Introduzione alla Teoria dell'Informazione Quantistica

Antonio Causa

Dipartimento di Matematica e Informatica

11 Aprile 2016

Piano della Presentazione

Il formalismo matematico

L'oggetto matematico che ricopre un ruolo fondamentale in Meccanica Quantistica è senza alcun dubbio lo spazio di Hilbert.
Per l'utilizzo che ne faremo in questa presentazione tutti gli spazi vettoriali a cui faremo riferimento saranno di dimensione finita e a coefficienti complessi.
Inoltre su tali spazi considereremo definito un prodotto scalare hermitiano.

Spazi di Hilbert

Indicato con $\mathcal{H}$ uno spazio vettoriale, un prodotto scalare hermitiano è una applicazione

$$\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$$

che soddisfa le seguenti proprietà:

- $\langle \psi | \phi + \eta \rangle = \langle \psi | \phi \rangle + \langle \psi | \eta \rangle$, $\langle \psi + \phi | \eta \rangle = \langle \psi | \eta \rangle + \langle \phi | \eta \rangle$
- $\langle \alpha\psi + \beta\phi | \eta \rangle = \alpha^* \langle \psi | \phi \rangle + \beta^* \langle \phi | \eta \rangle$, $\langle \psi | \alpha\phi + \beta\eta \rangle = \alpha \langle \psi | \phi \rangle + \beta \langle \phi | \eta \rangle$
- $\langle \psi | \phi \rangle = \langle \phi | \psi \rangle^*$
- $\langle \psi | \psi \rangle \geq 0$, $\langle \psi | \psi \rangle = 0 \Leftrightarrow \psi = 0$

Definizione 1

Uno spazio di Hilbert è uno spazio vettoriale (di dimensione finita) su cui è definito un prodotto scalare hermitiano.

Operatori hermitiani e matrici

Un operatore è una applicazione lineare $A : \mathcal{H} \longrightarrow \mathcal{H}$.
Dato un operatore A su uno spazio di Hilbert, si può definire l'operatore aggiunto $A^\dagger$ come quell'operatore che soddisfa la condizione seguente:

$$\langle\psi|A|\phi\rangle = \langle\phi|A^\dagger|\psi\rangle^* \qquad \forall\, \psi, \phi \in \mathcal{H}$$

Definizione 2

Un operatore si dice hermitiano se $A = A^\dagger$.

Definizione 3

Una matrice che coincide con la propria trasposta coniugata si dice hermitiana.

Esercizio

Sia $\mathcal{B}$ una base ortonormale di $\mathcal{H}$. Dimostrare che la matrice associata ad un operatore hermitiano rispetto a $\mathcal{B}$ coincide con la propria trasposta coniugata.

Operatori unitari e matrici

Definizione 4

Un operatore $U : \mathcal{H} \longrightarrow \mathcal{H}$ *si dice unitario se vale*

$$U \cdot U^\dagger = U^\dagger \cdot U = I \text{ o, equivalentemente } U^\dagger = U^{-1}$$

Una proprietà caratteristica degli operatori unitari consiste nel fatto che tali operatori conservano il prodotto scalare.

Esercizio

Data una base ortonormale, la matrice associata ad un operatore unitario è una matrice le cui colonne (o righe) formano una base ortonormale di $\mathbb{C}^n$.

Matrici di Pauli e di Hadamard

Le seguenti matrici, chiamate matrici di Pauli, hanno un ruolo molto importante in Meccanica Quantistica e verrano utilizzate in tutte le applicazioni mostrate in seguito.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

La matrice di Hadamard è

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

Esercizio

Verificare che $XY - YX = 2iZ$.

Notazione di Dirac

La notazione universalmente usata per descrivere un vettore in Meccanica Quantistica è quella di Dirac che consiste nel rappresentare un vettore nel seguente modo

$$|\psi\rangle$$

e quindi il simbolo ψ adesso si deve considerare come un'etichetta che descrive il vettore.
La notazione $|\cdot\rangle$ è usata per indicare che tale oggetto è un vettore ed è chiamato un *ket*.

Attenzione. $|0\rangle \neq 0$.

La base computazionale

Uno dei casi più semplici che si possano considerare è il caso in cui $\dim \mathcal{H} = 2$. Fissata una base in $\mathcal{H}$ gli operatori hermitiani si possono rappresentare mediante matrici *hermitiane* 2×2.
Gli autovettori della matrice di Pauli Z, associati rispettivamente agli autovalori -1 e $+1$, si indicano con i simboli $|0\rangle$ e $|1\rangle$.

Esercizio

Verificare che gli autovettori della matrice X, associati rispettivamente agli autovalori $+1$ e -1, sono

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Esercizio. Calcolare autovalori ed autovettori delle matrici Y e H.

Prodotto tensoriale

Se V e W sono spazi di Hilbert di dimensione n ed m allora $V \otimes W$ è uno spazio di Hilbert con dim $V \otimes W = n \cdot m$.
La maniera più semplice di descrivere un prodotto tensoriale è quella di dire che se $\{|i\rangle : i = 1, \dots n\}$ e $\{|j\rangle : j = 1, \dots m\}$ sono basi ortonormali, allora $\mathcal{B} = \{|i\rangle \otimes |j\rangle : i = 1, \dots n; j = 1 \dots . m\}$ forma una base ortonormale di $V \otimes W$.
Spesso per indicare un prodotto tensoriale tra due ket si sottintende il simbolo $\otimes$ e si identificano i seguenti simboli

$$|a\rangle \otimes |b\rangle = |a\rangle|b\rangle = |a, b\rangle$$

I Postulati della Meccanica Quantistica

Postulato 1

Ad ogni sistema fisico isolato è associato uno spazio di Hilbert chiamato spazio degli stati del sistema. Il sistema è completamente determinato da un suo vettore di stato, che è un vettore unitario nello spazio degli stati del sistema.

La Meccanica Quantistica non ci dice, per un dato sistema fisico quale sia il suo spazio degli stati né quale sia il suo vettore di stato.
Ottenere le regole che descrivono specifici sistemi fisici è compito della Fisica Teorica.

Lo spazio dei qubits

Il più semplice sistema fisico che si possa immaginare è denominato *qubit* (abbreviazione di quantum-bit).
L'insieme dei qubits forma uno spazio degli stati bidimensionale.
Tra tutte le basi ortonormali di questo spazio se ne individua una, chiamata base computazionale, di solito indicata come $\{|0\rangle, |1\rangle\}$ e quindi un arbitrario vettore in questo spazio si potrà esprimere come:
$|\psi\rangle = a|0\rangle + b|1\rangle$ con $a, b \in \mathbb{C}$.
La condizione di normalizzazione: $\langle\psi|\psi\rangle = 1$, fornisce $|a|^2 + |b|^2 = 1$.

Evoluzione di un sistema isolato

Postulato 2

L'evoluzione di un sistema (quantitistico) isolato è descritta da una trasformazione unitaria. Ovvero, lo stato $|\psi_1\rangle$ al tempo t_1 e lo stato $|\psi_2\rangle$ al tempo t_2 sono collegati da un operatore unitario U, che dipende solo dai tempi t_1 e t_2, nel modo seguente

$$U|\psi_1\rangle = |\psi_2\rangle.$$

Commenti al secondo postulato

Anche in questo caso la Meccanica Quantistica non ci dice quale sia l'operatore unitario che decrive l'evoluzione di un particolare sistema fisico.
Si può comunque, legittimamente, porre la domanda di *quali* siano gli operatori unitari che si possono utilizzare.
La risposta è che la Natura non pone alcun limite sul tipo di evoluzione di un sistema fisico quindi, in linea di principio, dato un qualsiasi operatore unitario esisterà un sistema fisico la cui evoluzione sarà descritta da tale operatore.

Misurazione quantistica
Formulazione di Von Neumann

La misura di una particolare proprietà (osservabile) di un sistema quantistico è descritta dal seguente postulato.

Postulato 3

Una Misurazione Proiettiva è descritta da un operatore Hermitiano M che agisce sullo spazio degli stati del sistema.

Misurazione Quantistica

In quanto Hermitiano, l'operatore ammette una decomposizione spettrale

$$M = \sum mP_m$$

dove P_m è l'operatore di proiezione sull'autospazio di M associato all'autovalore m. I possibili risultati della misura corrispondono agli autovalori m.

Se si misura il sistema nello stato $|\psi\rangle$, la probabilità di ottenere il risultato m è $p(m) = \langle\psi|P_m|\psi\rangle$. Una volta ottenuto il risultato m, lo stato del sistema immediatamente dopo la misura diventa

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$$

Ancora sulla Misurazione Quantistica

Una maniera pragmatica di descrivere una Misurazione Quantistica consiste nel fissare una base ortonormale nello spazio degli stati, in tal caso i proiettori non sono nient'altro che le applicazioni che associano ad un vettore le sue componenti lungo un vettore di base. Il risultato di una misura rispetto a tale base è semplicemente una etichetta i che identifica un particolare vettore di tale base.
Immediatamente dopo la misura lo stato $|\psi\rangle$ del sistema si troverà nello stato che corrisponde alla proiezione del ket $|\psi\rangle$ sul vettore $|i\rangle$.

Esempio 1

Sia $\mathcal{H}$ uno spazio di Hilbert bidimensionale e $|\psi\rangle \in \mathcal{H}$.
Misurare un sistema nello stato $|\psi\rangle$ rispetto alla base $\{|0\rangle, |1\rangle\}$, ovvero gli autostati della matrice Z, significa ottenere il risultato '0' con probabilità $|\langle 0|\psi\rangle|^2$ ed in tal caso lo stato del sistema diventa $|0\rangle$; analogamente, si otterrà il risultato '1' con probabilità $|\langle 1|\psi\rangle|^2$ ed in tal caso lo stato del sistema diventa $|1\rangle$.

Se lo stato del sistema è rappresentato dal vettore $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, allora il risultato '0' e il risultato '1' si otterranno entrambi con probabilità $1/2$.

Esercizio. Verificare l'ultimo risultato.

Osservazione 1

È importante osservare che una volta effettuata la prima misura, una successiva misura effettuata ripetto alla medesima base darà sempre lo stesso risultato con probabilità 1.
In altre parole, effettuare la stessa misura più di una volta non aumenta l'informazione che abbiamo ottenuto dopo la prima.

Sistemi composti

Quest'ultimo postulato descrive come costruire lo spazio degli stati di un sistema composto ottenuto mediante l'unione di due sistemi più semplici.

Postulato 4

Lo spazio degli stati di un sistema composto è il prodotto tensoriale degli spazi degli stati dei componenti il sistema. Inoltre dati n sistemi preparati negli stati $|\psi_i\rangle$ lo stato composto mediante l'unione di questi n stati è $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Entanglement quantistico

Il Postulato 4 permette di introdurre un concetto relativo ai sistemi composti che non ha corrispondenti dal punto di vista classico.
Consideriamo, per esempio, uno stato formato da due qubits

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Questo stato *non* può essere espresso come il prodotto di due qubits, ovvero non è possibile trovare $|a\rangle$, $|b\rangle$ tali che

$$|\psi\rangle = |a\rangle|b\rangle.$$

L'utilizzo dell'entanglement consente di introdurre il primo risultato che sembra non avere equivalenti dal punto di vista classico.

Codifica superdensa

Questo schema di comunicazione coinvolge due entità, convenzionalmente note come 'Alice' e 'Bob'.
Alice vorrebbe inviare a Bob un messaggio contenente due bits classici ma ha a disposizione soltanto un canale di comunicazione quantistica e per di più le è permesso di inviare un solo qubit.
Una maniera di ottenere questo risultato consiste nel seguire la procedura seguente.

Codifica superdensa

La risorsa dell'Entanglement

Supponiamo che Alice e Bob condividano una coppia di qubits in uno stato entangled. Per esempio

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Alice è in possesso del primo qubit e Bob del secondo.

Codifica superdensa

La ricetta

In funzione del messaggio che Alice vuole mandare, Alice eseguirà una trasformazione unitaria sul qubit in suo possesso.
Se vuole mandare la coppia 00 applica l'identità;
se vuole mandare la coppia 01 applica Z;
se vuole mandare la coppia 10 applica X;
ed infine, se vuole mandare la coppia 11 applica iY.

La base di Bell

Il risultato di queste trasformazioni è il seguente

$$00 : |\psi\rangle \xrightarrow{I\otimes I} \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$01 : |\psi\rangle \xrightarrow{Z\otimes I} \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$10 : |\psi\rangle \xrightarrow{X\otimes I} \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$11 : |\psi\rangle \xrightarrow{iY\otimes I} \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Questi quattro stati formano una base ortonormale nota come *Base di Bell*, e quindi possono essere riconosciuti senza ambiguità da una misurazione quantistica.
A questo punto Alice manda a Bob il suo qubit trasformato e Bob effettua una misura dello stato così ottenuto rispetto alla base di Bell.
A seconda del risultato ottenuto Bob capirà quale coppia di bit è il messaggio inviato da Alice.
Vale la pena ripetere che tale comunicazione tra Alice e Bob è stata ottenuta inviando *un solo* qubit di informazione.

Inutile origliare

Supponiamo che una terza entità, Eve, voglia ottenere informazioni sul messaggio inviato da Alice a Bob.
Una interessante proprietà di questo protocollo di comunicazione consiste nel fatto che non è possibile per una terza parta inferire, anche parzialmente, quale messaggio Alice abbia inviato a Bob semplicemente misurando il qubit di Alice.
Infatti l'unica cosa che Eve può fare è misurare il qubit inviato da Alice a Bob durante il suo trasferimento lungo il canale quantistico.
Tele misura può essere effettuata con un operatore hermitiano necessariamente della forma $E \otimes I$, in quanto Eve può interagire esclusivamente con il qubit che è stato manipolato da Alice.
Con un semplice calcolo si può verificare che, se $|\psi\rangle$ è un qualsiasi elemento della base di Bell, allora

$$\langle\psi|E \otimes I|\psi\rangle = \frac{1}{\sqrt{2}}(\langle 0|E|0\rangle + \langle 1|E|1\rangle)$$

e quindi *nessuna* misurazione effettuata da Eve può rivelare informazioni sul messaggio inviato dal Alice a Bob.

Cosa significa 'Teletrasporto quantistico'

Supponiamo che Alice voglia trasmettere un qubit a Bob ma l'unica possibilità che i due hanno di comunicare è attraverso un canale classico. Inoltre, a complicare ulteriormente il problema, Alice potrebbe non conoscere il qubit che vuole trasmettere a Bob ma soltanto esserne in possesso.
Supponiamo adesso che Alice e Bob abbiano in comune una coppia *EPR*. Per esempio Alice e Bob condividono la coppia

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

e, come al solito, supponiamo Alice in possesso del primo qubit e Bob del secondo qubit.

Descrizione del Protocollo di QT

Supponiamo che lo stato da 'teletrasportare' sia $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
Unendo tale stato con quello in possesso di Alice si ottiene il nuovo stato

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\big[(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)\big] =$$

$$\frac{1}{\sqrt{2}}\big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\big].$$

A questo punto Alice si trova in possesso dei primi due qubits mentre Bob è in possesso del terzo.
Alice esegue l'operatore unitario CNOT sui due qubits in suo possesso ed ottiene il nuovo stato $|\psi_1\rangle = \frac{1}{\sqrt{2}}\big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\big]$ e quindi esegue l'operatore di Hadamard sul primo qubit ed ottiene infine lo stato $|\psi_2\rangle = \frac{1}{2}\big[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\big]$.

Lo stato $|\psi_2\rangle$ si può riscrivere in modo equivalente semplicemente raggruppando i termini in modo diverso:

$$\begin{aligned}|\psi_2\rangle =& \frac{1}{2}\big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + \\ &+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\end{aligned}$$

dove il primo fattore di ogni addendo rappresenta i qubits in possesso di Alice.
A questo punto per Alice sarà sufficiente eseguire una misura nella base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ (base standard) e trasmettere il risultato a Bob.

Infatti, per effetto della misura di Alice, lo stato di Bob collasserà in uno degli stati seguenti

$$\begin{aligned} 00 &\longmapsto |\psi(00)\rangle \equiv \alpha|0\rangle + \beta|1\rangle \\ 01 &\longmapsto |\psi(01)\rangle \equiv \alpha|1\rangle + \beta|0\rangle \\ 10 &\longmapsto |\psi(10)\rangle \equiv \alpha|0\rangle - \beta|1\rangle \\ 11 &\longmapsto |\psi(11)\rangle \equiv \alpha|1\rangle - \beta|0\rangle \end{aligned}$$

Ovviamente Bob, per sapere in quale stato si trova il suo qubit, deve essere informato del risultato della misura effettuata da Alice.

Una volta venuto a conoscenza del risultato, attraverso un canale di comunicazione classico, gli basterà eseguire una certa trasformazione unitaria in funzione della coppia di bits che gli è stata comunicata.
Bob applicherà la trasformazione identica se riceve la coppia di bits 00;
applicherà la trasformazione X se riceve la coppia 01;
applicherà la trasformazione Z se riceve la coppia 10;
ed infine applicherà in sequenza le trasformazioni X e Z, ovvero ZX, se riceve la coppia 11.
Dopo aver eseguito quest a procedura il qubit di Bob si troverà nello stato $\alpha|0\rangle + \beta|1\rangle$.

Il protocollo BB84

Descrizione del problema

Il protocollo BB84 descrive una procedura che permette lo scambio di una stringa casuale di bits di cui *solo* Alice e Bob sono a conoscenza. Questo permetterà ad Alice e Bob di effettuare una comunicazione garantita dalla segretezza.
Supponiamo che Alice e Bob desiderano scambiare una *chiave*, la stringa segreta di bits, avendo a disposizione due canali uno classico e uno quantististico.

Il protocollo BB84

Set up

- Alice ha a disposizione una stringa casuale di bits lunga $2n$.
- Alice ha a disposizione due basi di $\mathcal{H}$: la base computazionale $\{|0\rangle, |1\rangle\}$ e la base $\{|+\rangle, |-\rangle\}$.

La prima base è una base formata dagli autostati di Z.
La seconda base è una base formata dagli autostati di X.

Il protocollo BB84

Procedura

1. Alice sceglie una sequenza casuale b di bits (classici) lunga $2n$.
2. Poi sceglie, sempre in maniera random, una sequenza di X e di Z che le serviranno per codificare b.

Per esempio

0	0	1	0	1	1	1	0	1	1	0	0	0
Z	Z	X	X	X	Z	X	Z	X	X	Z	Z	X
$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$

Alice manda la stringa di qubits a Bob.
Bob, dopo averli ricevuti, esegue le seguenti operazioni.

1. Sceglie a caso una sequenza di X e Z.
2. Utilizza le basi associate ad X oppure a Z per misurare la stringa di qubits ricevuta da Alice.
3. Supponiamo che Bob utilizzi la sequenza seguente.

$$Z \quad X \quad X \quad Z \quad X \quad X \quad Z \quad Z \quad Z \quad X \quad Z \quad X \quad X$$

Questo significa che, dopo aver effettuato le misurazioni, Bob otterrà i seguenti risultati.

0	0	1	0	1	1	1	0	1	1	0	0	0
Z	Z	X	X	X	Z	X	Z	X	X	Z	Z	X
$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$
Z	X	X	Z	X	X	Z	Z	Z	X	Z	X	X
$\|0\rangle$	$\|\pm\rangle$	$\|+\rangle$	$\|0/1\rangle$	$\|+\rangle$	$\|\pm\rangle$	$\|0/1\rangle$	$\|0\rangle$	$\|0/1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|\pm\rangle$	$\|-\rangle$

Bob comunica ad Alice che ha completato la misurazione.

Nota. I simboli $|\pm\rangle$ significano che il risultato della misura di Bob può essere indistintamente $+$ oppure $-$, (ed analogamente per il simbolo $|0/1\rangle$).

A questo punto Alice e Bob comunicano, sul canale classico, la sequenza di basi che hanno rispettivamente usato.

- Alice ha usato la *sua* sequenza di basi per codificare la stringa classica mediante qubits.
- Bob ha usato la *sua* sequenza di basi per misurare la sequenza di qubits ricevuta.
- Solo quando Alice e Bob concordano sulla base utilizzata hanno la certezza che il qubit inviato da Alice e il qubit misurato da Bob coincidono.
- La probabilità che Alice e Bob concordino sulla scelta della base è $1/2$, quindi circa il 50% dei bits inviati da Alice saranno utilizzabili per la stringa segreta condivisa.

Distillazione della chiave segreta

Alice e Bob conservano solo i bits corrispondenti alle basi sulle quali erano concordi.

0	0	1	0	1	1	1	0	1	1	0	0	0
Z	Z	X	X	X	Z	X	Z	X	X	Z	Z	X
Z	X	X	Z	X	X	Z	Z	Z	X	Z	X	X

Quindi solo i bits in corrispondenza dei simboli evidenziati.
Tale sequenza è la stringa di bits classici condivisa da Alice e Bob.

Eavesdropping and noise

Se del rumore sul canale quantistico disturba i qubits trasmessi, come possono fare Alice e Bob ad accorgersene?
Bob ed Alice possono decidere di 'sacrificare' k bits della loro stringa e confrontarli attraverso una comuncazione sul canale classico.
Se una data percentuale di tali bits non sono concordi Alice e Bob possono decidere di ripetere la procedura.

Cosa potrebbe accadere invece, se Eve avesse completo accesso al canale quantistico?
Intendendo con ciò che Eve può agire sul canale quantistico utilizzando tutte le operazioni permesse dai postulati della MQ. Per avere informazioni sui qubits inviati da Alice, una terza entità che abbia accesso al canale quantistico deve necessariamente misurare i qubits e quindi perturbarli.
Misurare significa scegliere una base ed ottenere una distribuzione di probabilità.
Non essendo a conoscenza della base utilizzata da Alice, una strategia che Eve potrebbe seguire è quella di misurare in maniera casuale rispetto ad X o rispetto a Z i qubits inviati da Alice.

Eavesdropping

Analizziamo il risultato che Eve può ottenere. Anche Eve può scegliere una sequenza di basi con cui misurare i qubits inviati da Alice a Bob ma, non conoscendo in anticipo la sequenza scelta da Alice, le due sequenze daranno risultati concordi solo in un caso su quattro.
Per esempio:

0	0	1	0	1	1	1	0	1	1	0	0	0
Z	Z	X	X	X	Z	X	Z	X	X	Z	Z	X
Z	X	X	Z	X	X	Z	Z	Z	X	Z	X	X
Z	Z	X	Z	Z	X	Z	Z	X	X	X	X	X

Verificare la affidabilità

Per Alice e Bob sarà semplice verificare, almeno entro un certo limite di confidenza, se qualcuno ha tentato di scoprire la sequenza di bits che si sono trasmessi.
Come?
Semplicemente confrontando i primi k bits della stringa in loro possesso.
Questo confronto verrà fatto dichiarando pubblicamente i primi k bits e verificando se coincidono.
Ovviamente dopo questa operazione i primi k bits della stringa non saranno più utilizzabili da Alice e Bob.

No-cloning theorem

Cosa accadrebbe se potessimo copiare i qubits?
In tal caso Eve potrebbe copiare la sequenza di qubits inviata da Alice a Bob e *solo* in un secondo tempo effettuare la misura sui qubits copiati.
Il seguente teorema afferma che questa strategia non può essere seguita.

No-cloning theorem

Non esiste *nessuna* possibilità, utilizzando gli assiomi della MQ, di copiare un arbitrario qubit.

No-cloning theorem

Dimostrazione

Cosa significa copiare un qubit?
Idealmente dovrebbe significare avere un dispositivo che opera sullo stato iniziale $|\psi\rangle \otimes |s\rangle$ e restituisce lo stato finale $|\psi\rangle \otimes |\psi\rangle$.
Ovvero, dovrebbe esistere una trasformazione unitaria U che realizza la procedura di copiatura

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Supponiamo che tale procedura funzioni per due particolari qubits $|\psi\rangle$ e $|\phi\rangle$ distinti tra loro, allora

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$$

Considerando il prodotto scalare dei membri di queste equazioni si ottiene

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$$

che è valida solo se $|\psi\rangle$ e $|\phi\rangle$ sono ortogonali tra loro.

Dov'è la Luna quando nessuno la guarda?

È possibile che la MQ dia una descrizione solo parziale della realtà fisica? In tal caso questo significherebbe che la descrizione di un sistema fisico mediante i kets non è completa e dovrebbero esserci delle ulteriori 'variabili' che rappresentano caratteristiche non descritte dal vettore di stato. Utilizzando il 'buon senso' potremmo affermare che: una teoria fisica dovrebbe soddisfare una qualche definizione di Realismo.

Definizione 5

Realismo significa affermare che gli oggetti del mondo esterno hanno una esistenza del tutto indipendente dalla loro percezione.

Definizione 6

Un elemento di realtà è una caratteristica oggettiva posseduta da un sistema fisico.

Il paradosso EPR

In un articolo del 1935 i fisici Einstein, Podolksi e Rosen scrissero un articolo in cui ritenevano di aver dimostrato che la MQ non fornisce una descrizione completa della realtà.
Per ottenere tale risultato proposero un esperimento concettuale che, nelle sue linee essenziali, può essere descritto nel modo seguente.
Si consideri una coppia di qubit nel seguente stato (entangled)

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Supponiamo che il primo qubit sia in possesso di Alice e il secondo qubit di Bob.
Nota. La formulazione del paradosso EPR descritta qui di seguito è quella proposta da Bohm, e non quella originariamente descritta nell'articolo del 1935.

Elementi di realtà dei qubits

Se Alice effettua una misura dell'osservabile Z gli unici risultati possibili sono $\{+1, -1\}$.
Se Alice ottenesse il risultato $+1$ e a questo punto Bob effettuasse una misura di Z sul qubit in suo possesso otterrebbe *certamente* il risultato -1.
EPR deducono che il secondo qubit deve avere già la proprietà misurata perchè altrimenti questo significherebbe che il qubit in possesso di Bob sarebbe stato influenzato dalla misura effettuata sul qubit di Alice.

Elementi di realtà

Seguendo le regole del "buon senso" (ovvero che la Realtà soddisfi l'Assioma del Realismo definito nella definizione 6) EPR affermano che, poichè sappiamo prevedere quale sarà il risultato della misura sul qubit di Bob, non è necessario effettuarla.
Inoltre, la caratteristica fisica descritta dall'osservabile Z deve essere un elemento di realtà.
Si può dimostrare che se Alice effettua una misura $v_x X + v_y Y + v_z Z$ lungo la direzione $\vec{v}$ e ottiene come risultato $+1$ allora si può predire con certezza che Bob otterrà il risultato -1 come risultato della stessa misura sul qubit in suo possesso.

La disuguaglianza di Bell vs MQ

A questo punto il ragionamento di EPR è il seguente: vi abbiamo mostrato che, anche se non possiamo misurare simultaneamente Z e X, questi sono elementi di realtà e quindi in una teoria completa entrambi tali valori dovrebbero essere parte della descrizione del sistema fisico.
Poichè questo non si verifica in MQ ne segue che la MQ non può essere considerata una teoria completa.

La disuguglianaza di Bell

Esiste un modo sperimentale per decidere se la Natura si trova d'accordo con la MQ oppure con EPR?
La risposta è si e lo strumento utilizzato per dirimere tale questione è la disuguaglianza di Bell.
Vale la pena osservare che la Disuguaglianza di Bell non è un risultato rigurdante la MQ ma un risultato ottenuto seguendo le regole del "buon senso" e quindi una conseguenza delle caratteristiche a cui la Natura dovrebbe obbedire secondo EPR.

Preparazione dell'esperimento

Immaginiamo di eseguire il seguente esperimento. Charlie prepara due particelle e manda la prima ad Alice e la seconda a Bob.
Una volta ricevuta la particella Alice ha a disposizione due apparati di misura che le consentono di misurare le caratteristiche fisiche P_R e P_Qe i risultati che può ottenere sono solo $+1$ e -1.
Se Alice misura Q per la proprietà P_Q assumiamo che questa sia una caratteristica oggettiva della particella in possesso di Alice.
Analogamente supponiamo che Bob abbia a disposizione gli apparati per misurare le proprietà P_S e P_T e, anche in tal caso, gli unici risultati che può ottenere sono $+1$ e -1.
L'eperimento è progettato in modo che Alice e Bob effettuino le loro misure in modo casuale e simultaneamente.

Algebra elementare

La quantità $QS + RS + RT - QT$ è ovviamente

$$QS + RS + RT - QT = (Q + R)S - (R - Q)T$$

e quindi può assumere solo i valori $+2$ oppure -2.
Supponiamo che $p(q, r, s, t)$ sia la probabilità che, prima che le misure siano effettuate, il sistema sia in uno stato corrispondente a $Q = q$, $R = r$, $S = s$, $T = t$.
In ogni caso, se $E(\cdot)$ rappresenta il valor medio di una variabile casuale, si avrà

$$E(QS + RS + RT - QT) = \sum_{q,r,s,t} p(q, r, s, t)(qs + rs + rt - qt) \leq$$

$$\leq \left(\sum_{q,r,s,t} p(q, r, s, t) \right) 2 = 2$$

La Disuguaglianza di Bell

Inoltre, per la proprietà di linearità del valor medio si ha

$$E(QS + RS + RT - QT) = E(QS) + E(RS) + E(RT) - E(QT)$$

e quindi si ottiene finalmente la Disuguaglianza di Bell

$$E(QS) + E(RS) + E(RT) - E(QT) \leq 2$$

La risposta della MQ

Se supponiamo di eseguire le misure delle seguenti osservabili

$$Q = Z_1 \quad R = X_1 \quad S = \frac{-Z_2 - X_2}{\sqrt{2}} \quad T = \frac{Z_2 - X_2}{\sqrt{2}}$$

sullo stato $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$.

Nota. L'indice 1 significa che la misura viene effettuata sul qubit di Alice e l'indice 2 sul qubit di Bob.

La MQ prevede per tali grandezze i seguenti valori medi

$$E(Q \otimes S) = \frac{1}{\sqrt{2}} \quad E(R \otimes S) = \frac{1}{\sqrt{2}} \quad E(R \otimes T) = \frac{1}{\sqrt{2}} \quad E(Q \otimes T) = -\frac{1}{\sqrt{2}}$$

da cui

$$E(QS) + E(RS) + E(RT) - E(QT) = 2\sqrt{2}$$

Ovviamente $2 < 2\sqrt{2}$

Si può effettuare un esperimento e chiedere alla Natura di dire chi ha ragione.
Chi ha ragione?
Anche in questo caso, tutti gli eseprimenti effettuati concordano con le previsioni della MQ in quanto la disuguaglianza di Bell viene violata.

Bibliografia


Michael A. Nielsen, and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 10th Anniversary Edition, 2011.