffoli, ogni porta logica classica irreversibile a più ingressi può essere emulata da una reversibile, purché siano disponibili dei bit ausiliari.

In generale, nella teoria booleana si introduce il concetto di `circuito booleano`, con n ingressi e m uscite, definito come un grafo aciclico, monodirezionale e finito. In ogni vertice (o nodo) di tale grafo possiamo collocare una porta logica, tratta da un insieme finito di esse, ad eccezione di n nodi riservati agli input ed m agli output. Inoltre gli archi di connessione devono avere un qualche ordinamento, per distinguere tra diversi argomenti che puntano alla stessa funzione. Ad esempio, un circuito potrebbe contenere solo porte binarie AND e OR e porte unarie NOT, oppure essere interamente descritto da porte binarie NAND. A queste bisogna aggiunger INPUT e COPY, che consentono di assegnare i valori di ingresso e leggere i risultati. In definitiva, nel caso di circuiti booleani irreversibili è possibile far corrispondere dei circuiti equivalenti reversibili, cioé costruiti solo con porte reversibili. Per esempio un insieme siffatto è dato da: INPUT, NOT, Toffoli e COPY. Ma quello che preme sottolineare è che esso realizza un `insieme universale finito di porte logiche`, con le quali costruire ogni altra possibile funzione o circuito booleano.

Nel caso quantistico, le trasformazioni unitarie costituiscono, invece, un insieme infinito, operanti sul prototipo di spazio di Hilbert $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes n}$ qui adottato. Anche se può sembrare superfluo, la situazione ideale nella quale ci stiamo ponendo consente di far agire tutte le porte logiche quantistiche solo su stati puri producendo stati puri, rappresentabili in termini dei soli vettori di stato corrispondenti. Gli eventuali effetti di decoerenza non vengono inclusi a questo livello di trattazione e considerati in maniera perturbativa: si suppone che in un computer quantistico esista un tempo minimo di decoerenza, entro il

quale lo stato complessivo dei qubit rimane puro. Nella Figura 20 sono riportati i tempi di decoerenza T_1 medi tipici per diversi sistemi di calcolo quantistico reali. Come ultima avvertenza ai fini di alleggerire la notazione, le porte logiche verranno indicate con lettere maiuscole, e non in grassetto, per quanto rappresentino sempre operatori unitari. In linea di principio, una sola di esse realizzerebbe il passaggio dallo stato iniziale a quello finale, simbolicamente

$$|i_1 i_2 i_3 \dots i_n\rangle \xrightarrow{U} |i'_1 i'_2 i'_3 \dots i'_n\rangle$$

con $i_j, i'_{j'} = 0, 1$. Ma questo vorrebbe dire costruire un apparato apposito per ogni singolo calcolo, il che non porterebbe nessun vantaggio!

L'idea è che la generica trasformazione unitaria su un n-qubit si possa costruire, almeno in forma approssimata, combinando un numero finito di trasformazioni unitarie standard. A loro volta, ognuna di esse agisce su un sottoinsieme di qubit di fissato numero, relativamente piccolo rispetto ad n. Con questa idea si propone di sostituire le porte logiche classiche con delle porte logiche quantistiche. Esse debbono costituire un `insieme universale` finito, nel senso che, a meno di casi eccezionali, ogni trasformazione unitaria si possa scrivere con un circuito, analogo a un circuito booleano, nei cui nodi sono collocati gli elementi dell'ipotetico insieme universale. Ovviamente indipendentemente dall'implementazione fisica specifica, ogni porta compie sempre la stessa operazione logica.

Per perseguire questi scopi si possono utilizzare vari teoremi, il primo dei quali è quello detto di Solovay-Kitaev per le trasformazioni $U \in SU(2)$, cioé su 1-qubit. Usando la compattezza del gruppo, si mostra che 1) esiste almeno una famiglia finita G di suoi elementi che generano sotto-insiemi densi in esso, 2) che per qualsiasi porta U è possibile trovare una sua approssimazione U_ϵ, con precisione ϵ in norma traccia, utilizzando al più $O(\log^4(1/\epsilon))$ elementi tratti da G [70]. Questo teorema ci consente di costruire una qualunque trasformazione su un qubit a partire, per esempio, dall'insieme finito di porte costituito come segue.

Le tre porte di Pauli

$$X = \sigma_1, Y = \sigma_2, Z = \sigma_3,$$

tra le quali X è l'analoga della porta NOT e le altre cambiano le fasi relative tra gli stati di base. La porta di Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{8}$$

la cui azione sugli elementi della base computazionale è data da

$$|0\rangle \text{ —}\boxed{H}\text{— } \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \; |1\rangle \text{ —}\boxed{H}\text{— } \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Infine si aggiungono le porte di fase

$$S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{\imath \frac{\pi}{2}} \end{pmatrix} = \sqrt{Z},$$

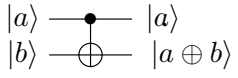
e

$$T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{\imath \frac{\pi}{4}} \end{pmatrix} = \sqrt{S}.$$

Fatto questo, si deve passare alla costruzione di trasformazioni unitarie di dimensioni superiori. Un altro teorema ci viene in soccorso: esso afferma che, a meno di un insieme di misura nulla in norma traccia, una trasformazione unitaria di n-qubit può essere costruita da porte a due qubit. Questo risultato è particolarmente importante, perché ci consente di approssimare ogni possibile trasformazione solo con porte a 1 qubit e a 2 qubit. Non c'è la necessità di coinvolgere porte con 3 qubit, analoghe a quella di Toffoli nel caso classico. Da un punto di vista fisico esse realizzano lo scopo di porre in *entanglement* i due qubit coinvolti. Procedendo ad accoppiamenti di questo tipo, l'intero insieme di qubit può essere correlato. In realtà, si può far vedere che basta un solo tipo di porta a 2-qubit. Ad esempio la porta NOT controllata cNOT, definita da

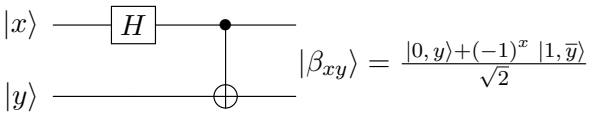
$$c\text{NOT} = |0\rangle\langle 0|_c \, \mathbf{1}_t + |1\rangle\langle 1|_c \, X_t,$$

dove i pedici indicano rispettivamente il qubit di controllo c e t per *target*. Una sua rappresentazione grafica è



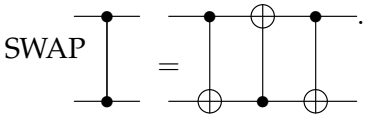
cNOT consente di realizzare la base degli stati di Bell, tutti massimalmente *entangled*, secondo la

relazione circuitale



nella base computazionale $\{\,|0\rangle,\ |1\rangle\}$.

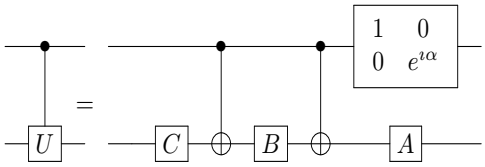
Per il ruolo cruciale che questa porta svolge nello sviluppo dell'idea di computazione quantistica, essa è stata anche la prima ad essere considerata da un punto di vista implementativo ad opera di Cirac e Zoller [71], che proposero l'utilizzo di una trappola ionica. Altro aspetto importante è che essa consente di realizzare, in combinazione con porte a 1-qubit, ogni porta logica a 2-qubit. Ad esempio, la porta SWAP che esegue la permutazione di c con t, secondo l'equivalenza circuitale



Così anche per ogni porta controllata

$$cU = |0\rangle\langle 0\,|_c \mathbf{1}_t + |1\rangle\langle 1\,|_c\, U_t\ ,$$

che, usando $U = e^{\imath\,\alpha} AXBXC$ con $ABC = \mathbf{1}$, in forma circuitale è espressa come:



Procedendo in maniera analoga si possono costruire porte logiche per ogni numero di qubit. Ad esempio l'analoga della porta Toffoli a 3 qubit

$$\begin{aligned} cc\text{NOT} &= (\mathbf{1}_{c_1}\mathbf{1}_{c_2} - |1\rangle\langle 1\,|_{c_1}\,|1\rangle\langle 1\,|_{c_2})\,\mathbf{1}_t \\ &+ |1\rangle\langle 1\,|_{c_1}\,|1\rangle\langle 1\,|_{c_2} X_t \end{aligned}$$

si rappresenta con il circuito di porte a 1 e 2 qubit presentato dalla Fig. 7.

In definitiva, estendendo il precedente teorema di Solovay-Kitaev per elementi $U \in U\,(2^n)$, è possibile dimostrare che, usando un circuito quantistico costituito da un insieme universale di porte (chiuso rispetto all'inversione), si può realizzare una trasformazione approssimata U_ϵ con un numero di risorse computazionali che

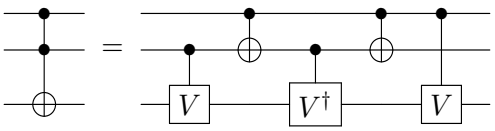


Figura 7: Rappresentazione circuitale della porta a 3 qubit ccNOT in termini di porte a 1- e 2-qubit. La porta indicata con V rappresenta l'operatore $V = (1-\imath)\,(\mathbf{1}+\imath\,X)\,/2$.

cresce al più come una potenza di $\log_2 1/\epsilon$. Il che ci rende confidenti che in linea di principio sia possibile calcolare concretamente, con una successione ordinata di operazioni tipiche, implementabili fisicamente con un certo numero fisso di dispositivi scelti in partenza, una data funzione booleana. Intuitivamente, l'utilizzo efficiente di un algoritmo quantistico è possibile perché qualsiasi circuito può essere costruito da un insieme universale di porte logiche. Ma, essendo vero che esistono operazioni unitarie non approssimabili efficientemente (si veda la discussione precedente), è possibile immaginare sistemi quantistici che non possono essere simulati efficientemente su un computer quantistico. Forse tali sistemi non sono realizzati in Natura, altrimenti saremmo in grado di sfruttarli per elaborare informazioni oltre il modello del circuito quantistico.

L'ultimo passaggio che ci rimane è leggere il risultato del calcolo, che consiste in una misurazione ortogonale di tutti i qubit (o un sottoinsieme di essi), proiettando ciascun qubit sulla base $\{\,|0\rangle,\ |1\rangle\}$. L'esito di questa misurazione è il risultato del calcolo, ma ovviamente esso compare con una certa probabilità, la cui distribuzione statistica si può calcolare conoscendo il circuito. In definitiva il risultato di una computazione quantistica ha un valore probabilistico, non è certo nel senso di un algoritmo classico sequenziale. Pertanto, in generale, si dovrà ripetere il calcolo più volte, per essere confidenti che si sia ottenuto il risultato corretto. In alternativa, si potrebbe procedere ad una verifica a posteriori del risultato ottenuto, almeno per certe classi di problemi.

Con queste premesse, oltre alle applicazioni indicate nel precedente paragrafo, si possono riconoscere e sviluppare alcune aree algoritmiche generali, per le quali il modello quantistico sembra offrire vantaggi sostanziali rispetto alle

alternative classiche più conosciute.

- `Trasformata quantistica di Fourier e Stima della Fase`
  La QFT è un algoritmo di generale utilizzo che consente di calcolare la trasformata di Fourier di una funzione in maniera più efficiente di quanto non faccia il corrispondente classico *Fast Fourier Transform*. Dettagli su questo punto saranno discussi in una prossima Sezione. Anche l'algoritmo della Stima della Fase è una sorta di *subroutine*, in quanto può essere applicato in tutti i casi si debbano valutare gli autovalori di operatori unitari.

- `Amplificazione di ampiezza`
  Questa procedura consente di aumentare (amplificare) il peso associato a uno stato desiderato all'interno di una sovrapposizione quantistica, in modo che sia più probabile che esso venga misurato. L'amplificazione dell'ampiezza può essere utilizzata come strumento generico per trovare in modo efficiente la soluzione per un'ampia varietà di problemi di ricerca e ottimizzazione. Una discussione di questa tecnica verrà illustrata nella sezione riguardante l'algoritmo di Grover.

- `Quantum Random Walk` (QRW)
  Essa può essere applicata per risolvere un'ampia varietà di problemi di stima statistica in modo più efficiente di quanto non possa fare l'analogo classico. Un'introduzione molto dettagliata all'uso QRW in informatica può essere trovata in [72].

- `Simulazione di sistemi fisici`
  Non dovrebbe sorprendere che i fenomeni quantistici possano essere simulati in modo più efficiente sull'*hardware* quantistico di quanto sia possibile classicamente, che si è già detto motivò Feynman. Tra i diversi approcci alle simulazioni, negli ultimi anni si è sviluppato un grande interesse verso gli algoritmi quantistici adiabatici, cioè che si basano sul teorema delle perturbazioni adiabatiche [73]. Essi sono stati utilizzati per risolvere problemi impegnativi in bioinformatica, come la conformazione e il ripiegamento delle proteine [74], ed in Fisica del nucleo. [23, 75]. Sebbene queste applicazioni promettano progressi rivoluzionari in una varietà di settori scientifici e ingegneristici, non è chiaro fino a che punto una simulazione possa rappresentare fedelmente il comportamento di un sistema reale esteso, tornando così alle osservazioni di [26].

- `Correzione degli errori quantistici`
  La QEC è analoga alle classiche tecniche di correzione degli errori, tranne per il fatto che può riconoscere e correggere errori di qubit, al contrario della sola negazione di bit [36]. Le sue applicazioni risiedono nell'implementazione dell'architettura complessiva del sistema di calcolo (sia quantistica che classica di controllo), anche con la progettazione di algoritmi ibridi.

Non avendo lo scopo di trattare in dettaglio tutte le menzionate vaste aree di ricerca ed applicazioni, si rimanda il lettore alla manualistica già citata [36]-[43], ad altri articoli presenti su **Ithaca** e alla letteratura specialistica. A titolo esemplificativo, qui si riportano le idee di fondo di alcune delle tecniche citate.

Simulazioni Quantistiche

Come sappiamo da molto tempo ormai, una delle applicazioni pratiche più importanti del calcolo è la simulazione di sistemi fisici, sia a scopo progettuale/ingegneristico, che di scoperta di base là dove la comprensione e l'immaginazione umana non riesce ancora spingersi. Il cuore delle simulazioni è la ricerca di soluzioni alle equazioni che esprimono le leggi dinamiche di un dato sistema fisico. Le soluzioni vengono solitamente ottenute approssimando le equazioni ed eventuali altre informazioni, quali condizioni iniziali o al bordo o vincoli al sistema, tramite una loro rappresentazione digitale. Intrinseca alla procedura di discretizzazione è la comparsa di un margine di errore, che cresce per propagazione ai passi successivi di una iterazione algoritmica. Perciò è importante che l'errore in questa procedura sia limitato e che non cresca più velocemente di una piccola potenza del numero di iterazioni. Inoltre, non tutti i sistemi dinamici possono essere simulati efficientemente: generalmente, solo quei sistemi per i quali si conosca

l'esistenza della soluzione globale, per ogni dato iniziale.

Focalizzandosi sui sistemi quantistici isolati, in accordo al postulato di evoluzione riportato in Appendice, il problema centrale consiste nel risolvere l'equazione di Schrödinger per la matrice di stato $\boldsymbol{\rho}$. Questo comporta che per un sistema di n qubit si debba determinare l'evoluzione temporale di $4^n - 1$ componenti reali (vedi l'Eq. (3)). Quindi la difficoltà base consiste nella crescita esponenziale nel numero di equazioni che si debbono risolvere.

Si sa che esistono molti importanti sistemi quantistici per i quali la simulazione con algoritmi classici è computazionalmente proibitiva, tra i quali il già citato modello di Heisenberg/Ising (vedi Fig. 2) o il più complesso modello di Hubbard. Tali modelli sono utili nello studio della superconduttività, del magnetismo e di molte altre proprietà fisiche dei materiali. Ad essi si affiancano modelli più sofisticati, come la cromodinamica quantistica (QCD), i quali possono essere utilizzati per calcolare le proprietà dei costituenti elementari dell'Universo. Pertanto in Fisica si è ben presto compreso il potenziale della nuova tecnologia della computazione quantistica, intraprendendo l'esplorazione di semplici modelli nucleari [76],[77], modellando la fisica del neutrino [78] e la preparazione degli stati di input [79]. Tuttavia, l'analisi fatta in [80] suggerisce che calcoli accurati delle strutture molecolari possono essere effettuati con certi algoritmi classici efficienti, nel senso che hanno un costo computazionale crescente con una potenza (e non esponenzialmente) delle dimensioni del sistema. Perciò i computer quantistici non necessariamente costituiscono una alternativa vantaggiosa. Tuttavia, rimane il fatto che la simulazione di processi dinamici in tempo reale ponga ancora sfide formidabili all'informatica classica, e molti sforzi sono stati dedicati ad esplorare le proposte provenienti da quella quantistica [81]. Una rassegna sinottica delle varie idee e simulazioni riguardante questo settore di ricerca si può reperire in [82].

La situazione più semplice da considerare è costituita dalla simulazione [83] dell'equazione di Schrödinger mono-dimensionale, nell' intervallo $-d \leq x \leq d$, per la funzione d'onda $|\psi(t)\rangle$ di una particella soggetta ad potenziale, definita dall'operatore Hamiltoniano

$$\mathbf{H} = \frac{\mathbf{p}_x^2}{2m} + V(\mathbf{x}).$$

In rappresentazione di posizione significa che la funzione d'onda $\psi(x,t) = \langle x\,|\psi(t)\rangle$, con condizioni al bordo $\psi(-d,t) = \psi(d,t) = 0$ e condizione iniziale $\psi(x,0) = \psi_0(x)$, è soggetta alla arcinota equazione di Schrödinger

$$\imath\frac{\partial}{\partial t}\psi(x,t) = \left[-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x)\right]\psi(x,t).$$

La soluzione formale del problema è data dall'azione unitaria dell'operatore di evoluzione

$$|\psi(t)\rangle = e^{-\frac{\imath}{\hbar}\mathbf{H}t}\,|\psi(0)\rangle.$$

Come di consueto, per ottenere una soluzione numerica si procede discretizzando lo spazio ed il tempo. La regione del moto viene suddivisa in 2^n sottointervalli di lunghezza $\Delta = d/2^{n-1}$, dove n è stabilito dalle risorse computazionali disponibili. Ora, all'i-esimo intervallo è associato il vettore della base computazionale $|i\rangle$ $(i = 0, \ldots, 2^n - 1)$ di un sistema di n qubit. Si è così realizzata una approssimazione dello spazio di Hilbert originario, ∞-dimensionale, a $\mathbb{C}^{2^n}$ costituito da funzioni d'onda discretizzate della forma

$$\psi_d(t) = C\sum_{i=0}^{2^n-1}\psi(x_i,t)\;|i\rangle,$$

con

$$x_i = -d + (i + \tfrac{1}{2})\,\Delta,$$

dove C è la costante di normalizzazione. Nel contempo l'Hamiltoniano originario del sistema continuo assume implicitamente la forma discretizzata $\mathbf{H}_d = \sum_i^{2^n-1}\mathbf{H}_i$. Come noto gli operatori momento e posizione sono soggetti alla disuguaglianza di Heisenberg, ovvero $\mathbf{p}_x$ e $\mathbf{x}$ sono osservabili incompatibili. Questo si riflette nel fatto che $[\mathbf{H}_i, \mathbf{H}_j] \neq 0$. A sua volta per calcolare l'operatore di evoluzione approssimato non può valere una espressione ingenua, per esempio

$$e^{-\frac{\imath}{\hbar}\mathbf{H}_d t} \neq \prod_{i=0}^{2^n-1} e^{-\frac{\imath}{\hbar}\mathbf{H}_i t}.$$

Qui viene in soccorso la cosiddetta formula di Trotter per una coppia $\mathbf{A}, \mathbf{B}$ di operatori

hermitiani:

$$\lim_{k\to\infty} \left(e^{\imath \mathbf{A} t/k}\, e^{\imath \mathbf{B} t/k} \right)^k = e^{\imath(\mathbf{A}+\mathbf{B})t}$$

che, a meno di contributi di secondo ordine nel passo temporale Δt, consente di scrivere

$$\begin{aligned} e^{-\frac{\imath}{\hbar}\left(\frac{\mathbf{p}_x^2}{2m}+V(\mathbf{x})\right)\Delta t} \quad &\approx e^{-\frac{\imath}{\hbar}\frac{\mathbf{p}_x^2}{2m}\Delta t} e^{-\frac{\imath}{\hbar}V(\mathbf{x})\Delta t} = \\ U_F^\dagger \quad e^{-\frac{\imath}{\hbar}\frac{\mathbf{p}_x^2}{2m}\Delta t} \quad &U_F \;\; e^{-\frac{\imath}{\hbar}V(\mathbf{x})\Delta t}, \end{aligned}$$

dove nel secondo passaggio si è usata la rappresentazione di posizione e U_F rappresenta l'operatore unitario Trasformata di Fourier Quantistica, che sarà discussa in dettaglio in una successiva sezione. Di fatto essa rappresenta l'analogo sullo spazio dei qubit dell'abituale Trasformata di Fourier, la quale produce il cambiamento dalla base di posizione $\{|x\rangle\}$ in quella di momento $\{|p\rangle\}$.

Gli altri operatori presenti agiscono diagonalmente sugli stati di qubit, cioé come $e^{-\frac{\imath}{\hbar}V(\mathbf{x})\Delta t}|i\rangle = e^{-\frac{\imath}{\hbar}V(x_i)\Delta t}|i\rangle$ e analogamente per l'operatore nello spazio dei momenti.

Tutti questi operatori possono essere implementati per mezzo di 2^{n-1} porte di fase controllate $n-1$ volte, descritte nelle precedenti sezioni. Da questo punto di vista il metodo risulta ancora inefficiente, perché le risorse computazionali necessarie crescono esponenzialmente con la precisione desiderata nel calcolo. D'altra parte lo stato è descritto ed evoluto in parallelo con solo n qubit, piuttosto che dai 2^n valori della funzione d'onda. Per potenziali non troppo complessi, i primi studi hanno dimostrato che un simulatore quantistico con una decina di qubit è abbastanza robusto contro gli errori, ma per eseguire il calcolo occorrerebbero $O(10^4)$ porte quantistiche elementari, che sono ancora una sfida per un vero computer quantistico. Sviluppi in quest'area di ricerca sono ancora attuali [84, 85].

La lezione appresa dalla precedente procedura suggerisce che esiste un ampio spettro di tecniche quantistiche per lo studio di equazioni e modelli di Fisica, ma che esse stesse vanno studiate per coglierne gli aspetti più vantaggiosi per gli scopi ai quali sono destinate. Questo ha portato ad una nuova classe di algoritmi ibridi.

Per citare un esempio sappiamo che per trovare l'autovalore di un Hamiltoniano, potremmo usare l'algoritmo di `Stima della Fase Quantistica`, che analizzeremo nel seguito. In linea di principio con tale metodo si potrebbe ottenere l'intero spettro degli autovalori e i corrispondenti autostati. Inoltre, per i problemi di Materia Condensata o di Teoria dei Campi, nella maggior parte dei casi siamo interessati principalmente allo stato fondamentale. Tuttavia, per un'Hamiltoniano generico l'implementazione di una porta U controllata potrebbe non essere semplice. Per problemi realistici, la stima della fase quantistica richiede una grande profondità del circuito, il che implica la necessità di un lungo tempo di coerenza dei qubit, non disponibile con la tecnologia della NISQ era.

Per superare queste limitazioni, è stato recentemente introdotto il metodo `Variazionale agli autovalori quantistici` (VQES) [86, 87]. Esso è un algoritmo ibrido, la cui idea di base è quella di sfruttare i vantaggi sia dei computer quantistici che di quelli classici, facendo risolvere al computer quantistico la parte di calcolo che esso può eseguire efficientemente, mentre si assegnano al computer classico compiti risolvibili con algoritmi di per sè efficienti.

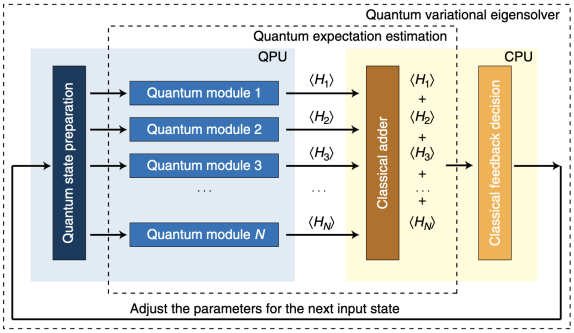


Figura 8: Diagramma di flusso dell'implementazione del risolutore di autovalori VQES, che utilizza un circuito ibrido classico-quantistico. La figura è adottata da [88]

In un contesto di Fisica Classica è noto che le simulazioni di fluidodinamica richiedono le nostre più potenti risorse computazionali e i computer quantistici offrono l'opportunità di accelerare gli algoritmi tradizionali. È stato mostrato [89, 90] che i metodi numerici su mesoscala, del tipo `Automa di Gas Reticolare` (LGA) o il metodo del `Reticolo di Boltzmann` (LBM), possono essere eseguiti con algoritmi quantistici efficienti. L'algoritmo è stato validato simulando

due equazioni alle derivate parziali (PDE) canoniche: l'equazione di `Diffusione` e quella di Burgers (un analogo semplificato dell'equazione di Navier-Stokes, comunque nonlineare) con diversi simulatori quantistici. È naturale in questo

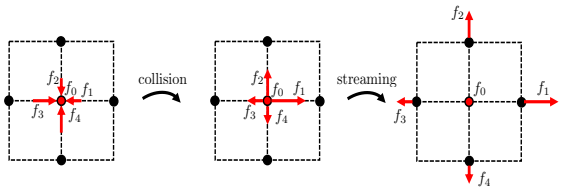


Figura 9: Le principali operazioni consentite su un Gas Reticolare di Boltzmann: collisione flusso. Esse possono essere rappresentate in un circuito quantistico che agisce su un insieme di qubit. La figura è ripresa da [89]

contesto cercare di risolvere anche equazioni differenziali classiche con metodi quantistici, il che ha prodotto una messe di risultati ancora da approfondire, per quanto riguarda la loro efficienza e robustezza rispetto agli errori [91, 92]. D'altro canto si è già citato in precedenza che si stanno sviluppando tecnologie di calcolo di multi-fisica basati su queste idee.

L'algoritmo di Deutsch

Il prototipo ed anche il più semplice algoritmo quantistico è quello di Deutsch [93], che consiste nel risolvere il seguente `problema decisionale`: data una funzione booleana

$$f \,:\, \{0,1\} \to \{0,1\}$$

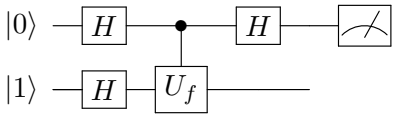
stabilire se essa sia costante o **bilanciata**. Con questo termine si intende dire che la funzione assume i valori 0 o 1 in uguale numerosità. È chiaro che nel caso delle classe delle funzioni considerate la risposta è immediata, perché esistono in totale quattro di esse :

$$f_1(x) \equiv 1, f_2(x) \equiv 0, f_3(x) = x, f_4(x) = \overline{x} \ ,$$

cioé due costanti e due bilanciate. Tuttavia, volendo esercitarsi a sviluppare un algoritmo apposito si deve inventare una opportuna porta logica

$$U_f \,:\, |x\rangle\,|y\rangle \;\to\; |x\rangle\,|y \oplus f(x)\rangle \ , \qquad (9)$$

detta **oracolo**, perché fornisce una risposta al problema senza che entri in una successione di verifiche sui singoli argomenti x. Per vedere come agisce l'algoritmo, si osservi in primo luogo che dalla sua definizione l'oracolo dipende dalla funzione f e la sua azione, su una coppia di qubit, produce uno stato da essa dipendente. Precisamente, realizzando il seguente circuito



lo stato inizialmente separato evolverà in un altro, anch'esso separato, secondo i seguenti passaggi

$$\begin{aligned}
& |0\rangle\,|1\rangle \overset{H\otimes H}{\to} \tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) \\
\overset{U_f}{\to}\ & \tfrac{1}{2}\left(|0\rangle\,|f(0)\rangle - |0\rangle\,|\overline{f(0)}\rangle + |1\rangle\,|f(1)\rangle - |1\rangle\,|\overline{f(1)}\rangle\right) = \\
& \tfrac{1}{2}\left((-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle\right)\left(|0\rangle - |1\rangle\right) \\
\overset{H}{\to}\ & \tfrac{1}{2}\left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \right. \\
& \left.\left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right]\ \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).
\end{aligned}$$

Si osservi che i valori della funzione f sono stati calcolati in parallelo su tutti gli argomenti $x \in \{0,1\}$ e trasferiti nelle fasi delle ampiezze del vettore di stato nel primo registro [1].

Procedendo ora ad effettuare una misurazione sul primo qubit, evidenziato dal simbolo di misura nella rappresentazione circuitale, si ottengono le due alternative

$$\begin{cases} |0\rangle & \Rightarrow f(0) = f(1) \quad f \texttt{ costante} \\ |1\rangle & \Rightarrow f(0) = \overline{f(1)} \quad f \texttt{ bilanciata} \end{cases} ,$$

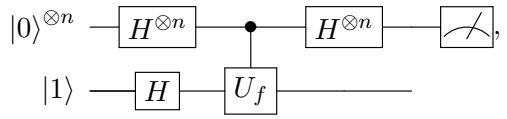
il che fornisce una risposta univoca al problema posto.

Il punto da sottolineare qui è che per ottenere questo risultato è stato sufficiente applicare una sola volta l'algoritmo quantistico, mentre classicamente avremmo dovuto calcolare f due volte. Questo dà un senso al termine oracolo: il calcolo della funzione f è effettuato in parallelo su tutti i possibili input descritti dal registro dei qubit di ingresso.

[1] Per registro si intende un gruppo di qubit i cui stati iniziale e finale sono separati da quelli dei restanti qubit. In questo caso il primo qubit da sinistra verso destra nella notazione di Dirac, o dall'alto verso il basso nella notazione circuitale.

Variazioni sul tema

Il vantaggio computazionale è modesto nell'esempio di Deutsch, ma si può enfatizzare nel caso si debba decidere se una funzione booleana sia costante o bilanciata su $\mathbb{Z}_2^n$, ovvero $f : \{0,1\}^n \to \{0,1\}$. Il corrispondente algoritmo di Deutsch - Josza, rappresentato dal circuito



produce uno stato finale (prima della misura) della forma

$$\frac{1}{2^n}\sum_{x,\,y=0}^{2^n-1}(-1)^{f(x)}\,(-1)^{x\cdot y}\,|y\rangle\otimes\frac{(\,|0\rangle-|1\rangle)}{\sqrt{2}}\quad,$$

con

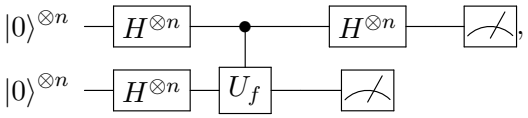
$$x\cdot y=(x_1\,y_1)\oplus(x_2\,y_2)\oplus\cdots\oplus(x_n\,y_n)\quad.$$

Come nel caso precedente, i valori della funzione f su $\mathbb{Z}_2^n$ simultaneamente calcolati vanno a definire le fasi dei coefficienti di tutti gli elementi del primo registro di qubit, inizialmente posti a $|0\rangle^{\otimes n} = |0\rangle$. Nello stato finale essi potrebbero assumere tutti i possibili valori della base computazionale $|y\rangle = |0\rangle, \ldots, |2^n-1\rangle$. Se a questo punto si procedesse alla misura di tale registro, potrebbe accadere di ottenere $y = 0$. Ma, da un'analisi delle ampiezze, questo si verifica solo se la funzione f è costante, mentre non può ottenersi nel caso fosse bilanciata, perché in questo caso i contributi alla sua ampiezza sarebbero in egual numero ± 1.

Osserviamo ora che in un algoritmo classico, verificato che per due valori diversi dell'argomento una funzione f assume valori distinti, se ne conclude con certezza che essa non è costante. Ma per verificare che la funzione sia effettivamente costante, dovremo calcolarla per tutti i 2^n valori dell'argomento. Diversamente, il calcolo quantistico fornisce una risposta definita in un solo passaggio. In questo senso (se pretendiamo la certezza assoluta) potremmo dichiarare di essere di fronte ad un'`accelerazione esponenziale` della procedura quantistica.

In realtà la questione è più sottile, perché è possibile trovare algoritmi classici probabilistici, che risolvono questo problema con probabilità $1-\epsilon$ con un numero di verifiche $k = O(-\log_2 \epsilon)$, cioé di complessità crescente a potenza con il numero di input in ingresso (classe BPP). Il problema non è in effetti veramente difficile e l'algoritmo quantistico fornisce solo un incremento relativo in velocità di computazione.

Sulla linea concettuale di Deutsch si sono sviluppati algoritmi di maggiore complessità computazionale. Qui basti citare quello di Simon [94], che consiste nel determinare il periodo $a \in \{0,1\}^n$ di una funzione booleana $f_a : \{0,1\}^n = \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Da un punto di vista classico questo è un problema NP, cioé difficile, ma consideriamo il circuito quantistico



dove si usa l'oracolo (9) secondo la relazione

$$\left[\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\right]|0\rangle\overset{U_f}{\to}\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\otimes|f(x)\rangle.$$

Applicandolo un numero sufficiente di volte ed effettuando la seguente misura sul primo registro, il problema si riduce a risolvere un sistema lineare omogeneo di n equazioni per l'incognita a. Quindi abbiamo trovato un esempio in cui, trovato un particolare oracolo quantistico, possiamo risolvere un problema in tempo polinomiale sfruttando il parallelismo quantistico, mentre è necessario un tempo esponenziale con algoritmi classici. In termini di classi di complessità computazionale si è dimostrato che BQP $\neq$ BPP.

La Trasformata di Fourier Quantistica e la Stima di Fase

La QFT

L'algoritmo di Simon offre un ottimo esempio di tecnica basata sull'`amplificazione di ampiezza` per ridurre un problema effettivamente difficile. Allora ci si può chiedere se sia possibile formulare analoghi algoritmi anche per problemi più complessi, quali la determinazione del periodo di funzioni definite su $\mathbb{Z}_{2^n}$. In questo caso, l'algoritmo classico ben noto, ed ampiamente utilizzato in tutti i domini della Scienza, è la Trasformata di Fourier, nella sua versione discreta, nota come `Fast Fourier Transform` (FFT). Ora, l'i-

dea chiave è che la trasformata di Fourier può essere valutata anche da un circuito quantistico efficiente [95, 96, 97]. La trasformata quantistica di Fourier (QFT) sfrutta la potenza del parallelismo quantistico per ottenere un'accelerazione esponenziale della FFT.

La QFT è definita dalla trasformazione unitaria

$$U_F \left|x\right\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \exp\left[2\pi\imath x\, y/2^n\right] \left|y\right\rangle, \qquad (10)$$

per cui agisce su un generico vettore di stato secondo la regola

$$U_F \sum_x a\left(x\right)\, \left|x\right\rangle = \sum_x A\left(x\right)\, \left|x\right\rangle,$$

dove

$$A\left(x\right) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a\left(k\right)\, \exp\left(2\pi\imath \frac{k\, x}{N}\right) \quad .$$

Esattamente producendo la trasformata di Fourier di una data funzione $a\left(x\right)$. Inoltre, ricordando la corrispondenza tra numeri in notazione binaria ed elementi della base computazionale data da

$$x = \sum_{k=0}^{n} \xi_k\, 2^k \;\leftrightarrow\; \left|x\right\rangle = \left|\xi_n, \ldots, \xi_1, \xi_0\right\rangle \;,$$

e introducendo la notazione abbreviata

$$\bigotimes_{\ell=0}^{n} \left|i_\ell\right\rangle = \left|i_0\right\rangle \otimes \left|i_1\right\rangle \otimes \cdots \otimes \left|i_n\right\rangle \quad ,$$

l'azione di U_F può essere espressa anche nella forma

$$U_F \left|x\right\rangle = \frac{1}{2^{n/2}} \bigotimes_{\ell=0}^{n} \left[\left|0\right\rangle + e^{2\pi\,\imath \sum_{k=0}^{\ell-1} \frac{\xi_k}{2^{\ell-k}}} \left|1\right\rangle\right].$$

In altre parole la QFT porta ogni stato della base computazionale in uno stato non *entangled* di n qubit. Non sembra quindi un impresa così difficile implementarlo.

La QFT per 1-qubit coincide con la porta di Hadamard H, definita in (8). Per calcolare la QFT per un sistema multi-qubit si può adottare una procedura ricorsiva, già nota per la FFT, della forma

$$\begin{aligned} U_F^{(k)} \;=\; & \left(H \otimes \mathbf{1}_{2^{k-1}}\right) \\ & \left(\left|0\right\rangle\!\left\langle 0\right| \otimes \mathbf{1}_{2^{k-1}} + \left|1\right\rangle\!\left\langle 1\right| \otimes D^{(k-1)}\right) \\ & \left(\mathbf{1}_2 \otimes U_F^{(k-1)}\right)\, R^{(k)}, \end{aligned}$$

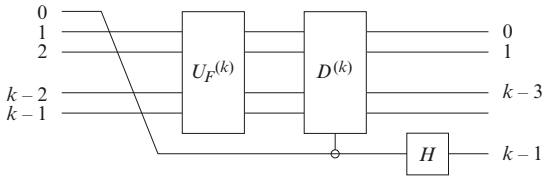
dove sono ora coinvolti gli operatori

$$D^{(k)} = D^{(k-1)} \otimes \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi\imath}{2^{k+1}}\right) \end{pmatrix},$$

e

$$R^{(k)} = \sum_{i=0}^{2^k-1} \left(\left|i\right\rangle\!\left\langle 2i\right| + \left|i+2^k\right\rangle\!\left\langle 2i+1\right|\right) \quad .$$

Quest'ultimo operatore è interpretabile come una successione di permutazioni tra qubit e, pertanto, si può implementare con delle porte SWAP. Il corrispondente circuito quantistico è



In conclusione la QFT può essere implementata con un numero di risorse computazionali $O(n^2)$, contro le $O(n2^n)$ richieste da FFT. Questo naturalmente non può che aumentare significativamente l'impatto sulle capacità di calcolo in tutte le innumerevoli applicazioni in cui la Trasformata di Fourier svolga un ruolo importante.

La Stima della Fase

Consideriamo ora il problema della `Stima della Fase` discusso in [97]. In generale, gli autovalori di un operatore unitario sono della forma $e^{2\pi\imath\phi}$. A meno che esso non sia anche hermitiano, come gli operatori di Pauli, tali autovalori non sono direttamente misurabili. Tuttavia, si può considerare il seguente circuito dove $\left|u\right\rangle$ denota il corrispondente autovettore di U e $\left|\psi\right\rangle = \cos\left(\pi\,\phi\right)\left|0\right\rangle + \imath\, \sin\left(\pi\,\phi\right)\left|1\right\rangle$. Come abbiamo discusso nel problema di Deutsch, questa procedura distingue con certezza tra $\phi = \pm 1$, ma per altri suoi valori si ha una minore confidenza

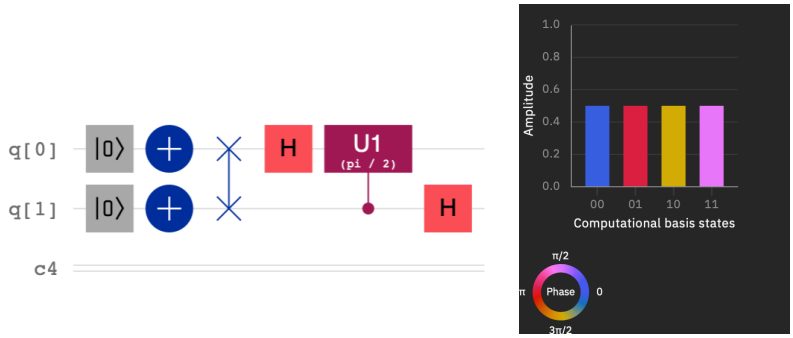


Figura 10: La $U_F^{(2)}$ applicata allo stato $|\bar{0},\bar{0}\rangle = |1,1\rangle$. Nel pannello a destra si riportano le ampiezze dei vettori della base computazionale, di modulo $1/2$, e le corrispondenti fasi. La porta H a sinistra svolge il ruolo di $QFT^{(1)}$. La porta NOT è simboleggiata da $\oplus$ in blu.

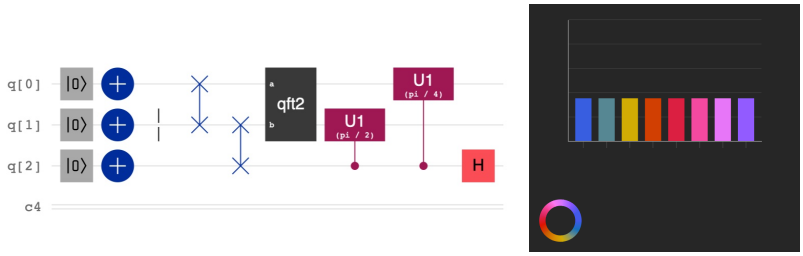
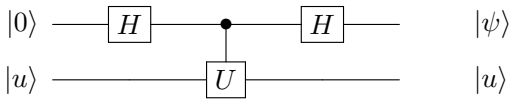


Figura 11: The $QFT^{(3)}$ applicata $|\bar{0},\bar{0},\bar{0}\rangle = |111\rangle$. Nel pannello a destra si riportano le ampiezze dei vettori della base computazionale, di modulo $2^{-3/2}$, e le corrispondenti fasi. Si osservi che essa è costruita ricorsivamente su $QFT^{(2)}$. La porta NOT è simboleggiata da $\oplus$ in blu.



statistica e sarà necessario ripetere molte volte il calcolo. C'è una maniera per evitarlo.

Supponiamo di avere un registro di n qubit e si ricordi che se $|u\rangle$ è un autovettore di un operatore U unitario, lo è anche di U^{2^j} con autovalore $e^{2^j\, 2\pi\imath\phi}$. Ora si implementa il circuito tracciato in Fig. 12 Nei primi n-qubit di controllo viene

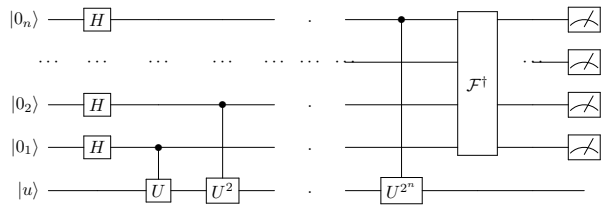


Figura 12:

generata la sovrapposizione

$$H^{\otimes n}\,|0\rangle^{\otimes n} = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle \quad .$$

A loro volta, ogni $c-U^{2^j}$ produce il contributo

$$\begin{aligned}&\frac{1}{\sqrt{2}}\left(|0_j\rangle + |1_j\rangle\right)|u\rangle\\ \xrightarrow{c-U^{2^j}}\ &\frac{1}{\sqrt{2}}\left(|0_j\rangle + e^{2\pi\imath 2^j\phi}\,|1\rangle\right)|u\rangle \quad .\end{aligned}$$

Se la rappresentazione binaria

$$\phi = \sum_{k=1}^{\infty}\frac{\phi_k}{2^k} \quad ,$$

con $\phi_k \in \{0,1\}$, si troncasse ai primi n termini, o la si assumesse come una approssimazione accettabile, tenendo conto che eventuali termini nella somma con potenze positive di 2 non contribuiscono alla fase, l'intero registro si porrebbe nello stato

$$\begin{aligned}&|0_n\ \ldots,\ 0_2, 0_1\rangle \longrightarrow\\ \frac{1}{2^{n/2}}\ &\left(|0_n\rangle + e^{2\pi\imath\frac{\phi_n}{2}}\,|1_n\rangle\right)\otimes\cdots\\ \cdots\otimes\ &\left(|0_1\rangle + e^{2\pi\imath\sum_{k=1}^{n}\frac{\phi_k}{2^k}}\,|1_1\rangle\right),\end{aligned}$$

analogo allo sviluppo per la trasformata di Fourier U_F visto in precedenza. Quindi, usando l'inverso della QFT (indicato con $\mathcal{F}^\dagger$ in Fig. 12, si può ottenere lo stato $|\phi\rangle = |\phi_n,\cdots,\phi_1\rangle$, che rappresenta la fase ϕ se avesse solo n cifre significative. In generale, una misurazione di tutti gli n qubit di controllo fornirà i valori ϕ_k con $k = 1,\ldots,n$ e, quindi, ϕ con accuratezza $2^{-(n+\log_2 2\epsilon)}$, dove $1-\epsilon$ è la probabilità di ottenere un'approssimazione con precisione 2^{-n}.

Ordine, Fattorizzazione e algoritmo di Shor

Gli algoritmi appena presentati possono essere utilizzati per risolvere una grande varietà di problemi interessanti. Tra di essi il problema di `fattorizzazione degli interi` e quello, ad esso collegato, del problema della `ricerca dell'ordine di un intero` nell'aritmetica modulare. Al di là dell'interesse strettamente matematico per essi, c'è anche quello applicativo legato alla possibile violazione dei sistemi crittografici a chiave pubblica tipo RSA [98].

L'obiettivo è valutare efficientemente la funzione esponenziale negli interi di base a, co-primo di M, nell'aritmetica $\mod M$

$$f_{M,a}(x) = a^x \bmod M, \quad GCD(a, M) = 1,$$

avendo indicato con GCD il Massimo Comune Divisore.

Per esemplificare, riportiamo l'insieme dei valori delle seguenti funzioni:

$$\{f_{15,7}(x)\} = \{7, 4, 13, 1, 7, 4, 13, 1, 7, 4, 13, 1, 7, 4\}$$

$$\begin{aligned}\{f_{17,3}(x)\} \quad = \quad & \{3, 9, 10, 13, 5, 15, 11, \\ & 16, 14, 8, 7, 4, 12, 2, 6, 1\}\end{aligned}$$

L'insieme dei valori di $f_{M,a}(x)$ è un gruppo rispetto alla moltiplicazione $\mod M$, il che comporta che deve esistere un qualche intero r per il quale

$$a^r = 1 \bmod M.$$

Il più piccolo di tali numeri r è chiamato l'**ordine** di $a \mod M$ ed è evidentemente il periodo della funzione $f_{M,a}(x)$. Riferendoci agli esempi precedenti, per ispezione l'ordine di $f_{15,7}$ è 4, mentre quello di $f_{17,3}$ è 16. Ma se i numeri M ed a sono molto grandi, il compito di determinare r può essere arduo nel senso NP.

A questo stadio può essere stabilita la connessione tra il calcolo dell'`ordine` e il problema della `Fattorizzazione di un intero` M, sintetizzandola nella procedura generale di risoluzione presentata nel riquadro sopra.

I Passi 1, 2 e 3 si possono eseguire con un dispendio di risorse computazionali che crescono con una potenza del numero in input, quindi efficientemente, da un algoritmo classico. Il punto cruciale è quindi il calcolo di r al Passo 4.

Passi dell'algoritmo di Shor

Passo	Operazione
1	Se M Pari, ritorna 2.
2	Se $M = p^m$ con p Primo, ritorna p.
3	Scegliere a caso $3 \leq a \leq M-1$: se $GCD(a, M) > 1$ ritorna $GCD(a, M)$.
4	Calcolare l' ordine r di $f_{M,a}$
5	Se r è Pari e $f_{M,a}\left(\frac{r}{2}\right) \neq M-1$, ritorna $GCD\left(a^{r/2} \pm 1, M\right) \neq 1$
6	Se r è Dispari, oppure $f_{M,a}\left(\frac{r}{2}\right) = M-1$, tornare al Passo 3

Tornando al calcolo della funzione $f_{M,a}$ e usando ancora una volta la rappresentazione binaria $x = \sum_{k=0}^{n} \xi_k 2^k$, esso può essere espresso anche nella forma

$$f_{M,a}(x) = \left(a^{2^n}\right)^{\xi_n} \left(a^{2^{n-1}}\right)^{\xi_{n-1}} \cdots \left(a^{2^0}\right)^{\xi_0} \bmod M.$$

Questa formula è efficientemente implementabile anche su un computer classico. Si può dimostrare che il numero di potenze da calcolare è dell'ordine $m \sim O(\log_2 M)$ e, in definitiva, la funzione $f_{M,a}(x)$ può essere valutata con un circuito classico di dimensione $O\left((\log_2 M)^3\right)$ avente la struttura simbolica presentata in Fig. 13 Ma esso non rappresenta un algoritmo quantistico, in quanto non è costituito da trasformazioni unitarie. D'altra parte, per trovare l'ordine r si dovrebbero calcolare tutti i possibili valori di $f_{M,a}(x)$ ed estrarlo poi con la tecnica della Trasformata di Fourier.

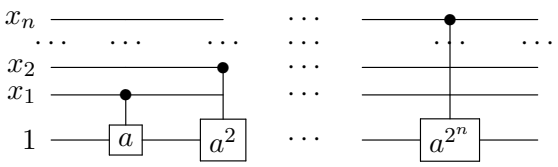


Figura 13: Circuito classico per calcolare l'esponenziale modulare di a^x

Ora siamo nelle condizioni per illustrare l'algoritmo di Shor [95], la cui prima realizzazione sperimentale fu riportata in [96]. L'idea è di as-

sociare ad un intero a coprìmo di M di ordine r, per ora incognito, l'operatore unitario

$$U_a : |x\rangle \to |a\,x \mod M\rangle, \quad x \in \{0, 1, \ldots, M-1\}\,.$$

Per esso si dimostra che la famiglia di vettori di stato

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[-\frac{2\pi\imath s k}{r}\right] |a^k \mod M\rangle \ ,$$

con $0 \leq s \leq r-1$, è costituita da suoi autovettori, con autovalori

$$\exp\left[-\frac{2\pi\imath s}{r}\right],$$

analoghi agli stati in (10) e indicativi della riduzione del problema dell'ordine a quello della stima della fase. Ma per quest'ultima ci sono due importanti requisiti da rispettare: 1) si devono avere procedure efficienti per implementare le operazioni di tipo $c{-}U^{2j}$ per qualsiasi intero j, 2) bisogna essere in grado di preparare in modo efficiente un autostato $|u_s\rangle$, o almeno una sovrapposizione di essi. Il primo requisito può essere soddisfatto ispirandosi alla procedura riportata nelle Figure 13 e 14. Usando un certo numero di qubit ausiliari è semplice costruire un circuito quantistico con due registri con almeno $L = \log_2 M$ qubit, che calcolano la trasformazione

$$c - U_a : |z\rangle\,|y\rangle \to |z\rangle\,|a^z y \mod M\rangle \ .$$

Il secondo requisito è più difficile da soddisfare, poiché dipende dalla conoscenza di r. L'idea si basa sull'osservazione che

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle = |1\rangle \ ,$$

e lo stato $|1\rangle$ è semplice da realizzare. Quindi, utilizzando

$$t = 2L + 1 + \log\left[2 + 1/\left(2\epsilon\right)\right]$$

qubit nel primo registro (con riferimento alla Figura 13) e preparando il secondo registro nello stato $|1\rangle$, con probabilità $(1-\epsilon)/r$ si ottiene una stima della fase $\phi \approx s/r$ per ogni $0 \leq s \leq r-1$ con l'accuratezza di $2L+1$ bit. Non abbiamo ancora r, ma sappiamo che a priori ϕ è un numero razionale con r al denominatore. Perciò se potessimo calcolare la frazione più vicina a ϕ potremmo anche ottenere r. Poiché ottenere la stima della fase con l' accuratezza di $2L+1$ bit significa che

$$|\phi - s/r| \leq 2^{-(2L+1)} \ ,$$

e, poiché $r \leq M \leq 2^L$, si ha anche che $1/2r^2 \geq 2^{-(2L+1)}$, ovvero

$$|\phi - s/r| \leq \frac{1}{2r^2}.$$

Questa relazione è sufficiente per garantire che s/r sia un `convergente` dello sviluppo in frazioni continue di

$$\phi = \cfrac{1}{p_1 + \cfrac{1}{p_2 + \cfrac{1}{\cdots}}} \ .$$

Quindi, dallo sviluppo in frazione continue di ϕ è possibile estrarre un convergente s'/r' costituito da coprìmi tra loro, per i quali vale anche $s'/r' = s/r$. Se si verifica che $a^{r'} = 1 \mod M$, allora $r' = r$ è l'ordine ricercato. Se così non fosse, s ed r devono avere un fattore comune. Ma è possibile dimostrare che se si ripete l'algoritmo almeno $2\log M$ si otterrà con alta probabilità s/r co-primi tra loro.

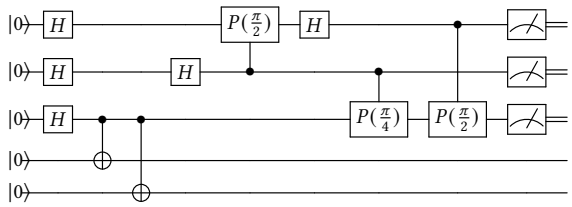


Figura 14: Il circuito ottimizzato in [96] che realizza l'algoritmo di Shor per fattorizzare $M = 15$ con $a = 11$.

L'algoritmo di Shor è un caso particolare di un più generale algoritmo quantistico, discusso da Kitaev per la prima volta [97] e poi esteso ed ottimizzato in [99], che risolve il problema di `Sottogruppo Nascosto`. Senza entrare in nessun dettaglio, ma solo per mostrare il suo carattere generale, tale problema può essere enunciato come segue:

> "sia f una funzione da un gruppo G a un insieme finito X, tale che essa sia

costante sui coset di un sottogruppo K e distinta su ciascuno di essi. Trovare il sottoinsieme generatore di K, usando un oracolo quantistico che esegue la trasformazione unitaria $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, per $g \in G$ e $h \in X$. ”

L'algoritmo di Grover

L'algoritmo di Grover [6] consente di trovare (con probabilità $> 1/2$) uno specifico elemento all'interno di un database disordinato, costituito da N oggetti, usando $O(\sqrt{N})$ operazioni, mentre un computer classico richiederebbe $O(N)$ operazioni per raggiungere lo stesso obiettivo. Pertanto, l'algoritmo di Grover fornisce un'accelerazione quadratica rispetto a un algoritmo classico ottimale. È stato anche dimostrato [100] che l'algoritmo di Grover è ottimo, nel senso che nessuna macchina di Turing quantistica può farlo con un numero inferiore di operazioni.

Sebbene l'algoritmo di Grover sia comunemente considerato utile per la ricerca in un database, le idee di base di questo algoritmo sono applicabili in un contesto molto più ampio. Questo approccio può essere utilizzato per accelerare gli algoritmi di ricerca in cui si potrebbe costruire un `oracolo quantistico` che distingua l'ago dal pagliaio. L'implementazione dell'oracolo può essere ridotta alla costruzione di un circuito quantistico che cambia lo stato di un qubit ausiliario, se esiste una certa funzione f, definita sull'insieme $\{x_1, x_2, \ldots, x_N\}$, tale che $f_*(x) = 0\ \forall x_i \neq x^*$ e $f_*(x) = 1$ se $x = x^*$, essendo x^* l'elemento da trovare.

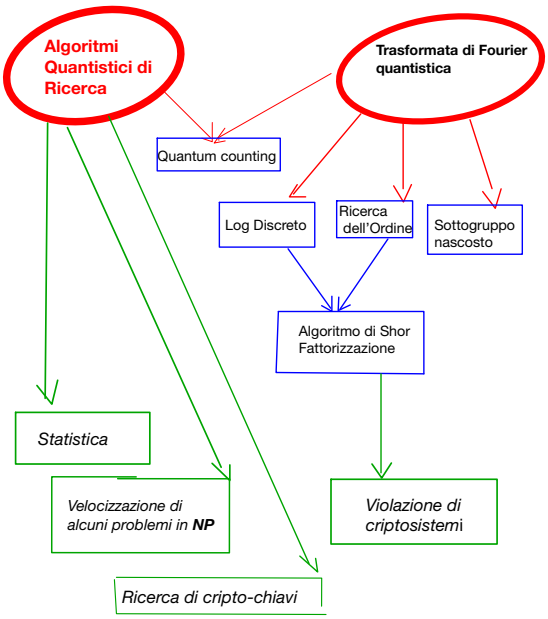


Figura 15: Due dei principali Algoritmi Quantistici e le loro relazioni, incluse alcune notevoli applicazioni.

Si costruisca uno spazio di Hilbert, le cui dimensioni siano $N = 2^n$ pari al numero di elementi del database, in particolare $|x^*\rangle$ faccia parte della base computazionale. L'elemento chiave dell'algoritmo di Grover è l'operatore definito da

$$U_\Psi = 2|\Psi\rangle\langle\Psi| - \mathbf{1},$$

dove

$$|\Psi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle.$$

L'azione di U_Ψ su un generico elemento dello spazio $\sum_i a_i|i\rangle$ è

$$U_\Psi \sum_i a_i|i\rangle = \sum_i (2\langle a\rangle - a_i)\ |i\rangle,$$

dove

$$\langle a\rangle = \frac{1}{N}\sum_i a_i$$

è l'ampiezza media degli stati di base. Questo ci dice che l'ampiezza di ogni singolo stato $|i\rangle$ è riflessa attorno a tale valor medio.

Per poter utilizzare l'operatore di Grover con successo in una ricerca, è necessario che il registro dei qubit di input sia opportunamente inizializzato. Esso viene posto nello stato Ψ precedentemente introdotto, mentre un qubit ancillare è posto nello stato $H|1\rangle$. A questo stadio viene applicato l'oracolo

$$U_{f_*} : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f_*(x)\rangle,$$

il quale lascia immutati tutti gli stati della base computazionale, eccetto che per x^* per il quale vale

$$U_{f_*}|x^*\rangle \otimes H|1\rangle = -|x^*\rangle \otimes H|1\rangle\ \ ,$$

cambiando la fase del qubit ancillare. Combinando questo risultato con l'azione successiva di $\mathbf{U}_\Psi$ si esalta l'ampiezza dello stato $|x\rangle^*$, decrementando quelle degli altri elementi di base. Una misura del registro principale di qubit darà x^*

con probabilità vicina a 1, se la precedente successione di operatori è ripetuta un numero circa uguale a $(\pi\sqrt{N})/4$ volte. Un algoritmo classico assolverebbe allo stesso compito con $O(N)$ tentativi, quindi Grover costituisce un significativo aumento di efficenza computazionale.

Il metodo di Grover è stato applicato in vari problemi di analisi topologica, quale quello della ricerca di triangoli in grafi costituiti da un fissato numero di nodi [101], o di Intelligenza Artificiale e Machine Learning [102].

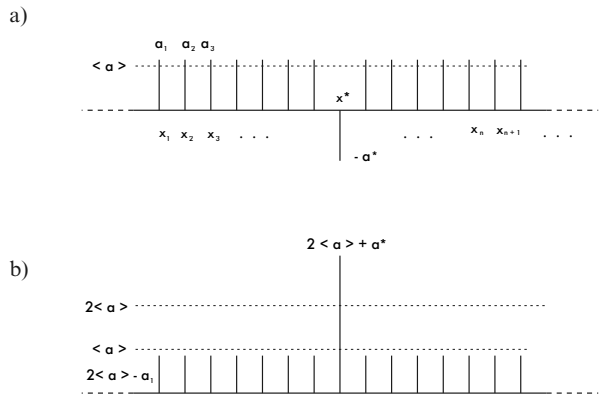


Figura 16: Descrizione grafica di un passo di iterazione dell'algoritmo di Grover. L'elemento da trovare è x^*. In (a) si è cambiato il segno della sua ampiezza attraverso l'azione dell'oracolo U_{f_*}. In (b) si è eseguita l'inversione rispetto alla media usando U_Ψ.

Decoerenza

In pratica è impossibile isolare completamente un computer quantistico dal suo ambiente. Si pensi, ad esempio, alle inevitabili fluttuazioni quantistiche del Campo Elettromagnetico interagenti con un dipolo magnetico, che potrebbe fisicamente costituire un qubit utilizzato in un computer quantistico. Questo va visto come un sottosistema di un sistema più ampio, costituito da esso stesso e dall'ambiente in cui è immerso, che sia termico, elettromagnetico o nucleare. Per ambiente si intende un sistema fisico sul quale non abbiamo alcun controllo: non possiamo ricavarne informazioni di dettaglio, mediante misurazioni o applicarvi azioni di controllo, ma al più valori medi statistici di alcune grandezze interpretate macroscopicamente. In alcuni casi, l'effetto di un'interazione ambientale sul sottosistema computazionale è reversibile, ma in generale produce l'effetto irreversibile della decoerenza. Nella decoerenza, l'informazione codificata nello stato del sottosistema computazionale viene persa nell'ambiente. Pertanto tali errori sono gravi e varie strategie di correzione degli errori, come la ridondanza tripla da un punto di vista computazionale, o comunque l'estensione per quanto possibile del tempo di decoerenza.

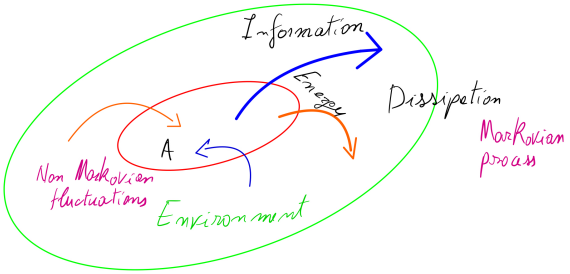


Figura 17: L'insieme dei qubit utilizzati nella computazione è rappresentato da A, mentre *Environment* è l'ambiente con il quale essi vengono a contatto. L'Energia è certamente scambiata in maniera incoerente tra A ed *Environment*, ma anche l'Informazione può fluire irreversibilmente da A verso *Environment*, a causa della decoerenza degli stati puri. Nella situazione più semplice si avranno processi Markoviani. Se le interazioni A-*Environment* godono di una certa `memoria` si avranno processi non Markoviani e fenomeni di `revival` degli stati antecedenti in A.

Sono state sviluppate varie tecniche per la descrizione dei processi di decoerenza nei sistemi computazionali, per comprenderne le caratteristiche e verificare la tolleranza, o robustezza, dei sistemi rispetto ad essa. Nonché per concepire metodi di correzione degli errori quantistici ad essa dovuti e contrastarne gli effetti.

L'idea base consiste nel pensare A e *Environment* come un unico sistema isolato *entangled* (vedi Fig. 17), a causa delle interazioni reciproche, le cui azioni sono espresse da operatori unitari. Allo stesso tempo l'*Environment* può essere anche visto come un osservatore del sistema computazionale A, saggiandone costantemente tutta una serie di proprietà osservabili. L'*entanglement* però modifica le probabilità di osservare un certo esito in una misura sul sottosistema A. Il che, per essere descritto correttamente, richiede una generalizzazione del-

lo schema consueto delle proiezioni ortogonali sugli autostati (vedi Appendice). Questa generalizzazione si esplica nell'esistenza di una famiglia $\{\mathbf{E}_m\}_{m\in\sigma(\mathbf{O}_A)}$ di `Operatori di Misura generalizzati` (POVM) associati ad un certo osservabile $\mathbf{O}_A$. Gli elementi di tale famiglia godono delle seguenti proprietà:

1. Hermitianità: $\mathbf{E}_m^\dagger = \mathbf{E}_m$
2. Positività : $\langle\psi\,|\mathbf{E}_m\,|\psi\rangle \geq 0 \quad \forall\ |\psi\rangle \in \mathcal{H}_A$
3. Completezza: $\sum_m \mathbf{E}_m = \mathbf{1}_A$

Data una POVM $\{\mathbf{E}_m\}$ esistono sempre degli operatori, detti `di Kraus`, che godono delle proprietà

$$\mathbf{Q}_m = \mathbf{U}_m\,\sqrt{\mathbf{E}_m},\ \ \sum_m \mathbf{Q}_m^\dagger\,\mathbf{Q}_m = \mathbf{1}_A$$

dove $\mathbf{U}_m$ sono unitari. Gli operatori di Kraus producono gli stati post-misura. Questo significa che se a seguito della misura si ottiene $m \in \sigma(\mathbf{O}_A)$, allora a riduzione del pacchetto d'onda è data da

$$|\psi\rangle \xrightarrow{m} \frac{\mathbf{Q}_m\,|\psi\rangle}{|\sqrt{\mathbf{E}_m}\,|\psi\rangle|}\ ,$$

o più in generale

$$\boldsymbol{\rho}_m = \frac{\mathbf{Q}_m\,\boldsymbol{\rho}\,\mathbf{Q}_m^\dagger}{\mathrm{tr}\Big(\mathbf{Q}_m\,\boldsymbol{\rho}\,\mathbf{Q}_m^\dagger\Big)}\ ,$$

Una POVM attribuisce probabilità a priori

$$\mathcal{P}_m = \mathrm{tr}\Big(\mathbf{Q}_m\,\boldsymbol{\rho}\,\mathbf{Q}_m^\dagger\Big)$$

di ottenere m nella misura di un dato operatore sullo stato $\boldsymbol{\rho}$. Inoltre, c'è completa libertà di scegliere l'operatore $\mathbf{U}_m$ per ogni m.

L'introduzione delle POVM consente di studiare, senza riferimento a quanto avvenga in *Environment*, le possibili trasformazioni finite in A secondo la mappa

$$\boldsymbol{\rho}_A\ \to\ \mathcal{E}\,(\boldsymbol{\rho}_A) = \sum_m \mathbf{Q}_m\,\boldsymbol{\rho}_A\,\mathbf{Q}_m^\dagger\ .$$

In tal modo, ogni trasformazione finita dello stato di un sistema quantistico in contatto con un *Environment* viene descritta da una mappa lineare `completamente positiva e che preserva la traccia` (TPCP) $\mathcal{E}$. Essa agisce solo sullo stato $\boldsymbol{\rho}_A$ del sistema computazionale A e viene detta **Canale Quantistico**. Si può dimostrare che più Canali Quantistici possono comporsi tra di loro. A differenza degli operatori unitari, in genere i canali quantistici non sono invertibili, quindi essi formano dei semi-gruppi. Per la stessa ragione non è detto che $\mathcal{E}$ rappresenti una trasformazione unitaria, il che implica la decoerenza e la possibilità di descrivere trasformazioni irreversibili in MQ.

Per fare un semplice esempio, si consideri un modello elementare costituito da un qubit che può subire, per cause non specificate e con uguale probabilità p, uno dei tre tipi di errore:

1. Bit flip : $|\psi\rangle \to \sigma_1\,|\psi\rangle$
2. Phase flip: $|\psi\rangle \to \sigma_3\,|\psi\rangle$
3. Bit-Phase flip: $|\psi\rangle \to \sigma_2\,|\psi\rangle$

Naturalmente c'è una probabilità $1-p$ che il qubit rimanga nel suo stato originale. Allora, con una opportuna argomentazione, si possono trovare quattro operatori di Kraus:

$$\mathbf{Q}_0 = \sqrt{1-p}\,\mathbf{1}_2 \quad , \quad \mathbf{Q}_1 = \sqrt{\frac{p}{3}}\sigma_1,$$
$$\mathbf{Q}_2 = \sqrt{\frac{p}{3}}\sigma_2 \quad , \quad \mathbf{Q}_3 = \sqrt{\frac{p}{3}}\sigma_3$$

i quali verificano la condizione di normalizzazione $\sum_m \mathbf{Q}_m^\dagger\mathbf{Q}_m = \mathbf{1}_2$. Inoltre, il corrispondente canale quantistico è fornito dalla mappa nella sfera di Bloch

$$\begin{aligned}\boldsymbol{\rho}\ \to\ \boldsymbol{\rho}' \ &= \ (1-p)\,\boldsymbol{\rho} \\ &+\ \frac{p}{3}\,(\sigma_1\boldsymbol{\rho}\sigma_1 + \sigma_2\boldsymbol{\rho}\sigma_2 + \sigma_3\boldsymbol{\rho}\sigma_3)\ .\end{aligned}$$

Quindi anche se lo stato originario poteva essere puro, la mappa lo fa diventare misto, facendogli perdere coerenza.

Moltissimi altri esempi si possono studiare, quali, ad esempio, singoli qubit accoppiati ad ambienti costituiti da altri qubit, o da oscillatori armonici, oppure da bagni termici variamente specificati. Si possono studiare oscillatori armonici quantistici smorzati, oppure a contatto con bagni termici. Molti esempi e tecniche di studio sono riportati in [47, 106, 105].

Il passaggio successivo consiste nel determinare le equazioni di evoluzione, a tempo continuo, degli stati di sotto-sistemi quantistici a contatto

con un Environment. Sotto le ipotesi di markovianità si ottiene la cosiddetta `Master Equation di Lindblad` [37, 103, 104]

$$\begin{aligned}\frac{d\boldsymbol{\rho}}{dt} &= -\imath\,[\mathbf{H},\boldsymbol{\rho}] \\ &+ \sum_{m>0}\left(\mathbf{L}_m\,\boldsymbol{\rho}\mathbf{L}_m^\dagger - \tfrac{1}{2}\left\{\mathbf{L}_m^\dagger\,\mathbf{L}_m,\,\boldsymbol{\rho}\right\}\right)\end{aligned}$$

dove $\mathbf{H}$ è l'operatore Hamiltoniano se A fosse isolato dall'*Environment*, quindi il primo termine del membro di destra è ovviamente lo stesso dell'equazione di Schrödinger. Gli altri termini invece provengono da operatori di Kraus infinitesimi, chiamati `Salti Quantici`, e descrivono l'effetto di *Environment* su A. Sono essi i responsabili della decoerenza dello stato di A.

Di questa equazione esiste anche una versione in rappresentazione di Heisenberg per gli osservabili di A.

Con l'equazione di Lindblad si possono studiare effetti di smorzamento e di depolarizzazione di sistemi quantistici soggetti a dissipazione e/o decoerenza e, quindi, estremamente rilevanti per l'effettiva dinamica di un computer quantistico. A titolo di esempio si consideri l'evoluzione libera di un qubit sotto l'azione di un effetto di smorzamento di ampiezza (una combinazione degli errori 1. e 3. sopra descritti) definito dal salto quantico $L_1 = \gamma\,(\sigma_1 + \imath\sigma_2)\,/2$ dove $\gamma > 0$ parametrizza l'intensità della perturbazione esterna. L'evoluzione delle popolazioni (gli elementi diagonali) e delle coerenze (gli elementi fuori diagonale) di $\boldsymbol{\rho}\,(t)$ è rappresentato dal grafico di Fig. 18, dove i `tempi di decoerenza` sono $T_1 = 1/\gamma$ e $T_2 = 2/\gamma$ rispettivamente. Come si nota, mentre gli elementi fuori diagonali si annullano, quelli sulla diagonale vanno a dei valori costanti, che debbono sommare a 1. Quindi lo stato finale si decompone solo nelle due possibili configurazioni, senza possibilità di considerare sovrapposizioni quantistiche. Il sistema si è ridotto al comportamento classico.

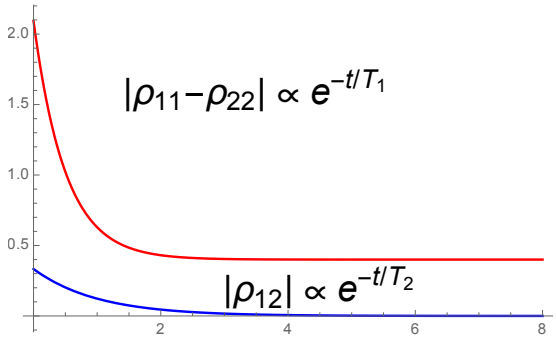


Figura 18

Qual è il valore economico della ricerca nelle Tecnologie Quantistiche?

Le tecnologie quantistiche hanno gridato vittoria grazie ad alcuni riconoscimenti di alto profilo nel 2022, quando Alain Aspect, John Clauser e Anton Zeilinger, che hanno lavorato sull'*entanglement* quantistico nei loro gruppi di ricerca, hanno ricevuto il Premio Nobel per la Fisica. Mentre il loro lavoro scientifico si è svolto effettivamente decenni fa, il progresso tecnologico si è sviluppato poi progressivamente negli anni seguenti. Negli ultimi anni, gli investimenti globali nelle tecnologie quantistiche sono aumentati da poche centinaia di milioni di dollari di dieci anni fa a quasi 2,5 miliardi nel 2022 [108]. Anno in cui IBM ha presentato un processore quantistico da 433 qubit, la macchina Osprey, e prevede di costruire un processore da 4.000 qubit entro il 2025. Un altro esempio è costituito dalla canadese Xanadu [34], che ha utilizzato il suo computer quantistico fotonico, per dimostrare il vantaggio quantistico nel campionamento dei bosoni gaussiani, seguendo i risultati ottenuti in precedenza da altre due squadre.

Tuttavia, accanto a questi riconoscimenti e risultati duramente conquistati si nota un rallentamento della ricerca sulla tecnologia quantistica. In tutto il mondo, nel 2022 sono stati concessi 1.589 brevetti relativi alla tecnologia quantistica, il 61% in meno rispetto al 2021. In effetti, dal 2021 al 2022, il numero di articoli pubblicati sulla tecnologia quantistica è diminuito del 5%. Queste tendenze potrebbero essere un segnale che le sfide rimanenti sono più difficili da risolvere. Forse perché il problema più pertinente e urgente resta tuttora irrisolto: costruire un computer quantistico con un numero e una qualità di qubit sufficienti per garantire che il calcolo non sia compromesso da rumore, ovvero un computer tollerante agli errori. Sebbene le dimensioni dei computer quantistici (in termini di numero di qubit al loro interno) e la fedeltà dei qubit siano

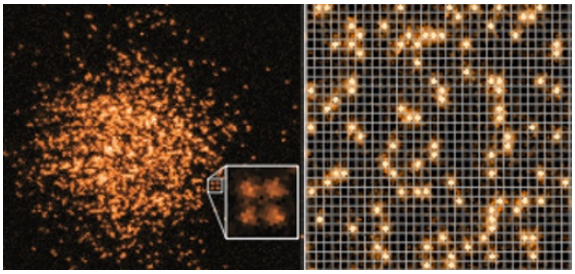


Figura 19: Atomi fermionici ripresi utilizzando un microscopio a gas. Il dispositivo consente di trovare la disposizione dei singoli atomi nel reticolo, nonché il loro spin. (K. Wright, Physics 12, 76 (2019))

cresciute costantemente, ciò non è ancora avvenuto in tandem. In altre parole, un computer quantistico più grande avrà solitamente una fedeltà inferiore rispetto a uno più piccolo. È di questi giorni [107] la notizia che Atom Computing ha realizzato il primo computer quantistico con 1180 qubit, utilizzando lo spin nucleare di atomi neutri di itterbio intrappolati un reticolo ottico bidimensionale. La compagnia sostiene di poter decuplicare la quantità di qbit in due anni. Inoltre, si afferma che l'insieme di qbit riesca a mantenere un tempo di coerenza dell'ordine del minuto, contro i 70-80 μsec dei sistemi a superconduttore. Se fosse vero, ci troveremmo di fronte ad una pietra miliare nella storia di questa tecnologia.

In ciascuno dei cinque approcci principali ai computer quantistici, permangono sfide impegnative. Ad esempio, i dispositivi basati sulla fotonica continuano a perdere fotoni, con conseguenti errori di calcolo. I dispositivi basati su trappola ionica e atomi neutri non hanno ancora dimostrato la capacità di condurre rapidamente calcoli man mano che il numero di qubit aumenta. I dispositivi a superconduttori devono ancora adattare i propri sistemi di controllo e raffreddamento per gestire potenzialmente migliaia di qubit.

Appendice: postulati della MQ

Ad un dato sistema fisico sia associato un opportuno spazio lineare (vettoriale) $\mathcal{H} = \{|\psi\rangle\}$ su $\mathbb{C}$, $dim(\mathcal{H}) = d$, dotato di prodotto scalare hermitiano $\langle\cdot|\cdot\rangle$, separabile, completo e di opportuna dimensione (detto spazio di Hilbert). In questa esposizione supporremo sempre d finito, anche se in molte circostanze è necessario adottare spazi di dimensione infinita numerabili. Valgono i seguenti postulati:

- Ad ogni stato fisico del sistema corrisponde un unico operatore di **stato $\boldsymbol{\rho}$**: hermitiano su $\mathcal{H}$, semipositivo e a traccia 1. In letteratura è anche chiamato *Matrice Densità*.

  Nel testo si userà spesso solo la parola `stato` per riferirsi all'operatore di stato.

- Combinazioni lineari convesse di stati sono ancora stati $\boldsymbol{\rho}(\lambda) = \lambda\,\boldsymbol{\rho}_1 + (1-\lambda)\,\boldsymbol{\rho}_2,\ 0 \leq \lambda \leq 1$.

- Gli stati che sono anche proiettori sul sottospazio generato dal vettore $|\psi\rangle$ (detto **vettore di stato**) sono espressi nella forma $\boldsymbol{\rho} = |\psi\rangle\langle\psi|\quad(\langle\psi\,|\psi\rangle = 1)$ e sono chiamati **stati puri**. Inoltre, data una qualunque base ortonormalizzata $\{|\phi\rangle_i,\ \langle\phi_i|\phi_j\rangle = \delta_{ij}\}_{i=1,\cdots,d}$ di $\mathcal{H}$, i coefficienti $a_i = \langle\phi_i|\psi\rangle$ di $|\psi\rangle$ rispetto ad essa sono detti **ampiezze di probabilità**, o collettivamente **funzione d'onda**.

- Ad ogni grandezza fisica $\mathcal{O}$ corrisponde un **osservabile**, cioé un operatore lineare hermitiano $\mathbf{O}$ su $\mathcal{H}$. Il suo **spettro** $\sigma(\mathbf{O}) = \{\mu:\ \mathbf{O}\,|\psi^h_\mu\rangle = \mu\,|\psi^h_\mu\rangle\} \subseteq \mathbb{R}$ costituisce l'insieme dei valori che si possono ottenere a seguito di una misura di $\mathcal{O}$.

- Observabili per i quali $[\mathbf{O},\ \mathbf{O}'] \neq 0$ si dicono **incompatibili**. Le loro distribuzioni di probabilità sono correlate. In particolare, si dimostra che per coppie di osservabili canonicamente coniugati $[\mathbf{p}_i, \mathbf{x}_i] = \imath\,\hbar$ vale la disuguaglianza $\Delta p_i \Delta x_i \geq \hbar/2$ (principio di Heisenberg)

- (Teorema di Decomposizione Spettrale) Ogni osservabile $\mathbf{O}$ possiede una famiglia completa di **proiettori ortogonali** $\mathbf{P}^\dagger_\lambda = \mathbf{P}_\lambda$, $\sum_{\sigma(\mathbf{O})}\mathbf{P}_\lambda = \mathbf{1}_\mathcal{H},\ \mathbf{P}_\lambda\mathbf{P}_\mu = \delta_{\lambda,\mu}\mathbf{P}_\lambda,\ \mathbf{P}_\lambda = \sum_g |\psi^g_\lambda\rangle\langle\psi^g_\lambda|$ tali che $\mathbf{O} = \sum_{\sigma(\mathbf{O})}\lambda\,\mathbf{P}_\lambda$.

- (**Regola di Born**) Introdotta la *traccia* di un operatore su $\mathcal{H}$ come l'applicazione $tr(\cdot)$: End $(\mathcal{H}) \to \mathbb{C}$ che sia lineare, indipendente dalla base scelta e ciclica, essa consente di

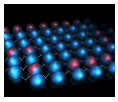
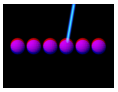
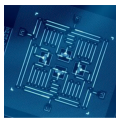
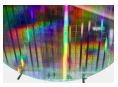
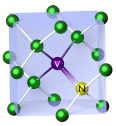
	Cold atoms	Trapped Ions	Superconducting	Silicon	NV centers	Photons
						
Number of physical qubits	324	32	433	15	10	216
Best two-qubit gate fidelity (%)	99.4	99.9	99.97	>99	99.2	98
Best readout fidelity (%)	99.1	99.9	99.4	99	98	50
Best gate time (ns)	1	10^5	20	$5 * 10^3$	10	<1
Best T_1 (s)	>1	0.2	$4 * 10^{-4}$	$1.2 * 10^{-4}$	$2.4 * 10^{-3}$	∞
Temperature (mK)	<1	<1	15	100	$4 * 10^3$	Room Temperature
Scalability (# qubits)	up to 10^4	<50	$\sim 10^3$	$\sim 10^6$	$\sim 10^2$	$\sim 10^6$

Figura 20: Confronto tra diversi tipi di implementazioni fisiche di qubit. La tabella ripresa da [23] è stata ottenuta raccogliendo i dati di numerosi altri lavori ivi citati. La Fedeltà di porta è definita da $F = |\langle\psi\,|_N\,|\psi\rangle_I|^2$ tra gli stati evoluti attraverso un porta sperimentale rumorosa e la corrispondente ideale. La Fedeltà in lettura misura la precisione, compresa tra 0.5 e 1, con cui è possibile determinare lo stato di un qubit. Il tempo di porta è il tempo necessario per eseguire la corrispondente operazione. T_1 è il tempo di rilassamento di un qubit, cioè la costante di decadimento nella probabilità di permanenza $p \propto e^{-t/T_1}$ del qubit nello stato $|1\rangle$. La temperatura si riferisce alla quella tipica alla quale devono funzionare i computer quantistici basati sulla data tecnologia . La scalabilità riporta una stima della capacità di aumentare il numero di qubit in un computer quantistico senza compromettere la qualità dei qubit con le attuali tecnologie. Il numero 216 di qubit fisici nella piattaforma fotonica corrisponde al numero di modalità GBS (Gaussian Boson Sampling). Le immagini sono indicative della tecnologia adottata.

calcolare il valore medio dell'osservabile $\mathbf{O}$ sullo stato $\boldsymbol{\rho}$ dalla formula

$$\langle\mathbf{O}\rangle = tr(\boldsymbol{\rho}\,\mathbf{O}).$$

- Nel caso della misura di un osservabile $\mathcal{O}$ su uno Stato Puro $\boldsymbol{\rho} = |\psi\rangle\langle\psi|$, la probabilità di ottenere l'autovalore m è data da

$$\mathcal{P}_m = \langle\psi\,|\mathbf{P}_m\,|\psi\rangle.$$

- Se un sistema, preparato in uno stato puro specificato da $|\psi\rangle$, è sottoposto alla misura di un osservabile $\mathbf{O}$, a seguito della quale si ottiene $m \in \sigma(\mathbf{O})$, lo stato conseguente è puro ed è il proiettato del vettore di stato

$$|\psi\rangle \overset{m}{\to} \frac{\mathbf{P}_m\,|\psi\rangle}{\sqrt{\langle\psi\,|\mathbf{P}_m\,|\psi\rangle}}\ ,$$

detto anche **stato ridotto**.

- Dato un sistema isolato che a $t = 0$ si trovi nello Stato $\boldsymbol{\rho}(0)$, esso evolverà **unitariamente** nel tempo, in accordo all'equazione di Schrödinger

$$\dot{\boldsymbol{\rho}}(t) = -\imath\,[\mathbf{H}(t)\,,\boldsymbol{\rho}(t)],$$

dove l'operatore hermitiano $\mathbf{H}(t)$ è detto **Hamiltoniano**.

- La descrizione dei sistemi quantistici non isolati richiede l'introduzione di alcune ipotesi aggiuntive e una apposita estensione dei precedenti concetti [36, 37, 47].

[1] R. P. Feynman: *Simulating physics with computers.* Int. J. Theoret. Phys., 21 (1981) 467.

[2] D.Deutsch: *Quantum theory, the Church-Turing principle and the universal quantum computer.* Proc. R. Soc. Lond. Ser. A Math. Phys. Sci., 400 (1985) 97.

[3] D. P. Di Vincenzo: *Two-bit gates are universal for quantum computation.* Phys. Rev. A, 50 (1995) 1015.

[4] P. W. Shor: *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer* SIAM Rev., 41 (1999) 303.

[5] A. Sanjeev; B. Boaz: *Computational complexity* Cambridge University Press, Cambridge UK, (2009) p. 230.

[6] L. K. Grover: *Quantum mechanics helps in searching for a needle in a haystack.* Phys. Rev. Lett., 79 (1997) 325.

[7] A. P. Lund, M. J. Bremner, T. C. Ralph: *Quantum sampling problems, Boson Sampling and quantum supremacy.* Quantum Inf., 3 (2017) 15.

[8] A. Harrow, A. Montanaro: *Quantum computational supremacy.* Nature, 549 (2017) 203.

[9] D. Loss, D. P. Di Vincenzo:: *Quantum computation with quantum dots.,* Phys. Rev. A, 57 (1998) 120.

[10] N. Gershenfeld, I. L. Chuang: *Bulk spin resonance quantum computation.* Science, 275 (1997) 350.

[11] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble. *Mea- surement of conditional phase shifts for quantum logic.* Phys. Rev. Lett., 75 (1995) 4710.

[12] P. Domokos, J. M. Raimond, M. Brune, S. Haroche: *Simple cavity-QED two-bit universal quantum logic gate: The principle and expected performances.* Phys. Rev. Lett., 52 (1995) 3554.

[13] D. Kielpinski, C. Monroe, D. Wineland: *Architecture for a large-scale ion-trap quantum computer.* Nature, 417 (2002) 709.

[14] H. Häffner, C.F. Roos, R. Blatt: *Quantum computing with trapped ions.* Phys. Rep., 469 (2008) 155.

[15] https://www.nist.gov/programs-projects/quantum-computing-trapped-ions

[16] S. Slussarenko, G. J. Pryde: *Photonic quantum information processing: A concise review.* Appl. Phys. Rev., 6 (2019) 041303.

[17] C. W. Fink, C. Salemi, B. A. Young, D. I. Schuster, N. A. Kurinsky: *The Superconducting Quasiparticle-Amplifying Transmon: A Qubit-Based Sensor for meV Scale Phonons and Single THz Photons*. https://doi.org/10.48550/arXiv.2310.01345

[18] A. Stern, N. H. Lindner: *Topological Quantum Computation—From Basic Concepts to First Experiments.* Science, 339 (2013) 1179.

[19] G Wendin: *Quantum information processing with superconducting circuits: a review.* Rep. Progr. Phys., 80 (2017), 106001.

[20] G. T. Byrd and Y. Ding: *Quantum Computing: Progress and Innovation.* Computer, 56 (2023) 20.

[21] H. Sahu, D. H. Gupta: *Quantum Computing Toolkit From Nuts and Bolts to Sack of Tools.* (2023). arXiv preprint arXiv:2302.08884

[22] L. Jaeger: *The second Quantum Revolution* Springer Nature Switzerland AG (2018).

[23] E. A. Ruiz Guzman: *Symmetry breaking and restoration for many-body problems treated on quantum computers.* PhD Thesis, Paris-Saclay (2023).

[24] F. Barahona: *On the computational complexity of Ising spin glass models.* J. Phys. A 15 (1982) 3421.

[25] S. Istrail, *Statistical Mechanics, Three-Dimensionality and NP-Completeness: I. Universality of Intracatability for the Partition Function of the Ising Model across Non-Planar Surfaces.* Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, Oregon, USA, (2000), 87. https://doi.org/10.1145/335305.335316.

[26] R. B. Laughlin and D. Pines: *The theory of everything.* Proc. Natl. Acad. Sci., 97 (2000) 28.

[27] D. DiVincenzo: *The Physical Implementation of Quantum Computation.* Fortschritte der Physik, 48 (2000) 771.

[28] D. Gottesman: *An introduction to quantum error correction and fault-tolerant quantum computation.* Proceedings of Symposia in Applied Matthematics, 68 (2010).

[29] https://quantumai.google

[30] https://www.ibm.com/quantum?mhsrc=ibmsearch_a&mhq=quantum%20computer

[31] J. Preskill: *Quantum Computing in the NISQ era and beyond.* Quantum, 2 (2018) 79.

[32] F. Arute et al. *Quantum supremacy using a programmable superconducting processor.* Nature, 574 (2019) 505.

[33] Y. Kim et al.: *Evidence for the utility of quantum computing before fault tolerance.* Nature, 618 (2023) 500.

[34] https://www.xanadu.ai

[35] J. M. Arrazola et al.: *Quantum circuits with many photons on a programmable nanophotonic chip.* Nature, 591 (2021) 54.

[36] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information.* Cambridge, UK (2000).

[37] J. Preskill, *Quantum Computation.* Lecture Notes Physics 219/CS219, http://theory.caltech.edu/~preskill/ph219/ph219_2023.html

[38] E. Rieffel, W. Polak: *Quantum Computing: a gentle introduction.* The MIT Press Cambridge, Massachusetts (2011).

[39] M. Lanzagorta, J. Uhlmann: *Quantum Computer Science.* Morgan & Claypool, San Rafael, USA (2009).

[40] M. M. Wilde: *Quantum information theory.* Cambridge Univ. Press, Cambridge UK (2017).

[41] G. Benenti, G. Casati, D. Rossini, G. Strini: *Principles of Quantum Computation and Information.* World Scisntific, Singapore (2018).

[42] J. D. Hidary: *Quantum Computing: An Applied Approach.* Springer Nature Switzerland AG (2019).

[43] J., Abhijith et al.: *Quantum Algorithm Implementations for Beginners.* ACM Transactions on Quantum Computing, 3 (2022) 18.

[44] C. Cohen-Tannoudji, B. Diu, F. Laloe: *Quantum Mechanics* John Wiley and Sons, New York (1977).

[45] L. E. Ballentine: *Quantum Mechanics, A Modern Development* 2nd Edition, World Scientific, Singapore, (2014).

[46] J. J. Sakurai: *Modern Quantum Mechanics* Addison-Wesley, Reading, Mass. (1995).

[47] U. Weiss: *Quantum dissipative Systems* World Scientific, Singapore (2022).

[48] A. Einstein, B. Podolsky, and N. Rosen: *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev., 47 (1935) 777.

[49] J. S. Bell: *On the Einstein-Podolsy-Rosen paradox.* Physics, 1 (1964) 195. Reprinted in J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics.* Cambridge University Press, Cambridge, (1987).

[50] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt: *Proposed experiment to test local hidden-variable theories.* Phys. Rev. Lett., 49 (1969) 1804.

[51] A. Aspect, P. Grangier, G. Roger: *Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities* Phys. Rev. Lett., 49 (1982) 91.

[52] https://www.nobelprize.org/prizes/physics/2022/summary/

[53] P. Colciaghi, Y. Li, Yifan, P. Treutlein, T. Zibold, *Einstein-Podolsky-Rosen Experiment with Two Bose-Einstein Condensates.* Phys. Rev. X, 13(2023) 021031.

[54] P. Calabrese, J. Cardy: *Entanglement entropy and quantum field theory.* J. Stat. Mech., 0406 (2004) P06002.

[55] K. Mattle, H. Weinfurter, P. G. Kwiat, A. Zeilinger: *Dense coding in experimental quantum communication.* Phys. Rev. Lett., 76 (1996) 4656.

[56] C. H. Bennett et al. *Purification of noisy entanglement and faithful teleportation via noisy channels.* Phys. Rev. Lett., 76 (1996) 722.

[57] D. Bouwmeester et al. *Experimental quantum teleportation.* Nature, 390 (1997) 575.

[58] M. A. Nielsen, E. Knill, and R. Laflamme: *Complete quantum teleportation using nuclear magnetic resonance.* Nature, 396 (1998) 52.

[59] D. Boschi et al.: *Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski-Rosen channels.* Phys. Rev. Lett., 80 (1998) 1121.

[60] N. Lee et al., *Teleportation of nonclassical wave packets of light.* Science, 332 (2011) 330.

[61] C. H. Bennett, G. Brassard: *Quantum cryptography: Public key distribution and coin tossing.* In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179, IEEE, New York, 1984. Bangalore, India, (1984).

[62] M. Sasaki et al. *Field test of quantum key distribution in the Tokyo QKD Network.* Opt. Express, 19 (2011) 10387.

[63] D. Stucki et al., *Long-term performance of the Swiss Quantum quantum key distribution network in a field environment.* N. J. Phys., 13 (2011) 123001.

[64] J. F. Dynes et al.: *Cambridge quantum network.* NPJ Quantum Inf., 5 (2019) 101.

[65] Y. H. Yang et al. *All optical metropolitan quantum key distribution network with post-quantum cryptography authentication.* Opt. Express, 29 (2021) 25859.

[66] S.-K. Liao et al. *Satellite-to-ground quantum key distribution.* Nature, 549 (2017) 43.

[67] Y.-A. Chen et al. *An integrated space-to-ground quantum communication network over 4600 kilometres.* Nature, 589 (2021) 214.

[68] S. K. Liao et al.: *Satellite-relayed intercontinental quantum network.* Phys. Rev. Lett., 120 (2018) 030501.

[69] R. Nagarajan,N. Papanikolaou, D. Williams: *Simulating and Compiling Code for the Sequential Quantum Random Access Machine.* In P. Selinger, Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005), Electronic Notes in Theoretical Computer Science 170 (2007) 101.

[70] A. W. Harrow B. Recht, I. L. Chuang: *Efficient discrete approximations of quantum gates.* J. Math. Phys., 43 (2002) 4445.

[71] J. I. Cirac, P. Zoller: *Quantum Computations with Cold Trapped Ions* Phys. Rev. Lett., 74 (1995) 4091.

[72] S. Venegas: *Quantum Walks for Computer Scientists. Morgan and Claypool.* (2008) DOI: 10.1145/1062261.1062335

[73] E. Farhi et al., *A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-Complete Problem.* Science, 292 (2001) 472.

[74] A. Robert et al.: *Resource-efficient quantum algorithm for protein folding.* Quantum Inf., 7 (2021) 38.

[75] A.Pardomo et al.: *On the construction of model hamiltonians for adiabatic quantum computing and its application to finding low energy conformations of lattice protein models.* Phys. Rev. A, 78 (2008) 012320.

[76] E. F. Dumitrescu et al.: *Cloud Quantum Computing of an Atomic Nucleus* Phys. Rev. Lett., 120 (2018) 210501.

[77] A. Perez-Obiol et al. *Nuclear shell-model simulation in digital quantum computers.* Scientific Reports, 13 (2023) 12291.

[78] V. Amitrano, A. Roggero, P. Luchi, F. Turro, L. Vespucci, F. Pederiva, *Trapped-ion quantum simulation of collective neutrino oscillations.* Phys. Rev. D, 107 (2023) 023007.

[79] D. Lacroix: *Symmetry-assisted preparation of entangled many-body states on a quantum computer.* Phys. Rev. Lett., 125 (2020) 230502.

[80] S. Lee et al.: *Evaluating the evidence for exponential quantum advantage in ground-state quantum chemistry.* Nature Commun., 14 (2023) 1952.

[81] S. Barison, F. Vicentini, G. Carleo: *An efficient quantum algorithm for the time evolution of parameterized circuits.* Quantum, 5 (2021) 512.

[82] I. M. Georgescu, S. Ashhab, F. Nori *Quantum simulation.* Rev. Mod. Phys., 86 (2014) 153.

[83] G. Benenti, G. Strini: *Quantum simulation of the single-particle Schrödinger equation.* Am. J. Phys., 76 (2008) 657.

[84] R. D. Somma: *Quantum Simulations of One Dimensional Quantum Systems.* Quantum Info. Comput., 16 (2016) 1125.

[85] Y. I. Bogdanov et al.: *Solution of the Schrödinger Equation on a Quantum Computer by the Zalka–Wiesner Method Including Quantum Noise.* Jetp. Lett., 114 (2021) 354.

[86] J. R. McClean, J. Romero, R. Babbush, and A. Aspuru-Guzik, *The theory of variational hybrid quantum-classical algorithms.* New Journal of Physics, 18 (2016) 023023.

[87] A. Montanaro. *Quantum algorithms: an overview.* Quantum Information, 2 (2016) 15023.

[88] A. Peruzzo et al.: *A variational eigenvalue solver on a photonic quantum processor.* Nat. Commun., 5 (2014) 4213.

[89] F. E. Chrit et al. *Fully quantum algorithm for lattice Boltzmann methods with application to partial differential equations*, arXiv 2305.07148 (2023).

[90] L. Budinski: *Going deeper into the quantum lattice Boltzmann method: exploring multiphysics applications in 2D.* Quantum Science, (2023), https://quanscient.com

[91] P. C. Costa, S. Jordan, A. Ostrander *Quantum algorithm for simulating the wave equation.* Phys. Rev. A, 99 (2019) 012323.

[92] A. Suau, G. Staffelbach, H. Calandra *Practical Quantum Computing: Solving the Wave Equation Using a Quantum Approach.* ACM Transactions on Quantum Computing 2 (2021). https://doi.org/10.1145/3430030

[93] D. Deutsch, R. Jozsa: *Rapid solution of problems by quantum computation.* Proc. R. Soc. London A, 439 (1992) 553.

[94] D. Simon: *On the power of quantum computation.* In Proceedings, 35th Annual Symposium on Foundations of Computer Science (1994) 116.

[95] P. W. Shor: *Algorithms for quantum computation: discrete logarithms and factoring.* In Proceedings, 35th Annual Symposium on Foundations of Computer Science, IEEE Press, Los Alamitos, CA, (1994).

[96] L. M. K.Vandersypen et al.: *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.* Nature, 414 (2001) 883.

[97] A. Y. Kitaev: *Quantum measurements and the Abelian stabilizer problem.* (1995). arXiv e-print quant-ph/9511026

[98] N. Koblitz: *A Course in Number Theory and Cryptography.* Springer-Verlag, New York, (1994).

[99] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca: *Quantum algorithms revisited.* Proc. R. Soc. London A, 454 (1969) 339.

[100] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani: *Strengths and weaknesses of quantum computing.* SIAM journal on Computing, 26 (1997) 1510.

[101] F. Magniez, M. Santha, M. Szegedy: *Quantum algorithms for the triangle problem.* SIAM J. Comput., (2007) 413.

[102] M. Schuld, I.Sinayskiy, F. Petruccione: *An introduction to quantum machine learning.* Contemporary Physics, 56 (2015) 172.

[103] G. Lindblad: *On the generators of quantum dynamical semigroups,* Comm. Math. Phys., 48 (1976) 119.

[104] V. Gorini, A. Kossakowski, E. C. G. Sudarshan: *Completely positive dynamical semigroups of N-level systems,* J. Math. Phys., 17 (1976) 821.

[105] H.-P. Breuer, F. Petruccione: *The Theory of Open Quantum Systems.* (Oxford, 2007; online edn, Oxford Academic), https://doi.org/10.1093/acprof:oso/9780199213900.001.0001

[106] D. A. Lidar: *Lecture Notes on the Theory of Open Quantum Systems.* arXiv: Quantum Physics, (2019). https://api.semanticscholar.org/CorpusID:119477176

[107] https://www.newscientist.com/article/2399246-record-breaking -quantum-computer-has-more-than-1000-qubits/?utm_source=nsday&utm_medium=email&utm_campaign=nsday_251023&utm_term=Newsletter%20NSDAY_Daily

[108] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap?utm_source=nsqp&utm_medium=email&utm_campaign=nsqp_071123&utm_term=Newsletter%20NSQP_Lost%20in%20Space%20Time

Luigi Martina: è Professore Associato di Fisica Teorica presso l'Università del Salento. Si occupa di sistemi integrabili e, più recentemente, di algoritmi quantistici.