



UNIVERSITÀ DEGLI STUDI DI UDINE

Scuola Superiore

Elaborato di Fine Anno

Meccanica quantistica e misure di
entanglement

RELATORE
Prof.ssa Carla Piazza
TUTOR
Prof. Pietro Corvaja

STUDENTE
Cristian Curaba

Anno Accademico 2020/2021

Indice

1	I postulati della meccanica quantistica	3
1.1	Gli stati di un sistema	3
1.2	Evoluzione	3
1.3	Misurazioni quantistiche	4
1.4	Sistemi composti	9
2	Gli operatori di densità e relative proprietà	11
2.1	Gli operatori di densità	11
2.2	Gli operatori di densità ridotti	17
2.3	La decomposizione di Schmidt	18
2.4	Purificazione	20
3	Quantificazione di entanglement	21
3.1	Il paradosso EPR e la disuguaglianza di Bell	22
3.2	Operatori di misura in generale	24
3.3	Correlazioni tra stati quantistici	26
3.4	Misure monotone di entanglement	27
3.5	Il teletrasporto quantistico	32

Introduzione

Il termine entanglement (letteralmente, in inglese, "groviglio", "intreccio") fu introdotto da Erwin Schrödinger in una recensione del famoso articolo sul paradosso EPR che, nel 1935, rivelò a livello teorico il fenomeno. L'entanglement quantistico è alla base di tecnologie emergenti come i computer quantistici e la crittografia quantistica ed ha permesso esperimenti relativi al teletrasporto quantistico, su cui si appuntano le speranze di nuove tecnologie. Sebbene non si possa trasmettere informazione attraverso il solo entanglement, l'utilizzo di un canale di comunicazione classico in congiunzione con uno stato entangled permette il teletrasporto di uno stato quantistico, che sarebbe altrimenti impossibile poiché richiederebbe un'infinita quantità di informazione per essere determinato. All'atto pratico, come conseguenza del teorema di no-cloning quantistico, questa ricca informazione non può comunque essere letta integralmente, ma può tuttavia essere impiegata nei calcoli.

Inizialmente si presentano i postulati della meccanica quantistica, i quali offrono una descrizione chiara e formale della teoria su cui si realizzano i fenomeni di entanglement. Successivamente si fornirà il formalismo degli operatori di densità e alcune delle proprietà fondamentali affinché sia possibile una descrizione efficace di stati mischiati di sistemi quantistici e delle loro trasformazioni. Si illustrerà il paradosso EPR e la teoria delle variabili nascoste, dimostrata inconsistente con le previsioni della meccanica quantistica (che si rivela "corretta" sperimentalmente) da Bell nel 1964 nell'articolo intitolato: "On the Einstein Podolsky Rosen Paradox". Infine vengono proposte delle misure di entanglement limitatamente al caso di sistemi bipartiti, puntualizzando la complessità nel realizzare una misura estesa a più sistemi quantistici a causa del quale, in letteratura, esistono un gran numero di misure diverse. L'elaborato termina con una delle applicazioni più sorprendenti degli stati entangled: il teletrasporto quantistico.

1 I postulati della meccanica quantistica

In seguito si fornisce una formalizzazione matematica che permette una descrizione rigorosa della meccanica quantistica.

1.1 Gli stati di un sistema

Il primo postulato definisce lo spazio nel quale la meccanica quantistica si sviluppa. Lo spazio ha la struttura di uno spazio di Hilbert.

Postulato 1: Lo stato di un sistema fisico isolato è rappresentato, in un fissato tempo t , da un *vettore di stato* $|\psi\rangle$ appartenente ad un sistema di Hilbert \mathcal{H} , detto *spazio degli stati*.

Il più semplice sistema quantistico, analogo del 'bit' classico, è il *qubit*. Un qubit è lo stato di uno spazio 2-dimensionale su campo complesso. Supponiamo $|0\rangle$ ed $|1\rangle$ formino una base ortonormale per lo stato del sistema. Allora un arbitrario vettore di stato dello spazio può essere scritto come

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

dove a e b sono numeri complessi. La condizione per cui $|\psi\rangle$ sia un vettore unitario, cioè $\langle\psi|\psi\rangle = 1$, può essere riscritta come $||a||^2 + ||b||^2 = 1$. Intuitivamente, gli stati $|0\rangle$ e $|1\rangle$ devono essere pensati come i due bit classici 0 ed 1. Tuttavia i qubit quantistici differiscono da quelli classici per quella che viene definita *sovrapposizione degli stati*. Infatti ogni qubit può esistere in una sovrapposizione degli stati $|0\rangle$ ed $|1\rangle$ e solo in seguito ad una misurazione il qubit collassa in un singolo stato. Si dice che ogni combinazione lineare $\sum_i \alpha_i |\psi_i\rangle$ è in sovrapposizione degli stati $|\psi_i\rangle$ con *ampiezza* α_i per ciascun stato $|\psi_i\rangle$.

1.2 Evoluzione

Il seguente postulato fornisce una descrizione di come un determinato stato di un sistema possa subire modifiche nel tempo.

Postulato 2: L'evoluzione di un sistema *chiuso* è descritto da una *trasformazione unitaria*. Ovvero, uno stato $|\psi\rangle$ di un sistema al tempo t_1 è trasformato allo stato $|\psi'\rangle$ del sistema al tempo t_2 da un operatore unitario U che dipende esclusivamente da t_1 e t_2 ,

$$|\psi'\rangle = U|\psi\rangle.$$

Risulta inoltre che ad ogni operatore unitario è possibile associare un sistema fisico reale. Il postulato 2 richiede che un sistema sia chiuso, ovvero che non

ci siano interazioni con altri sistemi, il che, nel caso reale, è possibile solo con buona approssimazione. Si può enunciare il secondo postulato evidenziando una descrizione continua dell'evoluzione di un sistema quantistico mediante *l'equazione di Schrödinger*.

Postulato 2': L'evoluzione temporale dello stato di un sistema quantistico chiuso è descritta dall'equazione di Schrödinger,

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle.$$

In questa equazione, \hbar è la nota costante di Planck il cui valore è sperimentalmente determinato, mentre H è un fissato operatore Hermitiano detto *Hamiltoniano* di un sistema chiuso. Nota la costante e l'operatore è dunque possibile prevedere completamente la dinamica del sistema. Concretamente, la descrizione dell'Hamiltoniano è un problema complesso che esula dall'obiettivo di questo elaborato.

La connessione tra le due formulazioni del medesimo postulato è data dalla corrispondenza biunivoca tra le soluzioni dell'equazione di Schrödinger e l'insieme degli operatori lineari.

Si nota che, nonostante il postulato ammetta tra le ipotesi un sistema chiuso, concretamente una trasformazione dello stato di un sistema è possibile solo attraverso l'interazione con altri sistemi.

1.3 Misurazioni quantistiche

Trasformazioni non lineari sono possibili per mezzo di interazioni di vari sistemi. È dunque necessario, per l'osservazione dello stato di sistema, un'interazione con dei sistemi introdotti nel terzo postulato.

Postulato 3: Misurazioni quantistiche sono descritte da una collezione $\{M_m\}$ di *operatori di misurazione*. Questi operano sullo stato del sistema che si sta misurando. L'indice m , si riferisce ai possibili risultati che possono occorrere a seguito della misurazione. Dato uno stato di un sistema quantistico $|\psi\rangle$, la probabilità che il risultato della misurazione sia m è dato da

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle,$$

e lo stato del sistema dopo la misurazione è

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}.$$

Gli operatori di misura soddisfano *l'equazione di completezza*,

$$\sum_m M_m^\dagger M_m = I.$$

L'equazione di completezza esprime il fatto che la somma di tutte le probabilità sia 1:

$$1 = \sum_m p(m) = \sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle.$$

Proposizione 1.1. *Supponiamo $\{L_l\}$ e $\{M_m\}$ siano due insiemi di operatori di misura. Allora una misurazione definita da M_l seguita da una misurazione da L_m è equivalente ad una misurazione di una collezione di operatori $\{N_{lm}\}$ rappresentati da $N_{lm} = M_m L_l$.*

Dimostrazione. Sia $|\psi\rangle$ un generico stato. Si ha che $p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$ e lo stato $|\psi'\rangle$ a seguito della misurazione da M_m è

$$|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}.$$

Segue la misurazione da L_l che trasforma lo stato in

$$|\psi''\rangle = \frac{L_l M_m |\psi\rangle}{p(l)}$$

con $p(l) = \langle \psi' | L_l^\dagger L_l | \psi' \rangle$ diventa

$$\frac{L_l M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger L_l^\dagger L_l M_m | \psi \rangle}}$$

equivalente alla singola misurazione con l'operatore $N_{lm} = L_l M_m$. Resta da dimostrare che la collezione degli operatori $\{N_{lm}\}$ soddisfi la relazione di completezza, il che segue banalmente dalle relazioni di completezza dei due insiemi di operatori di misura. \square

Proposizione 1.2. *Siano $|\psi_i\rangle$ ($1 \leq i \leq n$) un insieme di stati noto e supponiamo che $|\psi_i\rangle$ siano ortonormali. Allora esiste una procedura per distinguere uno di questi stati dagli altri.*

Dimostrazione. Definiamo gli operatori di misura $M_i = |\psi_i\rangle \langle \psi_i|$, uno per ogni possibile indice i ed un'addizionale operatore di misura M_0 tale per cui $(M_0)^2 = I - \sum_{i \neq 0} |\psi_i\rangle \langle \psi_i|$. Questi operatori soddisfano la relazione di completezza (verifica banale). Se è preparato lo stato $|\psi_i\rangle$, allora $p(j) = \langle \psi_i | M_j | \psi_i \rangle = \delta_{ij}$ con certezza. \square

D'altro canto, se gli stati $|\psi_i\rangle$ non sono ortogonali allora possiamo dimostrare che non esiste una procedura per distinguere con certezza uno stato dagli altri.

Proposizione 1.3. *Vi sono stati non ortogonali i cui elementi non possono essere distinti con certezza.*

Dimostrazione. Procediamo con una dimostrazione all'assurdo. Siano ψ_1 e ψ_2 due stati non ortogonali e supponiamo per assurdo esistano degli operatori di misura $\{E_j\}$ tali per cui $\sum_j E_j = I$ con $p(i) = \langle \psi_i | E_j | \psi_i \rangle = \delta_{ij}$. Consideriamo la decomposizione $|\psi_2\rangle = a|\psi_1\rangle + b|\phi\rangle$, con $|\phi\rangle$ ortonormale ad $|\psi_1\rangle$, $a^2 + b^2 = 1$ e $b < 1$ (ipotesi di non ortogonalità). Allora $\sqrt{E_2}|\psi_2\rangle = b\sqrt{E_2}|\phi\rangle$, che implica una contraddizione visto che

$$\langle \psi_2 | E_2 | \psi_2 \rangle = ||b||^2 \langle \phi | E_2 | \phi \rangle \leq ||b||^2 < 1.$$

□

Un'importante classe di operatori di misura è detta *operatori di misura di proiezione*. Questa classe, considerando i risultati del secondo postulato, risulta equivalente alla più generale classe di operatori introdotta nel terzo postulato.

Definizione 1.1. Operatori di misura di proiezione: *Un operatore di misura di proiezione è descritto da un osservabile M Hermitiano. L'osservabile ammette una decomposizione spettrale,*

$$M = \sum_m m P_m,$$

dove P_m è il proiettore sull'autospazio di M con autovalore m . I possibili risultati della misurazione corrispondono agli autovalori, m , dell'osservabile. Misurando lo stato $|\psi\rangle$, la probabilità di ottenere il risultato m è dato da

$$p(m) = \langle \psi | P_m | \psi \rangle.$$

Ottenuto il risultato m , lo stato del sistema collassa ad

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

È possibile riformulare il terzo postulato, aggiungendo alla relazione di completezza, la proprietà che gli operatori $\{M_m\}$ siano Hermitiani e soddisfano $M_m M_{m'} = \delta_{m,m'} M_m$ (cioè siano proiezioni ortogonali).

Gli operatori di proiezione hanno utili proprietà. In particolare, è semplice calcolare il valore medio per queste misurazioni:

$$\begin{aligned}
 \mathbf{E}(M) &= \sum_m mp(m) \\
 &= \sum_m m \langle \psi | P_m | \psi \rangle \\
 &= \langle \psi | \left(\sum_m m P_m \right) | \psi \rangle \\
 &= \langle \psi | M | \psi \rangle .
 \end{aligned}$$

Il valore medio dell'osservabile M è scritto come $\langle M \rangle = \langle \psi | M | \psi \rangle$. Da questa formula segue facilmente il calcolo per la deviazione standard sugli osservati di M :

$$\begin{aligned}
 [\Delta(M)]^2 &= \langle (M - \langle M \rangle)^2 \rangle \\
 &= \langle M^2 \rangle - \langle M \rangle^2 .
 \end{aligned}$$

Queste formulazioni di misurazioni e deviazione standard porta ad una formulazione del *principio di indeterminazione di Heisenberg*.

Notazione. Il commutatore tra due operatori A e B è definito da

$$[A, B] := AB - BA.$$

Notazione. L'anti-commutatore di due operatori A e B è definito da:

$$\{A, B\} := AB + BA.$$

Proposizione 1.4. (Teorema di simultanea diagonalizzazione) Supponiamo A e B siano operatori Hermitiani. Allora $[A, B] = 0$ se e solo se esiste una base ortonormale tale che sia A che B siano diagonali rispetto tale base.

Dimostrazione. Supponiamo esista una base ortonormale tale per cui A e B siano diagonali. Sia C la matrice del cambio di base ($C^{-1} = C^T$). Verifichiamo che

$$\begin{aligned}
 [A, B] &= 0 : \\
 [C^T A' C, C^T B' C] &= C^T A' C C^T B' C - C^T B' C C^T A' C \\
 &= C^T A' B' C - C^T B' A' C = 0
 \end{aligned}$$

Dove l'ultima uguaglianza è verificata perché matrici diagonali commutano. Supponiamo $[A, B] = 0$. Sia $|a\rangle$ base ortonormale per l'autospazio V_a di A per l'autovalore a . Si nota che

$$AB|a\rangle = BA|a\rangle = aB|a\rangle,$$

dunque $B|a\rangle$ è un elemento dell'autospazio V_a . Denotiamo P_a proiettore sullo spazio V_a e definiamo $B_a := P_a B P_a$. È banale da verificare che la restrizione di B_a su V_a è un operatore Hermitiano, dunque ammette una decomposizione spettrale. Indichiamo con $|a, b\rangle$ gli autovettori ortonormali, dove gli indici a e b indicano gli autovalori di A e B . Si nota che $B|a, b\rangle$ sono elementi di V_a , dunque $B|a, b\rangle = P_a B|a, b\rangle$. Inoltre $P_a|a, b\rangle = |a, b\rangle$, quindi

$$B|a, b\rangle = P_a B P_a|a, b\rangle = b|a, b\rangle.$$

Segue che $|a, b\rangle$ sono autovettori di B con autovalore b , dunque $|a, b\rangle$ è un insieme di autovettori ortonormali sia per A che per B . \square

Teorema 1.1. (Principio di indeterminazione di Heisenberg) Siano C e D due osservabili. Allora vale la disuguaglianza:

$$\Delta(C)\Delta(D) \geq \frac{|\langle \psi | [C, D] | \psi \rangle|}{2}.$$

Dimostrazione. Supponiamo A e B siano due operatori Hermitiani e $|\psi\rangle$ sia un vettore di stato. Supponiamo $\langle \psi | AB | \psi \rangle = x + iy$, con $x, y \in \mathbb{R}$. Notiamo che $\langle \psi | [A, B] | \psi \rangle = 2iy$ e $\langle \psi | \{A, B\} | \psi \rangle = 2x$. Questo implica che

$$|\langle \psi | [A, B] | \psi \rangle|^2 + |\langle \psi | \{A, B\} | \psi \rangle|^2 = 4|\langle \psi | AB | \psi \rangle|^2 = x + iy.$$

Per la disuguaglianza di Cauchy-Schwarz

$$|\langle \psi | AB | \psi \rangle|^2 \leq \langle \psi | A^2 | \psi \rangle \langle \psi | B^2 | \psi \rangle,$$

che combinata con la precedenza uguaglianza, tralasciando il secondo termine non negativo della somma, si ottiene

$$|\langle \psi | [A, B] | \psi \rangle|^2 \leq 4 \langle \psi | A^2 | \psi \rangle \langle \psi | B^2 | \psi \rangle.$$

Supponiamo C e D due osservabili. Sostituendo $A = C - \langle C \rangle$ e $B = D - \langle D \rangle$ nell'ultima equazione, si ottiene una formulazione del principio di Heisenberg:

$$\Delta(C)\Delta(D) \geq \frac{|\langle \psi | [C, D] | \psi \rangle|}{2}.$$

La corretta interpretazione della precedente disuguaglianza è la seguente: se si preparano un grande numero di sistemi quantici nello stesso stato, $|\psi\rangle$, e poi si produce una misurazione di C in alcuni di questi stati e D in altri, allora il prodotto tra la deviazione standard $\Delta(C)$ dei risultati di C e la deviazione standard $\Delta(D)$ dei risultati di D soddisferà la disuguaglianza sopra. \square

Positive Operator-Valued Measure. Supponiamo che una misurazione, descritta dagli operatori $\{M_m\}$, operi su un sistema quantistico di stato $|\psi\rangle$. Allora la probabilità di ottenere m è dato da $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$. Supponiamo di definire

$$E_m := M_m^\dagger M_m.$$

Allora, dal terzo postulato e in seguito a proprietà di algebra lineare, si ottiene che E_m sono operatori positivi che soddisfano $\sum_m E_m = I$ e $p(m) = \langle\psi| E_m |\psi\rangle$. Quindi gli operatori E_m sono sufficienti per determinare le probabilità di ciascun possibile risultato di una misurazione, mentre non si può determinare lo stato del sistema al seguito del collasso della misurazione. L'insieme completo degli operatori $\{E_m\}$ è detto POVM.

1.4 Sistemi composti

Il seguente postulato descrive come si costruisce lo spazio di un sistema composto da più componenti quantistici.

Postulato 4: Lo stato di un sistema fisico composto è il prodotto tensoriale degli stati delle sue componenti. Ovvero dati n stati $|\psi_i\rangle$ ($1 \leq i \leq n$), allora lo stato del sistema totale è $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Notazione. $|\psi_1\rangle |\psi_2\rangle := |\psi_1\rangle \otimes |\psi_2\rangle$. Un'altra possibile notazione per un sistema composto è $|\psi_1\psi_2\rangle$.

Proposizione 1.5. *Le proiezioni, insieme alle trasformazioni unitarie, sono sufficienti ad implementare una generale misurazione.*

Dimostrazione. La dimostrazione fa uso di un sistema composto. Supponiamo di avere uno spazio quantistico Q , e vogliamo svolgere una misurazione descritta dagli operatori $\{M_m\}$ sul sistema Q . Introduciamo un *sistema ancilla*, con stato M , di base ortonormale $|m\rangle$ in corrispondenza biettiva con i possibili risultati della misurazione che vogliamo implementare. Sia $|0\rangle$ qualunque stato fissato di M , definiamo un operatore U su $|\psi\rangle |0\rangle$, con $|\psi\rangle$ stato di Q nel seguente modo:

$$U |\psi\rangle |0\rangle := \sum_m M_m |\psi\rangle |m\rangle.$$

Usando l'ortonormalità degli stati $|m\rangle$ e la relazione di completezza $\sum_m M_m^\dagger M_m = I$, possiamo vedere che U preserva il prodotto interno tra gli

stati della forma $|\psi\rangle|0\rangle$,

$$\begin{aligned}\langle\phi|\langle 0|U^\dagger U|\psi\rangle|0\rangle &= \sum_{m,m'} \langle\psi|M_m^\dagger M_{m'}|\psi\rangle \langle m|m'\rangle \\ &= \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle \\ &= \langle\psi|\psi\rangle.\end{aligned}$$

U può essere esteso ad un operatore lineare su tutto $Q \otimes M$ che denoteremo sempre con U . Adesso supponiamo di effettuare una misurazione sui due sistemi descritti dalle proiezioni $P_m := I_Q \otimes |m\rangle\langle m|$. Si ottiene m con probabilità

$$\begin{aligned}p(m) &= \langle\psi|\langle 0|U^\dagger P_m U|\psi\rangle|0\rangle \\ &= \sum_{m',m''} \langle\psi|M_{m'}^\dagger \langle m'| (I_Q \otimes |m\rangle\langle m|) M_{m''} |\psi\rangle |m''\rangle \\ &= \langle\psi|M_m^\dagger M_m|\psi\rangle,\end{aligned}$$

come si ottiene dal terzo postulato. Inoltre lo stato del sistema QM dopo misurazione è dato da

$$\frac{P_m U|\psi\rangle|0\rangle}{\sqrt{\langle\psi|U^\dagger P_m U|\psi\rangle}} = \frac{M_m|\psi\rangle|0\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}.$$

□

Il quarto postulato permette inoltre di definire uno dei più interessanti puzzle dei sistemi quantistici composti: l'*entanglement*. Ad esempio, considerando lo stato a due qubit

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

si può facilmente dimostrare che non esistono due qubit singoli $|a\rangle, |b\rangle$ tali per cui $|\psi\rangle = |a\rangle|b\rangle$ (basta svolgere il prodotto tensoriale tra due generici stati e confrontarlo con lo stato di $|\psi\rangle$ per dedurre un assurdo). Uno stato composito che non si può scomporre come prodotto tensoriale di componenti è detto *entangled state*.

2 Gli operatori di densità e relative proprietà

2.1 Gli operatori di densità

È possibile formalizzare (in maniera equivalente) la meccanica quantistica facendo uso degli *operatori di densità* o *matrici di densità* invece che dei vettori di stato. Gli operatori di densità forniscono un modo conveniente per descrivere sistemi quantistici il cui stato non è completamente noto. Più precisamente, supponiamo che un sistema quantistico si trovi nello stato $|\psi_i\rangle$ con probabilità p_i . Chiameremo $\{p_i, |\psi_i\rangle\}$ un aggregato di stati puri. L'operatore di densità per il sistema è definito dall'equazione

$$\rho := \sum_i p_i |\psi_i\rangle \langle \psi_i|.$$

Risulta che tutti i postulati possano essere riformulati utilizzando gli operatori di densità. Supponiamo, per esempio, che l'evoluzione di un sistema quantistico chiuso sia descritto da un operatore unitario U . Se il sistema si trovava inizialmente nello stato $|\psi_i\rangle$ con probabilità p_i , allora in seguito all'evoluzione lo stato del sistema sarà $U|\psi_i\rangle$ con probabilità p_i . L'operatore di densità è descritto dall'equazione:

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle \langle \psi_i| U^\dagger = U\rho U^\dagger.$$

Anche le misurazioni sono facilmente descrivibili dagli operatori di densità. Supponiamo di effettuare una misurazione descritta dagli operatori $\{M_m\}$. Se lo stato iniziale era $|\psi_i\rangle$, allora la probabilità di ottenere il risultato m è

$$p(m|i) = \langle \psi_i | M_m^\dagger M_m | \psi_i \rangle = \text{tr}(M_m^\dagger M_m |\psi_i\rangle \langle \psi_i|),$$

da cui

$$\begin{aligned} p(m) &= \sum_i p(m|i)p_i \\ &= \sum_i \text{tr}(M_m^\dagger M_m |\psi_i\rangle \langle \psi_i|) p_i \\ &= \text{tr}(M_m^\dagger M_m \rho). \end{aligned}$$

Se lo stato del sistema era $|\psi_i\rangle$ allora, dopo aver ottenuto il risultato m , si trasforma in

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle}}.$$

Quindi, dopo una misurazione che porta al risultato m , si ottiene un aggregato di stati $|\psi_i^m\rangle$ con probabilità $p(i|m)$. Il corrispondente operatore di densità ρ_m è

$$\rho_m = \sum_i p(i|m) |\psi_i^m\rangle \langle \psi_i^m| = \sum_i p(i|m) \frac{M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger}{\langle \psi_i| M_m^\dagger M_m |\psi\rangle}.$$

Applicando la relazione $p(m|i) = p(i|m)/p(m)$ fornita dalla teoria della probabilità si ottiene

$$\begin{aligned} \rho_m &= \sum_i p_i \frac{M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)} \\ &= \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}. \end{aligned}$$

Definizione 2.1. *Un sistema quantistico il cui stato $|\psi\rangle$ è noto per certo è detto stato puro. L'operatore di densità di tale stato è $\rho = |\psi\rangle \langle \psi|$. Altrimenti un sistema è in uno stato detto stato mischiato. Si dice che vi è un miscuglio di differenti stati puri aggregati per ρ .*

L'esempio in seguito mostra la comodità nel descrivere uno stato mischiato facendo uso degli operatori di densità. Supponiamo che la registrazione del risultato m a seguito di una misurazione sia perso. Otterremmo un sistema quantistico nello stato ρ_m con probabilità $p(m)$, ma non conoscendo l'attuale valore di m . Lo stato di questo sistema quantistico può dunque essere descritto dall'operatore di densità:

$$\begin{aligned} \rho &= \sum_m p(m) \rho_m \\ &= \sum_m \text{tr}(M_m^\dagger M_m \rho) \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)} \\ &= \sum_m M_m \rho M_m^\dagger. \end{aligned}$$

È possibile descrivere la meccanica quantistica facendo esclusivamente uso degli operatori di densità, tralasciando i vettori di stato e l'interpretazione degli operatori di densità come aggregazioni di vettori di stato.

La classe degli operatori di densità è caratterizzata dal seguente utile teorema:

Teorema 2.1. (di caratterizzazione delle matrici di densità) *Un operatore hermitiano ρ è un operatore di densità associato all'aggregato $\{p_i, |\psi_i\rangle\}$ se e solo se soddisfa le seguenti condizioni:*

1. $tr(\rho) = 1$.

2. ρ è un operatore positivo.

Dimostrazione. Supponiamo $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ sia un operatore di densità. Allora

$$tr(\rho) = \sum_i p_i tr(|\psi_i\rangle \langle \psi_i|) = \sum_i p_i = 1.$$

Supponiamo $|\phi\rangle$ sia un generico vettore di stato. Allora

$$\begin{aligned} \langle \phi | \rho | \phi \rangle &= \sum_i p_i \langle \phi | \psi_i \rangle \langle \psi_i | \phi \rangle \\ &= \sum_i p_i |\langle \phi | \psi_i \rangle|^2 \geq 0. \end{aligned}$$

Viceversa, supponiamo ρ sia un operatore positivo con $tr(\rho) = 1$. Siccome ρ è positivo, deve avere una decomposizione spettrale

$$\rho = \sum_j \lambda_j |j\rangle \langle j|,$$

dove i vettori $|j\rangle$ sono ortogonali, $\lambda_j \in \mathbb{R}$ autovalori non negativi di ρ . Dalla condizione sulla traccia si ottiene $\sum_j \lambda_j = 1$. Dunque ρ è l'operatore di densità dell'aggregato $\{\lambda_j, |j\rangle\}$. \square

Da questo teorema si ottiene una proprietà intrinseca degli operatori di densità che esula dalla costruzione con i vettori di stato.

Definizione 2.2. *Un operatore hermitiano si definisce di densità se è positivo e di traccia pari ad uno.*

Si riformulano in seguito i postulati della meccanica quantistica:

Postulato 1: Ad ogni sistema fisico isolato vi è associato uno spazio di Hilbert. Lo stato del sistema è completamente descritto dal suo *operatore di densità*. Se un sistema si trova nello stato ρ_i , con probabilità p_i , allora l'operatore di densità per il sistema è $\sum_i p_i \rho_i$.

Postulato 2: L'evoluzione di un sistema quantistico *chiuso* è descritto da una *trasformazione unitaria*. Cioè, lo stato ρ del sistema al tempo t_1 è trasformato nello stato del sistema ρ' al tempo t_2 da un operatore unitario U che dipende da t_1 e t_2 ,

$$\rho' = U \rho U^\dagger. \quad (1)$$

Postulato 3: Misurazioni quantistiche sono descritte da una collezione $\{M_m\}$ di *operatori di misura*. Questi operatori agiscono sulla stato dello

spazio in misurazione. L'indice m si riferisce a tutti i possibili risultati che possono occorrere a seguito di una misurazione. Gli operatori di misura devono soddisfare la *relazione di completezza*,

$$\sum_m M_m^\dagger M_m = I.$$

Se lo stato di un sistema quantistico è ρ , allora la probabilità che il risultato m occorra è dato da

$$p(m) = \text{tr}(M_m^\dagger M_m \rho).$$

Lo stato del sistema, una volta misurato m , collassa ad

$$\frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}. \quad (2)$$

Postulato 4: Lo stato di uno spazio fisico composto è descritto dal prodotto tensoriale degli stati dei sistemi fisici che compongono il sistema totale.

Proposizione 2.1. *Sia ρ un operatore di densità. Allora vale $\text{tr}(\rho^2) \leq 1$. L'uguaglianza è vera se e solo se ρ è uno stato puro.*

Dimostrazione. Considero la decomposizione spettrale $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$. Allora vale che

$$\text{tr}(\rho^2) = \sum_i p_i^2 |\langle \psi_i | \psi_i \rangle|^2 \leq \left(\sum_i p_i^2 \right) \leq 1.$$

Si nota che l'uguaglianza vale se e solo se vi è un unico p_i , cioè lo stato è puro. \square

Osservazione. *Due differenti aggregati di stati quantistici possono generare la stessa matrice di densità. Ad esempio:*

$$\rho = \frac{3}{4} |0\rangle \langle 0| + \frac{1}{4} |1\rangle \langle 1|$$

non determina necessariamente che ρ debba essere nello stato $|0\rangle$ con probabilità $3/4$ e nello stato $|1\rangle$ con probabilità $1/4$. Infatti, definiti gli stati

$$\begin{aligned} |a\rangle &:= \sqrt{\frac{3}{4}} |0\rangle + \sqrt{\frac{1}{4}} |1\rangle \\ |b\rangle &:= \sqrt{\frac{3}{4}} |0\rangle - \sqrt{\frac{1}{4}} |1\rangle \end{aligned}$$

e considerando la matrice di densità ottenuta da

$$\frac{1}{2} |a\rangle \langle a| + \frac{1}{2} |b\rangle \langle b|$$

si ottiene proprio ρ . In generale, gli autovettori e gli autovalori indicano solo uno dei possibili aggregamenti di stati che possono originare la matrice di densità.

Notazione. Per un dato spazio di Hilbert H , l'insieme di tutti gli stati associati ad H è denotato da $S(H)$ ed è detto spazio degli stati.

Proposizione 2.2. Fissato uno spazio di Hilbert H , lo spazio degli stati è un insieme convesso, cioè dati $\rho_1, \rho_2 \in S(H)$ vale che $\lambda\rho_1 + (1 - \lambda)\rho_2$, con $\lambda \in [0, 1]$ sono inclusi in $S(H)$.

Dimostrazione. Sono stati mischiati ($\lambda + (1 - \lambda) = 1$) di stati che rappresentano uno stesso spazio di Hilbert. \square

I punti estremi di questo insieme convesso sono i proiettori uno-dimensionali di norma 1. Infatti ogni stato mischiato ρ ammette una rappresentazione del tipo

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$$

per il teorema 2.3 (Decomposizione di Schmidt). Tuttavia gli elementi di $S(H)$ non ammettono delle uniche rappresentazioni come stati mischiati dei proiettori uno-dimensionali.

È possibile classificare lo spazio degli stati che s'aggregano in una stessa matrice di densità:

Teorema 2.2. Gli insiemi $|\tilde{\psi}_i\rangle := \sqrt{p_i} |\psi_i\rangle$ e $|\tilde{\varphi}_i\rangle := \sqrt{p_i} |\varphi_i\rangle$ generano la stessa matrice di densità se e solo se

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle,$$

dove u_{ij} è una matrice unitaria di numeri complessi.

Dimostrazione. Supponiamo $|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle$ per qualche matrice unitaria u_{ij} . Allora

$$\begin{aligned} \sum_i |\tilde{\psi}_i\rangle \langle \tilde{\psi}_i| &= \sum_{ijk} u_{ij} u_{jk}^* |\tilde{\varphi}_j\rangle \langle \tilde{\varphi}_k| \\ &= \sum_{jk} \left(\sum_i u_{ki}^\dagger U_{ij} \right) |\tilde{\varphi}_j\rangle \langle \tilde{\varphi}_k| \\ &= \sum_{jk} \delta_{kj} |\tilde{\varphi}_j\rangle \\ &= \sum_j |\tilde{\varphi}_j\rangle \langle \tilde{\varphi}_j|, \end{aligned}$$

il che mostra che $|\tilde{\psi}_i\rangle$ e $|\tilde{\varphi}_j\rangle$ generano lo stesso operatore. \square

Notazione. Le matrici di De Pauli sono indicate come segue:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Inoltre, dato un vettore $\vec{r} \in \mathbb{R}^3$ con $\vec{r} = (r_1, r_2, r_3)^T$, si indicherà con $\vec{r} \cdot \vec{\sigma}$ la seguente matrice:

$$\vec{r} \cdot \vec{\sigma} = r_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + r_2 \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + r_3 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Proposizione 2.3. (Sfera di Bloch per stati mischiati) È possibile rappresentare geometricamente lo stato mischiato di un singolo qubit su di una sfera tridimensionale, identificando la superficie con gli stati puri di un qubit. In particolare, dimostriamo che una matrice di densità per un qubit di stato mischiato può essere scritto come:

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2},$$

dove \vec{r} è un vettore reale tale che $\|\vec{r}\| \leq 1$. Questo vettore è detto vettore di Bloch per lo stato ρ .

Dimostrazione. Notiamo che ρ rappresenta una matrice di densità, infatti visto che

$$\rho = \frac{1}{2} \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} r_3 & r_1 - ir_2 \\ r_1 + ir_2 & -r_3 \end{pmatrix} \right),$$

Si ottiene immediatamente che la matrice rappresenta una forma Hermitiana con $\text{tr}(\rho) = 1$. Inoltre, svolgendo un semplice calcolo, si ottiene che è anche

definita positiva. Con semplici ragionamenti si nota che una qualsiasi matrice soddisfacente le proprietà sopra è descrivibile dalla matrice:

$$\frac{1}{2} \begin{pmatrix} r_3 + 1 & r_1 - ir_2 \\ r_1 + ir_2 & -r_3 + 1 \end{pmatrix}.$$

Si ottiene infine che ρ è puro se e solo se $\text{tr}(\rho^2) = 1$ se e solo se

$$\begin{aligned} 1 &= \frac{1}{4}((r_3 + 1)^2 + r_1^2 + r_2^2 + r_1^2 + r_2^2 + (1 - r_3)^2) \\ 1 &= \frac{1}{2}(r_1^2 + r_2^2 + r_3^2 + 1) \end{aligned}$$

che si ottiene banalmente se e solo se $\|\vec{r}\| = 1$. Un modo equivalente per visualizzare un generico vettore puro $|\psi\rangle = a|0\rangle + b|1\rangle$, con $a, b \in \mathbb{C}$ e $a^2 + b^2 = 1$, sulla superficie della sfera di Bloch è il seguente:

$$\begin{aligned} |\psi\rangle &= a|0\rangle + b|1\rangle \\ &= e^{i\gamma} \left(\cos \frac{\theta}{2} + e^{i\varphi} \sin \frac{\theta}{2} \right) \end{aligned}$$

con $\gamma, \theta, \varphi \in \mathbb{R}$. Il fattore $e^{i\gamma}$ non produce effetti osservabili, dunque un generico vettore di stato può essere riscritto semplicemente come:

$$|\psi\rangle = \cos \frac{\theta}{2} + e^{i\varphi} \sin \frac{\theta}{2},$$

il che identifica univocamente un punto sulla superficie sferica (e viceversa). \square

2.2 Gli operatori di densità ridotti

Una delle applicazioni più importanti degli operatori di densità è quella di fornire una descrizione dei sottosistemi che compongono un sistema quantistico. Questa descrizione è ottenuta per mezzo dei *operatori di densità ridotti*, indispensabili per l'analisi di sistemi quantistici composti. In seguito si definisce la traccia parziale in generici spazi vettoriali finito-dimensionali.

Definizione 2.3. *Supponiamo V, W siano spazi vettoriali rispettivamente di dimensione n e m su un campo \mathcal{K} . Per ogni spazio A , denotiamo con $\mathcal{L}(A)$ l'insieme degli operatori lineari su A . La traccia parziale su W è l'unico operatore $\text{Tr}_W : \mathcal{L}(V \otimes W) \rightarrow \mathcal{L}(V)$ tale per cui:*

$$\text{Tr}_W(R \otimes S) = \text{Tr}(S)R \quad \forall R \in \mathcal{L}(V) \quad \forall S \in \mathcal{L}(W).$$

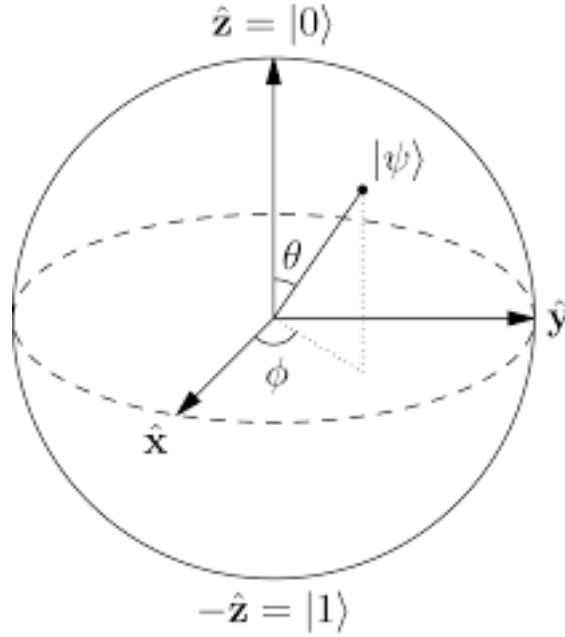


Figura 1: Sfera di Bloch

Nel caso semplice in cui si hanno due generici operatori $|a_1\rangle\langle a_2|$ e $|b_1\rangle\langle b_2|$, con $|a_1\rangle$ e $|a_2\rangle$ nello spazio degli stati di A e $|b_1\rangle$, $|b_2\rangle$ nello spazio degli stati di B , la traccia parziale sul sistema B è dato da

$$tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) := |a_1\rangle\langle a_2| tr(|b_1\rangle\langle b_2|).$$

Definizione 2.4. *Supponiamo di avere due sistemi fisici A e B descritti dall'operatore di densità ρ_{AB} . L'operatore di densità ridotto per il sistema A è definito da*

$$\rho^A := tr_B(\rho^{AB}),$$

dove tr_B è la traccia parziale sul sistema B .

Gli operatori di densità ridotti permettono di ottenere informazioni su una parte di un sistema composto più grande e per questo sono fondamentali nello studio di stati di entanglement, in quanto essi non sono descrivibili come semplice prodotto tensoriale dei sistemi di cui è composto.

2.3 La decomposizione di Schmidt

Teorema 2.3. (Decomposizione di Schmidt) *Supponiamo $|\psi\rangle$ sia uno stato puro di un sistema composto AB . Allora esistono $|i_A\rangle$ ortonormali per*

il sistema A , $|i_B\rangle$ ortonormali per il sistema B tali che

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle,$$

dove i coefficienti λ_i sono reali, non negativi che soddisfano $\sum_i \lambda_i^2 = 1$ detti coefficienti di Schmidt.

Dimostrazione. Dimostrerò per semplicità di notazione i casi in cui A e B hanno stessa dimensione, il caso generale è facilmente adattabile. Supponiamo $|j\rangle$ e $|k\rangle$ siano una fissata base ortonormale rispettivamente per i sistemi A e B . Allora $|\psi\rangle$ può essere scritto come

$$|\psi\rangle = \sum_{jk} a_{jk} |j\rangle |k\rangle,$$

per qualche matrice a di numeri complessi a_{jk} . Per la decomposizione ai valori singolari si ha che $a = u d v$, dove d è una matrice diagonale con termini non negativi, u e v sono matrici unitarie. Dunque

$$|\psi\rangle = \sum_{ijk} u_{ji} d_{ii} v_{ik} |j\rangle |k\rangle.$$

Definendo $|i_A\rangle := \sum_j u_{ij} |j\rangle$, $|i_B\rangle = \sum_k v_{ik} |k\rangle$, e $\lambda_i := d_{ii}$, si ottiene

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle.$$

Inoltre, essendo u e v unitarie, gli insiemi $|i_A\rangle$ e $|i_B\rangle$ risulteranno ortonormali. \square

Osservazione. Supponiamo di avere un sistema quantistico a tre componenti ABC . In questo caso, non è garantita la decomposizione di Schmidt di uno stato $|\psi\rangle$ puro nelle tre basi ortonormali. Cioè, dato $|\psi\rangle$ generico stato puro, non è garantita la possibilità di esser scritto nella forma

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle |i_C\rangle,$$

con $\lambda \in \mathbb{R}$ e $|i_A\rangle |i_B\rangle |i_C\rangle$ basi ortonormali dei relativi sistemi.

Definizione 2.5. Dato uno stato puro di un sistema composto $|\psi\rangle$ e la sua relativa decomposizione di Schmidt $|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$, allora le basi $|i_A\rangle$ e $|i_B\rangle$ sono dette basi di Schmidt per i sistemi A e B . Il numero di valori non nulli di λ_i è detto numero di Schmidt per lo stato $|\psi\rangle$.

Il numero di Schmidt è una proprietà importante per i sistemi quantistici compositi. Una banale applicazione è mostrata di seguito.

Proposizione 2.4. *Sia $|\psi\rangle$ il vettore di uno stato composito AB , allora sono equivalenti:*

1. AB è prodotto di due stati.
2. Il numero di Schmidt di $|\psi\rangle$ è 1.
3. ρ^A (e quindi ρ^B) sono stati puri.

Dimostrazione. 1) \rightarrow 2) Sia $|i_A\rangle$ e $|i_B\rangle$ gli unici due vettori normalizzati che descrivono rispettivamente gli stati dei sistemi A e B . Allora la decomposizione di Schmidt è univocamente determinata ed è $|\psi\rangle = |i_A\rangle |i_B\rangle$.

2) \rightarrow 3) Supponiamo ρ_A non sia uno stato puro. Allora, detto ρ la matrice di densità relativo al sistema A , deve valere che $\text{tr}(\rho^2) < 1$. Da ciò segue necessariamente che non vi è un solo coefficiente di Schmidt (altrimenti esisterebbe una decomposizione con $\lambda = 1$ che contraddice la condizione $\text{tr}(\rho^2) = 1$).

3) \rightarrow 1) Segue dal fatto che ρ_A descrive lo stato di A . □

2.4 Purificazione

La *purificazione* è una procedura meramente matematica che ci permette di associare stati puri a stati mischiati. Sia ρ^A lo stato di un sistema quantistico A . È possibile introdurre un altro sistema, denotato con R , e definire uno *stato puro* $|AR\rangle$ per sistema congiunto AR in modo tale che $\rho^A = \text{tr}_B(|AR\rangle\langle AR|)$. Così, lo stato puro AR si riduce ad ρ^A quando si guarda al singolo sistema A . Il sistema R è detto *reference system*: è un sistema fittizio, senza un diretto significato fisico. In seguito si dimostra che un tale sistema R è sempre costruibile.

Teorema 2.4. *La procedura di purificazione è possibile per ogni stato. Cioè, dato uno stato ρ^A per un sistema quantistico A , è sempre possibile introdurre un sistema R in modo tale che $\rho^A = \text{tr}_B(|AR\rangle\langle AR|)$.*

Dimostrazione. Sia R un sistema di stato identico a quello di A , con base ortonormale $|i^R\rangle$, e definiamo uno stato puro per lo stato combinato

$$|AR\rangle := \sum_i \sqrt{p_i} |i^A\rangle |i^R\rangle.$$

Calcoliamo l'operatore di densità ridotto per il sistema A corrispondente allo stato $|AR\rangle$:

$$\begin{aligned} \text{tr}_R(|AR\rangle\langle AR|) &= \sum_{ij} \sqrt{p_i p_j} |i^A\rangle\langle j^A| \text{tr}(|i^R\rangle\langle j^R|) \\ &= \sum_{ij} \sqrt{p_i p_j} |i^A\rangle\langle j^A| \delta_{ij} \\ &= \sum_i p_i |i^A\rangle\langle i^A| \\ &= \rho^A. \end{aligned}$$

Quindi AR è una purificazione per ρ^A . □

Osservazione. *Vi è una stretta correlazione tra la decomposizione di Schmidt e la purificazione: la procedura usata per purificare uno stato mischiato del sistema A è quella di definire uno stato puro la cui base di Schmidt per il sistema A è la base nel quale lo stato mischiato è diagonale, i cui coefficienti di Schmidt son le radici quadrate degli autovalori della matrice di densità che si vuole purificare.*

3 Quantificazione di entanglement

Qual è la "quantità" di entanglement in un dato stato di un sistema quantistico composito? Questo è uno dei problemi cruciali nella teoria quantistica dell'informazione, in cui è stata fatta molta ricerca. Una risposta univoca, nel caso più generale, non è stata trovata. Sono molte le informazioni utili che una buona misura di entanglement può fornire. Ad esempio, si può essere interessati a sapere quanti stati puri e massimamente entangled è possibile estrarre da una serie di sistemi quantistici preparati. Viceversa, si può essere interessati a misurare quanto entanglement è effettivamente necessario per preparare un certo sistema in un determinato stato. Per sistemi bipartiti il problema è essenzialmente risolto, ma in sistemi multi-partiti sembrano esistere diversi "tipi di entanglement". Il problema è complesso anche a causa del mescolarsi di operazioni classiche a quelle quantistiche.

In seguito (3.1) si mostra il noto paradosso EPR che, a causa dell'effetto meramente quantistico dell'entanglement, si risolve con la negazione del principio di località, postulato della meccanica classica. Dopo di che (3.2) si considera un approccio "dall'alto" per la descrizione degli operatori di misura che si possono realizzare su un sistema, comprendendo anche operazioni classiche (operatori di Kraus). In (3.3) si ribadiscono i concetti e definizioni

fondamentali per comprendere in che modo stati di sistemi possono essere correlati tra loro. Infine (3.4) verrà introdotta l'entropia di Von Neumann e chiarito il significato di misura di entanglement per un sistema bipartito presentando qualche buona e relative proprietà.

3.1 Il paradosso EPR e la disuguaglianza di Bell

Il paradosso di Einstein-Podolsky-Rosen è un esperimento mentale proposto nel 1935 che, assumendo il principio di località e considerando la velocità della luce quella limite per il trasporto di informazione, rende inconsistente l'interpretazione probabilistica della meccanica quantistica come teoria completa. Essi giungono alla conclusione che debbano esistere delle "variabili nascoste" che determinano con *esattezza* (non più in modo probabilistico, imprevedibile) i risultati di ogni misurazione.

L'esperimento mentale consiste nel considerare il decadimento di una particella in elettrone e positrone che, per la conservazione del momento angolare, devono assumere due valori di spin opposti. Sia dunque

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|e+\rangle |p-\rangle + |e-\rangle |p+\rangle) \quad (3)$$

lo stato del sistema composto da e elettrone e p positrone. Si nota che $\{|e+\rangle, |e-\rangle, |p+\rangle, |p-\rangle\}$ forma una base completa dell'insieme di tutti gli stati. Adesso supponiamo che Alice misuri lo spin dell'elettrone lungo l'asse \bar{a} mentre Bob misuri lo spin del positrone lungo un asse \bar{b} e che queste misurazioni avvengano ad una distanza spaziale e temporale tale che non vi possano essere scambi di informazioni che possano influenzare le due misurazioni (il limite è fornito dalla velocità della luce, come postulato precedentemente). Adesso supponiamo che Alice abbia ottenuto spin positivo ($+_A$). Lo stato del sistema dunque collassa ad $|\psi'\rangle = |e+\rangle |p+\rangle$. Dai postulati della meccanica quantistica si deduce che

$$\begin{aligned} P(+_B|+_A) &= \sin^2 \frac{\theta}{2} \\ P(-_B|+_A) &= \cos^2 \frac{\theta}{2}, \end{aligned}$$

con θ l'angolo tra i due assi \bar{a} e \bar{b} . Infatti, fissato senza perdita di generalità che \bar{a} sia lungo l'asse z , dato $|b\rangle = \sin(\frac{\theta}{2})e^{i\frac{\phi}{2}}|p-\rangle + \cos(\frac{\theta}{2})e^{-i\frac{\phi}{2}}|p+\rangle$ generico vettore sulla sfera unitaria (univocamente identificato dai due angoli θ e ϕ), vale che

$$P_B(+_B) = \|\langle b|p-\rangle\|^2 = \|\sin \frac{\theta}{2} e^{i\frac{\phi}{2}}\|^2 = \sin^2 \frac{\theta}{2}. \quad (4)$$

Viceversa

$$P_B(-B) = 1 - P_B(+B) = \cos^2 \frac{\theta}{2}. \quad (5)$$

Si nota che, in accordo con la conservazione del momento angolare, se $\theta = 0$ è garantito che la misurazione di Bob sia di spin opposto. Dunque secondo la meccanica quantistica, la misurazione di Alice influenza la misurazione di Bob, il che è in contraddizione con le ipotesi ritenute necessarie. Nell'articolo si suggerisce l'ipotesi che esistano delle variabili nascoste, sconosciute, che determinano esattamente il risultato delle due misurazioni, negando l'interpretazione probabilistica della meccanica quantistica. Tuttavia in un articolo del 1964, Bell dimostra come l'esistenza di variabili nascoste che determinano con certezza i risultati delle misurazioni sia inconsistente con i risultati quantistici che sperimentalmente si verificano. Indichiamo con $\sigma_A = \pm \frac{1}{2}$ il risultato della misurazione di Alice e con $\sigma_B = \pm \frac{1}{2}$ il risultato della misurazione di Bob. Il valore medio, sostituendo nella seconda uguaglianza le equazioni (4) e (5), è pari ad:

$$\langle \sigma_A \sigma_B \rangle = \frac{P(+A)P(+B|+A) + P(-A)P(-B|-A)}{4} \quad (6)$$

$$- \frac{P(+A)P(-B|+A) - P(-A)P(+B|-A)}{4} \quad (7)$$

$$= \frac{\sin^2 \frac{\theta}{2} - \cos^2 \frac{\theta}{2}}{4} \quad (8)$$

$$= - \frac{\cos \theta}{4} = - \frac{\bar{a} \cdot \bar{b}}{4}. \quad (9)$$

Supponiamo esistano due funzioni $\sigma_e(\bar{v}, \bar{a})$ e $\sigma_p(\bar{v}, \bar{b})$ che dati rispettivamente un vettore n-dimensione \bar{v} (rappresenta le variabili nascoste) e l'asse di misurazione \bar{a} , \bar{b} siano in grado di determinare con certezza lo spin dell'elettrone, positrone. Per conservazione del momento angolare valgono

$$\begin{aligned} \sigma_p(\bar{v}, \bar{b}) &= -\sigma_e(\bar{v}, \bar{b}) = \pm \frac{1}{2} \\ \sigma_p(\bar{v}, \bar{a}) &= -\sigma_e(\bar{v}, \bar{a}) = \pm \frac{1}{2}. \end{aligned}$$

In seguito si ricava la disuguaglianza di Bell. Sia \bar{c} un generico versore lungo la quale effettuare una misurazione e ρ l'operatore di densità probabilistica. Allora vale

$$\begin{aligned} &\langle \sigma_e(\bar{a}) \sigma_p(\bar{b}) \rangle_{\bar{v}} - \langle \sigma_e(\bar{a}) \sigma_p(\bar{c}) \rangle_{\bar{v}} = \\ &= \int d^n \bar{v} \rho \sigma_e(\bar{v}, \bar{a}) \sigma_p(\bar{v}, \bar{b}) - \int d^n \bar{v} \rho \sigma_e(\bar{v}, \bar{a}) \sigma_p(\bar{v}, \bar{c}). \end{aligned}$$

Raccogliendo e moltiplicando per $4\sigma_e^2(\bar{v}, \bar{b}) = 1$ si ottiene

$$= \int d^n \bar{v} \rho \sigma_e(\bar{v}, \bar{a}) \sigma_e(\bar{v}, \bar{b}) (1 - 4\sigma_e(\bar{v}, \bar{b}) \sigma_e(\bar{v}, \bar{c})).$$

Posso maggiorare ponendo $\sigma_e(\bar{v}, \bar{a}) \sigma_e(\bar{v}, \bar{b}) = \frac{1}{4}$ (può valere anche $-\frac{1}{4}$) e pongo $(1 - 4\sigma_e(\bar{v}, \bar{b}) \sigma_e(\bar{v}, \bar{c})) \leq 0$ (può valere 0 o 2) si ottiene la disuguaglianza di Bell:

$$\| \langle \sigma_e(\bar{a}) \sigma_p(\bar{b}) \rangle_{\bar{v}} - \langle \sigma_e(\bar{a}) \sigma_p(\bar{c}) \rangle_{\bar{v}} \| \leq \frac{1 - 4 \langle \sigma_e(\bar{b}) \sigma_p(\bar{c}) \rangle_{\bar{v}}}{4}. \quad (10)$$

Si nota che nell'ottenere la disuguaglianza non si è posta nessuna restrizione su $\bar{a}, \bar{b}, \bar{c}$.

Verifichiamo l'inconsistenza di questa disuguaglianza (ottenuta presupponendo l'esistenza di variabili nascoste che determina con certezza le misurazioni) con le previsioni meccanica quantistica. Sostituendo l'equazione 9 nella disuguaglianza si ottiene

$$\frac{\| \bar{a} \cdot (\bar{c} - \bar{b}) \|}{4} \leq \frac{1 - \bar{b} \cdot \bar{c}}{4}.$$

Scegliendo $\bar{a}, \bar{b}, \bar{c}$ in modo tale che $\bar{a} \cdot \bar{b} = 0$ e $\bar{c} = \bar{a} \sin \psi + \bar{b} \cos \psi$ si ottiene

$$\frac{\| \sin \psi \|}{4} \leq \frac{1 - \cos \psi}{4}$$

il che è contraddittorio per quasi ogni valore di ψ .

Dunque la teoria delle variabili nascoste è inconsistente con la teoria della meccanica quantistica. Sperimentalmente si rilevano i risultati previsti dalla meccanica quantistica.

3.2 Operatori di misura in generale

Considerando un approccio più assiomatico, si vuole considerare quali operatori tra tutte le mappe $\xi : S(H) \rightarrow S(H')$ sono ammissibili e sono consistenti con l'interpretazione probabilistica della teoria quantistica. Da considerazioni precedenti, abbiamo ottenuto che un generico operatore che agisce sullo stato di un sistema quantistico è descritto da combinazioni dei seguenti ingredienti:

- Dato $\rho \in H(S)$ ed $U : H \rightarrow H$ operatore unitario dipendente dal tempo, allora è ammissibile la trasformazione $\rho \rightarrow U\rho U^\dagger$, come affermato dall'equazione (1) del secondo postulato.

- Per il terzo postulato (equazione 2) è possibile operare sullo spazio degli stati di un sistema H attraverso operatori di misurazione. Come visto nella definizione (1.1), è sufficiente considerare una base ortonormale di proiettori π_i (dove gli i indicano tutti i possibili risultati di una misurazione), che soddisfano

$$\pi_i \pi_j = \delta_{ij} \pi_i, \quad \sum_i \pi_i = I.$$

Se un sistema quantistico si trova nello stato iniziale ρ , allora lo stato collasserà ad

$$\rho' = \frac{\pi_i \rho \pi_i}{\text{tr}(\pi_i \rho \pi_i)},$$

con probabilità di ottenere i pari ad

$$p_i = \text{tr}(\pi_i \rho) = \text{tr}(\pi_i \rho \pi_i).$$

- Dato uno stato ρ di H , è sempre possibile appendere un sistema ancilla di spazio K nello stato ω in modo tale che

$$\rho \rightarrow \rho \otimes \omega,$$

nel rispetto del quarto postulato.

- Viceversa, è sempre possibile perdere una parte del mio intero sistema quantistico. Questo è ottenuto dall'operatore traccia parziale definito in (2.3): dato un sistema composito con spazio $H \otimes K$ nello stato ρ , allora

$$\rho \rightarrow \sigma = \text{tr}_K(\rho),$$

è lo stato che descrive il sistema H isolato.

Dunque una generica mappa ξ deve essere necessariamente lineare, affinché possa conservare le combinazioni convesse in $S(H)$. Inoltre composizioni degli operatori descritti sopra formano sempre mappe positive dallo spazio degli stati in sé stesso. La positività di un generico ξ non è però condizione sufficiente. Essendo sempre possibile considerare un qualsiasi sistema come facente parte di un sistema quantistico più grande, si rende necessaria la seguente definizione:

Definizione 3.1. *Una mappa $\xi : S(H) \rightarrow S(H)$ è detta completamente positiva se $\xi \otimes I_N$ è positiva per ogni $N \in \mathbb{N}$.*

Piuttosto sorprendente è il fatto che essere *completamente positivi* è una condizione più forte della mera positività. Ne è un esempio la trasposizione.

Le operazioni ammissibili sono dunque identificate da operatori lineari completamente positivi, in particolare possono essere scritti nella forma

$$\rho \mapsto \xi(\rho) = \sum_i E_i \rho E_i^\dagger, \quad (11)$$

con $E_i : H \rightarrow H$ detti *operatori di Kraus*, non necessariamente Hermitiani. In questo modo vengono espresse operazioni che sono parzialmente classiche. Se si richiede che preservino la traccia allora è necessario richiedere che

$$\sum_i E_i^\dagger E_i = I, \quad \sum_i E_i E_i^\dagger = I,$$

e sono detti *operatori doppiamente stocastici*, i quali corrispondono ad operazioni quantistiche. Si ricorda, come dimostrato in 2.2, che una qualsiasi operazione quantistica determina una classe di operatori di Kraus, costituita dall'azione delle matrici unitarie.

Definizione 3.2. *Dato un sistema quantistico bipartito $H = H_A \otimes H_B$, si definisce un operatore locale ξ_A sul sistema A un qualsiasi operatore agente su H che lascia invariato lo stato di B .*

Due stati ρ_1 e ρ_2 di un sistema $A \otimes B$ sono detti *localmente distinguibili* se $tr_A(\rho_1)$ e $tr_B(\rho_2)$ oppure $tr_A(\rho_2)$ e $tr_B(\rho_1)$ sono ortogonali, cosicché esista un operatore di misura locale che possa discriminare i due stati con certezza, come dimostrato in 1.2 e 1.3.

Definizione 3.3. *Si definiscono operatori quantici con comunicazione classica (abbreviato LOCC) è costituito da una qualsiasi composizione di operazioni quantistiche locali e trasmissioni di informazioni tramite canali classici.*

L'insieme degli operatori LOCC è incluso nell'insieme degli *operatori separabili*, cioè l'insieme degli elementi i cui operatori di Kraus sono descrivibili con un prodotto tensoriale.

3.3 Correlazioni tra stati quantistici

Consideriamo un sistema bipartito quantistico AB il quale è ottenuto come prodotto tensoriale delle due parti A e B . Allora un qualsiasi insieme di misurazioni LOCC costituisce un insieme di eventi indipendenti. Questo non sorprende, visto che qualsiasi stato puro separabile, essendo esprimibile

come prodotto tensoriale delle sue parti, può essere preparato da sperimentatori che agiscono in modo localmente indipendente. D'altra parte, stati non esprimibili come prodotto tensoriale delle sue parti, non possono essere preparati facendo uso solo di operazioni LOCC. Esistono diversi criteri per classificare operazioni locali, ma tutte fanno uso della intrinseca distinzione tra *stati prodotto* e *stati correlati*. Questi stati correlati sono detti *stati di entanglement*. Di particolare interesse sono gli stati *massimamente entangled*, necessari per la realizzazione di alcuni protocolli o algoritmi nella teoria quantistica dell'informazione.

Definizione 3.4. *Un sistema bipartito è detto massimamente entangled se gli stati ridotti di entrambe le parti sono massimamente mischiati.*

Definizione 3.5. *Lo stato di un sistema quantistico bipartito è detto separabile o classicamente correlato se è combinazione convessa di prodotti di stati, cioè se ρ può essere scritto nella forma*

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i, \quad (12)$$

dove $0 \leq p_i \leq 1$, $\sum_i p_i = 1$, $\rho_A^i \in S(H_A)$ e $\rho_B^i \in S(H_B)$.

Uno stato della forma 12 può essere preparato con operazioni LOCC.

Notazione. *Gli insiemi degli stati separabili che descrivono un sistema H è denotato con $D(H)$. Si nota che ogni stato della forma 12 è sempre descrivibile per mezzo di stati puri, come spiegato nella sottosezione "Purificazione".*

Definizione 3.6. *Stati che non possono essere scritti nella forma 12 sono detti di Entanglement.*

Uno dei maggiori problemi in teoria quantistica dell'informazione è quella di determinare se uno stato ρ sia separabile o meno.

Stati massimamente entangled sono necessari per applicare molti protocolli in teoria quantistica dell'informazione. Il problema di determinare se, data una serie di n qubit identici in stato mischiato, vi sia possibile estrarre qualche copia di stato massimamente entangled è una questione di utile applicazione.

3.4 Misure monotone di entanglement

Misure monotone di entanglement sono funzionali che mappano stati in numeri positivi che quantificano l'entanglement dello stato. La principale caratteristica è quella di distinguere tra correlazioni quantistiche e classiche.

Non vi è una unica funzione, ma esistono una serie di proprietà che un funzionale $E : S(H) \rightarrow \mathbb{R}^+$ deve soddisfare affinché sia una buona misura di entanglement. In seguito sono elencate le proprietà considerate necessarie per definire un funzionale monotono di entanglement.

- $E : S(H) \rightarrow \mathbb{R}^+$ è un funzionale positivo tale che per ogni $\sigma \in D(H)$ stato separabile valga $E(\sigma) = 0$.
- E è un funzionale convesso, cioè

$$E\left(\sum_i p_i \sigma_i\right) \leq \sum_i p_i E(\sigma_i) \quad (13)$$

con $p_i \in [0, 1]$, $\sum_i p_i = 1$ e $\sigma_i \in S(H)$.

- E è monotona sotto l'azione di operazioni locali: se uno delle parti produce una misurazione generalizzata locale, allora l'entanglement non può incrementare. Questo significa che, supponiamo Alice implementi una operazione locale che porta agli stati

$$\sigma_i = \frac{\sum_{i,j} (A_{i,j} \otimes I_B) \sigma (A_{i,j} \otimes I_B)^\dagger}{p_i} \text{ per ogni } i,$$

con probabilità $p_i = \text{tr}(A_{i,j} \sigma A_{i,j}^\dagger)$, dove $\sum_{i,j} A_{i,j} A_{i,j}^\dagger = I_A$, allora

$$E(\sigma) \geq \sum_i p_i E(\sigma_i). \quad (14)$$

Osservazione. La condizione 14 implica l'invarianza per l'azione locale di operatori unitari, ovvero $E(U\rho U^\dagger) = E(\rho)$ per ogni $\rho \in S(H)$ e per ogni operatore unitario locale $U : H \rightarrow H$.

Perfino per stati pure, le precedenti tre proprietà non determinano univocamente una misura di entanglement. Sono necessarie le seguenti due proprietà affinché E sia completamente determinato per stati puri:

- E è debolmente additivo, cioè $E(|\psi\rangle\langle\psi|^{\otimes n}) = nE(|\psi\rangle\langle\psi|)$ per ogni $\psi \in H$ e per ogni $n \in \mathbb{N}$.
- Per un dato $|\psi\rangle \in H$ siano $(\sigma_n)_{n \in \mathbb{N}}$ una successione di stati $\sigma_n \in S(H^{\otimes n})$ con la proprietà che $\lim_{n \rightarrow \infty} \|\|\|\|\psi\rangle\langle\psi|^{\otimes n} - \sigma_n\|\|\|_{tr} = 0$, dove $\|\|\|\cdot\|\|\|_{tr}$ denota la norma indotta dalla traccia, cioè $\|\|\|A\|\|\|_{tr} = \text{tr}(\sqrt{AA^\dagger})$. E allora soddisfa la proprietà:

$$\lim_{n \rightarrow \infty} \frac{\|E(|\psi\rangle\langle\psi|^{\otimes n}) - E(\sigma_n)\|}{n} = 0 \quad (15)$$

L'unica misura di entanglement per stati bipartiti puri è data da

$$E(|\psi\rangle\langle\psi|) = S(\text{tr}_A(|\psi\rangle\langle\psi|)) = S(\text{tr}_B(|\psi\rangle\langle\psi|)), \quad (16)$$

dove S denota l'entropia di Von Neumann. L'entropia di Von Neumann è "l'analogo quantistico" dell'entropia di Shannon, cioè è una misura di quanto un determinato stato quantistico si trovi in stato mischiato. L'entropia di Von Neumann si annulla per stati puri e assume massimo negli stati massimamente entangled. Dall'osservazione 2.1 sappiamo che un generico stato mischiato ρ prevede diverse scomposizioni nella forma $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. In questa decomposizione, i proiettori non sono necessariamente ortogonali, dunque ad ogni scomposizione vi può essere una differente informazione di Shannon $H = -\sum_i p_i \log_2 p_i$ associata, corrispondendo ad un diverso "grado di mischiatezza". L'entropia di Von Neumann di un dato stato ρ è definito come il più piccolo valore tra l'insieme dei valori dell'entropia di Shannon che sono associati all'insieme di tutte le decomposizioni possibili di ρ in proiettori (anche non ortogonali). Questo valore corrisponde al caso in cui i proiettori sono ortogonali, dunque

$$S(\rho) = -\text{tr}(\rho \log \rho), \quad (17)$$

che coincide con

$$S(\rho) = -\sum_i p_i \log_2(p_i), \quad (18)$$

dove i p_i sono ottenuti dai coefficienti della decomposizione spettrale $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

Per visualizzare il comportamento della misura di entanglement indotta dall'entropia di Von Neumann, consideriamo l'insieme di stati parametrizzati dal valore di $p \in [0, 1]$

$$|\psi\rangle = \sqrt{p}|00\rangle + \sqrt{(1-p)}|11\rangle.$$

La misura di entanglement per lo stato $|\psi\rangle\langle\psi|$ è dato da $S(\text{tr}_A(|\psi\rangle\langle\psi|))$. Il calcolo della matrice di densità ridotta per il primo sottosistema è immediato poiché il calcolo della decomposizione di Schimidt è banale, e si ottiene che $\rho_1 = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$. L'entropia di Von Neumann per questo stato è:

$$S(\rho_1) = -p \log_2(p) - (1-p) \log_2(p).$$

Notiamo (si veda figura 2) che il massimo è raggiunto in $p = \frac{1}{2}$ ovvero nello stato massimamente mischiato, mentre in $p = 0, 1$ si annulla (stato del sistema è puro).

In seguito sono elencate le principali proprietà dell'entropia di Von Neumann. Siano σ, ρ e ρ_i, σ_i stati in $S(H)$. Inoltre siano $\rho^{(1)}, \sigma^{(1)} \in S(H^{(1)})$ e $\rho^{(2)}, \sigma^{(2)} \in S(H^{(2)})$ stati di un sistema composito $H^{(1)} \otimes H^{(2)}$, valgono

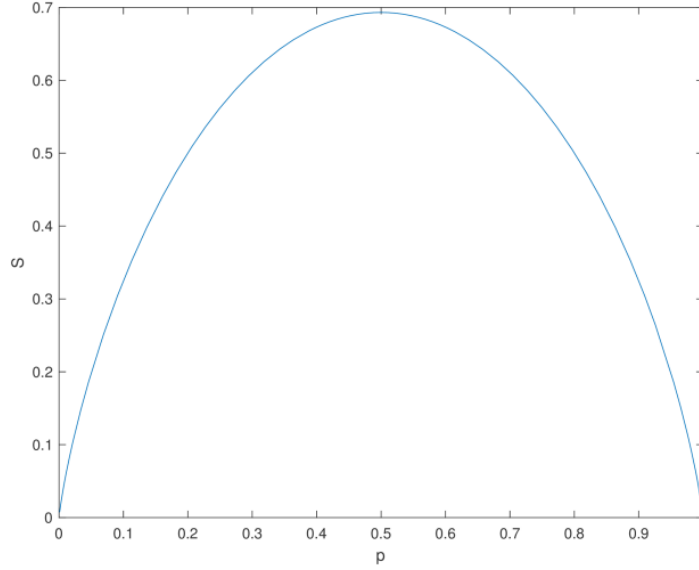


Figura 2: Dipendenza dell'entropia di Von Neumann da parametro p

- Positività: $S(\rho) \geq 0$.
- Simmetria: se $\sigma = U\rho U^\dagger$ per qualsiasi operatore unitario U , allora $S(\sigma) = S(\rho)$.
- Concavità: $S(\lambda\rho_1 + (1-\lambda)\rho_2) \geq \lambda S(\rho_1) + (1-\lambda)S(\rho_2)$ per ogni $\lambda \in [0, 1]$.
- Additività: $S(\rho^{(1)} \otimes \rho^{(2)}) = S(\rho^{(1)}) + S(\rho^{(2)})$.
- Siano $\rho^{(1)} = tr_2(\rho)$ e $\rho^{(2)} = tr_1(\rho)$ stati ridotti di ρ . Allora $S(\rho) \leq S(\rho^{(1)}) + S(\rho^{(2)})$.
- Semi-continuità inferiore: se $\lim_{n \rightarrow \infty} |||\rho_n - \rho|||_{tr} = 0$, allora

$$S(\rho) \leq \liminf_{n \rightarrow \infty} S(\rho_n).$$

- Monotonicità: $S(\xi(\rho)) \geq S(\rho)$ per ogni mappa ξ completamente positivo e doppiamente stocastica.

È possibile definire attraverso l'entropia di Von Neumann un'altra misura di entanglement, detta *entropia funzionale relativa*. In seguito la si definisce considerando solo una coppia di stati ρ e σ .

Definizione 3.7. *Dati due generici stati $\rho, \sigma \in S(H)$ si definisce l'entropia funzionale relativa di σ rispetto a ρ come*

$$S(\sigma||\rho) = tr(\sigma(\log_2 \sigma - \log_2 \rho)). \quad (19)$$

Questo, misura quanto differente è σ rispetto a ρ in senso statistico. Se ρ e σ sono identici, l'entropia relativa si annulla, mentre maggiore è il valore dell'entropia relativa, maggiore è la quantità di informazione che può essere ottenuta da una misurazione discriminando tra σ e ρ . Siano $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ e $\sigma = \sum_j q_j |\phi_j\rangle \langle \phi_j|$ le decomposizioni spettrali di due generici stati di un sistema H , allora è possibile riscrivere l'equazione 19 nel seguente modo:

$$S(\sigma||\rho) = \sum_{i,j} (q_j \log_2 q_j - q_j \log_2 p_i) |\langle \psi_i | \phi_j \rangle|^2. \quad (20)$$

In seguito si elencano le principali proprietà dell'entropia funzionale relativa. Siano σ, ρ e ρ_i, σ_i stati in $S(H)$. Inoltre siano $\rho^{(1)}, \sigma^{(1)} \in S(H^{(1)})$ e $\rho^{(2)}, \sigma^{(2)} \in S(H^{(2)})$ stati di un sistema composito $H^{(1)} \otimes H^{(2)}$, valgono

- Positività: $S(\sigma||\rho) \geq 0$.
- Nilpotenza: $S(\rho||\rho) = 0$.
- Convessità: per ogni $\lambda \in [0, 1]$ vale

$$S(\lambda\sigma_1 + (1-\lambda)\sigma_2 || \lambda\rho_1 + (1-\lambda)\rho_2) \leq \lambda S(\sigma_1||\rho_1) + (1-\lambda)S(\sigma_2||\rho_2).$$

- Additività: $S(\sigma^{(1)} \otimes \sigma^{(2)} || \rho^{(1)} \otimes \rho^{(2)}) = S(\sigma^{(1)}||\rho^{(1)}) + S(\sigma^{(2)}||\rho^{(2)})$.
- Semi-continuità inferiore: se $\lim_{n \rightarrow \infty} |||\sigma_n - \sigma|||_{tr} = 0$ e $\lim_{n \rightarrow \infty} |||\rho_n - \rho|||_{tr} = 0$, allora $S(\sigma||\rho) \leq \lim_{n \rightarrow \infty} \inf S(\sigma_n||\rho_n)$. Se esiste un numero positivo λ tale che $\sigma_n \leq \lambda\rho_n$, allora $\lim_{n \rightarrow \infty} S(\sigma_n||\rho_n) = S(\sigma||\rho)$.
- Monotonicità: per ogni operatore doppiamente stocastico ξ vale

$$S(\xi(\sigma)||\xi(\rho)) \leq S(\sigma||\rho).$$

- Invarianza: per ogni matrice unitaria U

$$S(U\sigma U^\dagger || U\rho U^\dagger) = S(\sigma||\rho).$$

Si nota che l'entropia funzionale relativa non è metrica, in particolare non è simmetrica, cioè in generale vale $S(\sigma||\rho) \neq S(\rho||\sigma)$.

In seguito si definisce un'altra misura di entanglement per un sistema bipartito che si propone di quantificare quanto entanglement è necessario per costruire un determinato sistema.

Definizione 3.8. Dato un sistema bipartito H ed uno stato puro $|\psi\rangle$, si definisce entanglement di formazione la funzione $E_f : S(H) \rightarrow \mathbb{R}$ tale che

$$E_f(\psi) = - \sum_i \lambda_i \log \lambda_i,$$

dove i λ_i sono gli autovalori della matrice di densità ridotta di uno dei due sottosistemi.

La definizione è estendibile anche per stati mischiati nel seguente modo: dato un generico stato mischiato ρ , per l'osservazione 2.1 sappiamo esistere diversi insiemi pesati di vettori che decompongono lo stato in modo tale che $\rho = \sum_n p_n |\psi_n\rangle \langle \psi_n|$. Tra questi, consideriamo l'aggregato ottimale, cioè le coppie $(p_i^*, |\psi_i^*\rangle)$ la cui media pesata degli entanglement di formazione è minima. Questa definirà l'entanglement di formazione dello stato mischiato ρ :

$$E_f(\rho) = \inf \sum_j p_j E_f(\psi_j),$$

dove con "inf" indichiamo che stiamo considerando la decomposizione ottimale.

3.5 Il teletrasporto quantistico

In seguito si illustrerà il fenomeno del teletrasporto quantistico che è possibile realizzare esclusivamente grazie all'uso di quella che è la principale risorsa della meccanica quantistica: stati in entanglement.

Si premette un teorema fondamentale della teoria quantistica dell'informazione: il teorema di no-cloning quantistico. Esso si ottiene come semplice conseguenza dei postulati della meccanica quantistica e vieta la creazione di un duplicato esatto di uno stato quantistico sconosciuto.

Teorema 3.1. (no-cloning) Si consideri un sistema composto quantistico nello stato $|E\rangle \otimes |\phi\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$, in cui si indica con $|\phi\rangle$ lo stato conosciuto da clonare, $|E\rangle$ lo stato ambiente e $|\psi_1\rangle, \dots, |\psi_n\rangle$ gli stati iniziali degli n sistemi su cui si vorrebbe clonare $|\phi\rangle$. Un generico processo di duplicazione consiste in un operatore unitario U tale per cui, per ogni $|\phi\rangle$, valga

$$U |E\rangle \otimes |\phi\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle = |E_\phi\rangle \otimes |\phi\rangle \otimes |\phi\rangle \dots |\phi\rangle.$$

Dimostriamo che un operatore unitario non esiste.

Dimostrazione. Per dimostrare l'enunciato si considerano due stati $|\phi\rangle$ e $|\eta\rangle$ sottoposti al processo di cloning. L'operatore U conserva il prodotto scalare (tra prima e dopo la clonazione dei due stati scelti), dunque

$$||\langle\phi|\psi\rangle|| = ||\langle E_\phi|E_\psi\rangle|| ||\langle\phi|\psi\rangle||^n.$$

Considerato che, per stati normalizzati, vale $0 \leq \langle\phi|\psi\rangle \leq 1$ l'equazione sopra non può essere soddisfatta per generici $|\phi\rangle, |\psi\rangle$. \square

È però possibile trasferire lo stato quantistico di un sistema in un altro sistema. Questo, ovviamente, a patto di rispettare il teorema di no-cloning, ossia eliminare l'informazione nel sistema originale.

Esistono diversi schemi di teletrasporto quantistico. Il caso più semplice è quello del teletrasporto di un qubit. Per la realizzazione del protocollo saranno necessarie le trasformazioni definite nel seguito:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Lo stato iniziale dei sistemi di Alice e Bob è il seguente:

$$\frac{1}{\sqrt{2}} |\psi\rangle_{A_0} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B),$$

dove $|\psi\rangle_{A_0} = \alpha |0\rangle_{A_0} + \beta |1\rangle_{A_0}$ è il qubit in mano ad Alice che si vuole teletrasportare nelle mani di Bob facendo uso del sistema entangled AB . Omettendo i pedici ed eseguendo il prodotto si ottiene:

$$\frac{\alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle}{\sqrt{2}}. \quad (21)$$

A questo punto viene applicato l'operatore unitario CNOT alla prima coppia di qubit, dove il primo è usato come controllo, mentre il secondo è il target. Così facendo lo stato complessivo del sistema diventa:

$$\frac{\alpha |000\rangle + \alpha |011\rangle + \beta |110\rangle + \beta |101\rangle}{\sqrt{2}}. \quad (22)$$

Successivamente si applica l'operatore Hadamard risultando:

$$\frac{\alpha |000\rangle + \alpha |100\rangle + \alpha |011\rangle + \alpha |111\rangle + \beta |010\rangle - \beta |110\rangle + \beta |001\rangle - \beta |101\rangle}{2}.$$

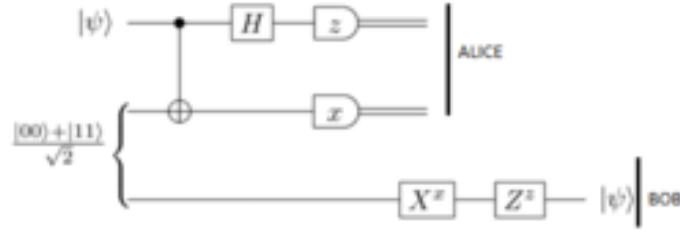


Figura 3: Schema del teletrasporto quantistico di un qubit.

Raccogliendo i primi due qubit di Alice si ottiene:

$$\frac{|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle)}{2} + \quad (23)$$

$$+ \frac{|10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)}{2}. \quad (24)$$

A questo punto Alice procede misurando i suoi due qubit (denotato in figura 3 rispettivamente con "z" e "x"). Così facendo per ciascuna delle quattro basi $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ si ha probabilità $\frac{1}{4} = \frac{\|\alpha\|^2}{4} + \frac{\|\beta\|^2}{4}$ di ottenerla. A seconda del risultato della misurazione, Alice comunica classicamente quale matrice applicare allo stato che si ritrova Bob per ottenere $|\psi\rangle$. Indicando con X, Z le matrici di Pauli definite in 2.1, vale che

- Se Alice misura 00 allora lo stato di Bob diventa $|\psi\rangle$;
- Se Alice misura 01 allora lo stato di Bob diventa $X|\psi\rangle$;
- Se Alice misura 10 allora lo stato di Bob diventa $Z|\psi\rangle$;
- Infine se Alice misura 11 allora lo stato di Bob diventa $XZ|\psi\rangle$.

Dunque Bob, visto che I, X, Z, XZ sono matrici unitarie, è sufficiente che applichi (in base a quanto riferito da Alice) rispettivamente $I, X^\dagger, Z^\dagger, Z^\dagger X^\dagger$ per ottenere $|\psi\rangle$.

Osservazione. *Si osserva che senza alcuna informazione su quale sia il risultato della misurazione di Alice, la matrice di densità che rappresenta lo stato mischiato di Bob è l'identità:*

$$\rho = \frac{1}{4}(|\psi\rangle + X|\psi\rangle + Z|\psi\rangle + XZ|\psi\rangle) = I.$$

Dunque non vi è alcuna informazione trasmessa a Bob, in accordo con la relatività speciale secondo cui non vi possono essere trasmissione di informazioni a velocità superluminale.

Nel prossimo futuro, una delle applicazioni del teletrasporto quantistico è quella di distribuzioni di chiavi quantistiche per crittografia.

Riferimenti bibliografici

- [1] Michael A. Nielsen & Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University, 2010.
- [2] Jens Eisert, *Entanglement in Quantum Information Theory*, University of potsdam, Germany, 2001.
- [3] Stefan Hollands & Ko Sanders, *Entanglement measures and their properties in quantum field theory*, Universität Leipzig, 2018.
- [4] JS Bell, *On the einstein podolsky rosen paradox*, Physics Physique Fizika, 1964.