Alma Mater Studiorum · Università di Bologna

Scuola di Scienze
Dipartimento di Fisica e Astronomia
Corso di Laurea in Fisica

Entanglement quantistico dal punto di vista della teoria delle risorse

Relatore:
Dott. Lorenzo Piroli

Presentata da:
Filippo Pretolani

Anno Accademico 2022/2023

Sommario

L'entanglement è uno dei concetti fondanti della meccanica quantistica. Esso ha assunto un ruolo centrale nello sviluppo dell'informatica quantistica negli ultimi due decenni. Questa tesi si posiziona in questo contesto e si concentra sul problema di quantificare l'entanglement e inquadrarlo nell'ambito della teoria quantistica delle risorse. Dopo una prima introduzione ai concetti della meccanica quantistica si studia cosa sia una teoria quantistica delle risorse. Si mostra poi che si può costruire una teoria quantistica delle risorse per l'entanglement tramite le operazioni LOCC("local operations classical communication"). Successivamente si studia in dettaglio il caso bipartito. In particolare si enuncia e dimostra il Teorema di Nielsen. Esso mostra il legame tra l'entanglement bipartito e la teoria della maggiorazione, permettendo di definire un preordine fra gli stati entangled. Si definisce poi l'entanglement di formazione, una prima misura dell'entanglement bipartito strettamente legata all'entropia di Neumann. Per concludere si vedono alcune generalizzazioni dei risultati precedenti. Prima si analizza come si possa usare la probabilità di transizione come misura dell'entanglement bipartito. Poi si studia come, considerando una generalizzazione delle operazioni LOCC, si possano dividere gli stati in classi di equivalenza diverse, che rappresentano diversi tipi di entanglement. In particolare si studia in dettaglio il caso con tre qubit.

Indice

Introduzione

Nel 1935 fu pubblicato un articolo da Einstein, Podolsky e Rosen (EPR) [10] che voleva cercare di provare la non completezza della meccanica quantistica. Essi trovarono che la meccanica quantistica fa predizioni controintuitive quando lavora con stati preparati in un modo particolare. In seguito Schrödinger scrisse a Einstein una lettera [14] dove, per riferirsi a quegli stati, usò la parola Verschränkung, da lui tradotta come entanglement, che sottolinea un ordine di relazioni statistiche tra i sottosistemi del sistema composto. Successivamente Schrödinger pubblicò un articolo [18] dove definì più generalmente la nozione di entanglement, e ne sottolineò la particolare importanza all'interno della teoria quantistica, scrivendo: "Non definirei l'entanglement un elemento, ma piuttosto il tratto caratteristico della meccanica quantistica, quello che ne sancisce l'intero allontanamento dalle linee di pensiero classiche".

Einstein, Podolsky e Rosen usarono questi stati, detti entangled, per attribuire a priori dei valori alle quantità fisiche prima della misura, ma nel 1964 Bell [4] pubblicò un articolo in cui mostrò il contrario. In particolare mostrò che le ipotesi fatte da Einstein, Podolsky e Rosen per una teoria completa imponevano vincoli sulle correlazioni statistiche tra sistemi bipartiti, che espresse in forma di disuguaglianze. Mostrò inoltre che esse venivano violate se si consideravano stati entangled, e concluse che l'entanglement è quella proprietà del formalismo quantistico che rende impossibile simulare le correlazioni quantistiche con un qualsiasi formalismo classico.

Questi risultati furono poi verificati sperimentalmente nei seguenti anni. Di particolare importanza furono l'esperimento di Freedman e Clauser [11] e gli esperimenti di Aspect [2, 1]. Questi esperimenti confermarono fortemente le predizioni fatte da Bell.

La teoria dell'entanglement moderna è strettamente legata al concetto di manipolazione dell'entanglement, in particolare Bennet e altri suoi collaboratori [6] scoprìrono che una classe di trasformazioni naturali adatte a manipolare l'entanglement. Sono le trasformazioni LOCC("local operations and classical communication"), non possono infatti generare stati entangled partendo da stati non entangled. Sotto queste ipotesi sono stati trovati diversi risultati, uno dei più importanti nonché argomento centrale di questa tesi, fu l'articolo scritto da Nielsen nel 1999 [15], dove introdusse un criterio sulla convertibilità fra stati puri bipartiti. Questi risultati furono poi generalizzati da Vidal nel 1999 [20] considerando trasformazioni LOCC stocastiche. Tramite queste trasformazioni

LOCC stocastiche si possono classificare i diversi tipi di entanglement, come fatto nel caso di tre qubit da Dür, Vidal e Cirac [9].

Negli ultimi due decenni l'entanglement è stato al centro dello sviluppo della teoria dell'informatica quantistica, che studia il trasporto di informazioni dal punto di vista della fisica quantistica. Tra le applicazioni dell'entanglement nell'ambito dell'informatica quantistica c'è per esempio la crittografia quantistica, in particolare con la teoria della privacy, dove la correlazione fra i sottosistemi che distingue l'entanglement permette di generare una chiave crittografica condivisa solo dalle parti interessate. Altri esempi di applicazioni sono il superdense coding [5], che permette di ridurre la complessità della comunicazione classica, e il teletrasporto quantistico [7], che permette il trasferimento di uno stato quantistico. L'entanglement può quindi essere visto come una risorsa, che può essere usata per svolgere compiti non possibili tramite risorse classiche.

L'obbiettivo di questa tesi è quindi quello di concentrarsi sul problema di quantificare l'entanglement e inquadrarlo nell'ambito della teoria delle risorse quantistiche.

Capitolo 1

Richiami di meccanica quantistica

1.1 Postulati della meccanica quantistica

Secondo la meccanica quantistica, ogni sistema fisico, che chiamiamo $A, B, etc.$, è associato a uno spazio di Hilbert $\mathcal{H}^A, \mathcal{H}^B, etc.$. Un sistema fisico composto dai due sistemi A e B viene indicato da AB e associato dallo spazio di Hilbert $\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$. In questa tesi ci limitiamo a spazi di Hilbert di dimensione finita. In questo modo tutti gli operatori lineari sono anche limitati. Uno stato quantistico puro sarà rappresentato da uno stato nello spazio di Hilbert o da una matrice densità che definiamo quì di seguito. Faremo uso della notazione standard, e indicheremo uno stato $\psi \in \mathcal{H}$ come $|\psi\rangle$. Analogamente, l'operatore lineare duale allo stato ψ verrà indicato come $\langle\psi|$. Ricordiamo che gli stati $|\psi\rangle \in \mathcal{H}$ vengono chiamati puri.

1.1.1 Matrici densità

Vogliamo studiare sistemi composti, in particolare i loro sottosistemi individuali. Ci conviene quindi usare la formulazione della meccanica quantistica tramite matrici densità. Considerando un ensemble di stati puri con relativa distribuzione di probabilità $\{\psi_k, p_k\}$ definiamo la matrice densità come:

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|. \tag{1.1}$$

Si possono riformulare tutti i postulati della meccanica quantistica tramite le matrici densità. Utilizzare il formalismo delle matrici densità o quello dei vettori nello spazio di Hilbert (stati puri) porta quindi agli stessi risultati, ma è spesso molto più semplice studiare i problemi da uno solo dei punti di vista.

L'evoluzione di un sistema chiuso descritta dall'operatore unitario U ha la forma:

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k| \xrightarrow{U} \sum_k p_k U|\psi_k\rangle\langle\psi_k|U^\dagger = U\rho U^\dagger. \tag{1.2}$$

Si può fare una caratterizzazione delle matrici densità, in base alla certezza con cui conosciamo lo stato del sistema. Se infatti sappiamo che il sistema è descritto con certezza dallo stato $|\psi\rangle$ allora si avrà $\rho = |\psi\rangle\langle\psi|$, che viene detto stato puro (come abbiamo menzionato sopra). Quando una matrice densità non può essere scritta in questo modo per nessun vettore $|\psi\rangle \in \mathcal{H}$, diciamo che ρ è uno stato misto. Da ciò possiamo vedere che se un sistema quantistico viene preparato nello stato ρ_k con probabilità p_k allora sarà descritto dalla matrice densità $\sum_k p_k \rho_k$.

La matrice densità soddisfa inoltre le seguenti proprietà, che ci limitiamo a elencare:

Proposizione 1.1. *La matrice densità ρ soddisfa le seguenti proprietà:*

1. *È positiva, cioè $\forall|\phi\rangle \in \mathcal{H}$ $\langle\phi|\rho|\phi\rangle \geq 0$.*
2. *È autoaggiunta, cioè $\rho^\dagger = \rho$.*
3. *Ha traccia unitaria: $Tr(\rho) = 1$.*
4. *$\rho^2 = \rho \Leftrightarrow \rho$ è uno stato puro.*

Indicheremo l'insieme delle matrici densità del sistema fisico A come $\mathcal{S}(A)$.

1.1.2 Misura quantistica

Per la misura quantistica useremo il formalismo POVM. Abbiamo quindi l'insieme di risultati della misura $\{\lambda_m\}$ e dei rispettivi operatori di misura $\{M_m\}$ tali che $\sum_m M_m^\dagger M_m = \mathbb{I}$. Perciò abbiamo che la probabilità di ottenere come risultato della misura λ_m è $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$ e dopo la misura lo stato collassa come:

$$|\psi\rangle \to \frac{M_m|\psi\rangle}{\langle\psi|M_m^\dagger M_m|\psi\rangle}. \tag{1.3}$$

Vogliamo estendere questa trattazione alle matrici densità. Considerando lo stato $\rho = \sum_k p_k|\psi_k\rangle\langle\psi_k|$, abbiamo che, se lo stato iniziale è $\rho_k = |\psi_k\rangle\langle\psi_k|$, la probabilità di avere come risultato della misura λ_m è $p(m|k) = \langle\psi_k|M_m^\dagger M_m|\psi_k\rangle = \mathrm{Tr}(M_m^\dagger M_m|\psi_k\rangle\langle\psi_k|)$. Quindi, per lo stato ρ, avremo che la probabilità di ottenere il risultato λ_m è:

$$p(m) = \sum_k p(m|k)p_k = \sum_k p_k \mathrm{Tr}(M_m^\dagger M_m|\psi_k\rangle\langle\psi_k|) = \sum_k \mathrm{Tr}(M_m^\dagger M_m \rho) \tag{1.4}$$

e analogamente si ha che dopo la misura lo stato ρ collassa come:

$$\rho \to \frac{M_m|\psi_k\rangle\langle\psi_k|M_m^\dagger}{\mathrm{Tr}(M_m^\dagger M_m \rho)}. \tag{1.5}$$

Una proprietà interessante della misura è che, se abbiamo più misure una in seguito all'altra, possiamo sintetizzarle in un unica misura, infatti:

Proposizione 1.2. *Siano $\{L_l\}$ e $\{M_m\}$ due insiemi di operatori di misura, allora una misura definita dagli $\{L_l\}$ seguita da una misura definita da $\{M_m\}$ è fisicamente equivalente a una misura definita dall'insieme di operatori di misura $\{N_{lm}\}$, con $N_{lm} = M_m L_l$*

Dimostrazione. Consideriamo lo stato iniziale ρ_ψ, facciamo prima la misura con l'operatore L_l e poi con l'operatore M_m:

$$\rho_\psi \to L_l \rho_\psi L_l^\dagger \to M_m L_l \rho_\psi L_l^\dagger M_m^\dagger = (M_m L_l)\rho_\psi (M_m L_l)^\dagger = N_{lm}\rho_\psi N_{lm}^\dagger \tag{1.6}$$

basta quindi verificare che:

$$\sum_{l,m} N_{lm}^\dagger N_{lm} = \sum_l L_l^\dagger \left(\sum_m M_m^\dagger M_m \right) L_l = \sum_l L_l^\dagger L_l = \mathbb{I}. \tag{1.7}$$

□

1.2 Matrice densità ridotta

L'utilità delle matrici densità è in particolare evidente quando si ha a che fare con sistemi composti e si vogliono studiare i sottosistemi individuali. Supponiamo di avere due sistemi fisici A e B. Lo stato del sistema composto AB è ρ^{AB}. Possiamo allora definire la matrice densità ridotta per il sistema A come:

$$\rho^A = \mathrm{Tr}_B(\rho^{AB}) = \sum_k \langle b_k | \rho^{AB} | b_k \rangle \tag{1.8}$$

dove Tr_B è la traccia parziale definita sul sistema B e $|b_k\rangle$ una base di $\mathcal{H}^B$. Il motivo di questa definizione risulta evidente se si considera $\rho^{AB} = \rho \otimes \sigma$, dove ρ e σ sono matrici densità rispettivamente per il sistema A e B. Abbiamo infatti che $\rho^A = \mathrm{Tr}_B(\rho \otimes \sigma) = \rho$ e analogamente $\rho^B = \sigma$ e quindi si vede che la matrice densità ridotta descrive il sottosistema.

1.3 Canale quantistico

Nello studio dei sistemi chiusi l'evoluzione è descritta da operatori unitari. Nel mondo reale però non ci sono sistemi completamente chiusi, eccetto l'universo. C'è quindi bisogno di trovare uno strumento che ci permetta di studiare l'evoluzione di un sistema interagente con l'esterno. Costruiamo quindi il formalismo matematico che ci permette di studiare queste operazioni quantistiche.

La trasformazione fisica è rappresentata da una mappa $\mathcal{E} : \mathcal{S}(A) \to \mathcal{S}(B)$ tale che $\rho' = \mathcal{E}(\rho)$, che deve soddisfare alcune proprietà.
La prima è che preservi la traccia, cioè $\mathrm{Tr}(\mathcal{E}(\rho)) = 1$. Essa deve mandare infatti una matrice densità in un'altra.
La seconda proprietà è che $\mathcal{E}$ deve essere una mappa lineare, cioè per i coefficienti complessi a_k e le matrici densità ρ_k vale:

$$\mathcal{E}\left(\sum_k a_k \rho_k\right) = \sum_k a_k \mathcal{E}(\rho_k). \tag{1.9}$$

La terza proprietà è che $\mathcal{E}$ è una mappa completamente positiva, la cui definizione è:

Definizione 1.1. *Una mappa $\Phi : \mathbb{X} \to \mathbb{Y}$ è completamente positiva(CP) se:*

- *$\Phi(A)$ è positivo per ogni operatore $A \in \mathbb{X}$ positivo.*
- *Se introduciamo un sistema R allora $(\mathbb{I} \otimes \Phi)(A)$ è positivo per ogni operatore A positivo, dove $\mathbb{I}$ è l'identità sul sistema R.*

Quest'ultima proprietà è dovuta al fatto che vogliamo che $\mathcal{E}(\rho)$ sia anch'essa una matrice densità. Deve quindi essere positiva. Vogliamo anche che se ρ_{RA} è una matrice del sistema composto RA e agisce solo sul sistema A allora ρ_{RA} deve essere matrice densità su tutto il sistema composto. Queste mappe sono chiamate *canali quantistici*, o alternativamente mappe CPTP("completely positive trace preserving"). Indicheremo l'insieme dei canali quantistici che vanno dal sistema A al sistema Bcon $\mathcal{Q}(A \to B)$.

Il formalismo appena utilizzato è detto approccio assiomatico, per i canali quantistici ci sono però altri approcci, che risultano molto utili in alcuni casi, li riassumiamo brevemente.
Uno di questi è l'approccio della *rappresentazione di Kraus* che risulta molto utile nei calcoli. Si ha in questo caso una famiglia di operatori $\{E_k\}$ detti operatori di Kraus tali che $\sum_k E_k^\dagger E_k = \mathbb{I}$, e il canale quantistico può quindi essere espresso come:

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger. \tag{1.10}$$

1.4 Introduzione all'entanglement

Nello studio della meccanica quantistica fu riconosciuta da Einstein, Podolsky, Rosen e Schrödinger una proprietà che definirono come "spaventosa". Questa proprietà consiste nel fatto che esistono stati globali di un sistema composto che non possono essere scritti come prodotto di stati dei sottosistemi individuali. Questo fenomeno è conosciuto come *entanglement* ed evidenzia una correlazione fra i sottosistemi individuali del sistema

composto. Per comprendere ciò conviene introdurre un esempio. Consideriamo i due stati di due qubit:

$$|\psi\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right), \quad |\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.11}$$

Lo stato $|\psi\rangle$ può essere espresso come prodotto degli stati dei due qubit singoli, quindi una misura fatta su uno dei due qubit non influisce sulla misura dell'altro. Lo stato $|\phi\rangle$, invece, non può essere espresso come prodotto di stati dei due qubit singoli, risulta quindi uno stato detto *entangled*, e quando facciamo la misura su uno dei due qubit, andiamo a conoscere anche il risultato dell'altro qubit. È proprio questa correlazione fra i sottosistemi che caratterizza intuitivamente l'entanglement. La parte "spaventosa" dell'entanglement quindi è che disponiamo solo di una descrizione comune dei due qubit, mentre possiamo non avere nessuna informazione sullo stato del singolo qubit. Ciò implica che, nella meccanica quantistica, la miglior conoscenza possibile dello stato globale non include la miglior conoscenza possibile di tutte le sue parti.

1.4.1 Entanglement come risorsa

Questa correlazione fra i sottosistemi permette all'entanglement di essere usato come una risorsa quantistica che può essere utilizzata per svolgere compiti che non possono essere svolti tramite risorse classiche. In particolare, pur non portando lui stesso l'informazione, può essere usato per ridurre la complessità della comunicazione classica.
Un esempio di ciò è il *superdense coding*. Esso coinvolge due parti, che chiameremo Alice e Bob, che sono tra di loro molto distanti. Alice possiede due bit classici di informazione, e vuole trasmetterla a Bob mandandogli un solo qubit, è ciò possibile? La risposta è si, grazie proprio all'entanglement e tramite il processo di superdense coding.

Per mostrare ciò consideriamo lo stato entangled $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, dove il primo qubit è posseduto da Alice e il secondo da Bob, come mostrato in Fig. 1.1. Ad Alice basta quindi eseguire una operazione, dipendente dall'informazione che vuole inviare, sul proprio qubit prima di mandarlo a Bob, come indicato nel seguente schema:

$$\begin{aligned}
00: &\quad |\psi\rangle \to \mathbb{I}|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},\\
01: &\quad |\psi\rangle \to Z|\psi\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},\\
10: &\quad |\psi\rangle \to X|\psi\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}},\\
11: &\quad |\psi\rangle \to iY|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}},
\end{aligned}$$

dove X, Y, Z sono le matrici di Pauli. Quindi dopo l'operazione si ottiene come stato uno dei cosiddetti stati di Bell, che formano una base e quindi a Bob basta effettuare una misura nella base di Bell per completare il processo e ricevere l'informazione.
Questa operazione fatta da Alice sarebbe stata impossibile se si volesse usare un solo bit classico. Importante però notare che sono comunque coinvolti due qubit, ma ad Alice basta interagire con uno solo.

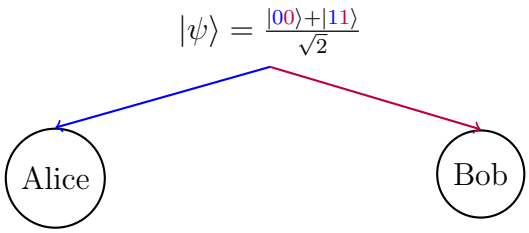

Figura 1.1: Schema che rappresenta la preparazione iniziale per il superdense coding. Viene preparato, da un agente esterno, lo stato entangled $|\psi\rangle$. Si inviano poi un qubit ad Alice e uno a Bob, che sono lontani fra loro.

Capitolo 2

Teoria quantistica delle risorse

In generale, quando si ha a che fare con un sistema fisico, non si può agire su di esso come vogliamo. Ad esempio in un laboratorio possiamo solo fare le operazioni che vengono permesse dai nostri strumenti. La teoria delle risorse si pone il compito di studiare sistemi fisici in cui abbiamo azioni libere, cioè che possono essere fatte liberamente, e azioni proibite. Gli oggetti che non si possono ottenere solo tramite operazioni libere verranno chiamati risorse. Uno degli interessi della teoria delle risorse è quello di studiare cosa si può fare quando in un sistema fisico, con relative operazioni libere, si ha accesso a delle risorse.

Questo approccio ha avuto particolare successo nell'ambito dell'informatica quantistica. Parliamo in questo caso di teoria quantistica delle risorse, dove le risorse coinvolgono oggetti o fenomeni dell'ordine atomico o subatomico, che devono essere studiati dal punto di vista quantistico.

Essa si sviluppò inizialmente per lo studio dell'entanglement. Come abbiamo infatti già visto l'entanglement è una risorsa. È quindi necessario definire strutture matematiche in grado di descriverla. L'obbiettivo è quello di studiare come caratterizzare, come manipolare, e come quantificare queste risorse. Alcune review sulla teoria delle risorse dell'entanglement sono [17, 13]. La teoria delle risorse è stata poi sviluppata anche in altri ambiti, come la termodinamica quantistica [12], i sistemi di riferimento quantistici e le asimmetrie [3], e la non Gaussianità [21].

Una struttura generale alle varie teorie quantistiche delle risorse è stato data in un articolo di review da Chitambar e Gour [8], che useremo in questa tesi.

2.1 Definizioni

Vogliamo per prima cosa dare una definizione di Teoria quantistica delle risorse:

Definizione 2.1. *Sia O una mappa che assegna a due sistemi di input/output A e B, con spazi di Hilbert $\mathcal{H}^A$ e $\mathcal{H}^B$, un unico insieme di operazioni CPTP $\mathcal{O}(A \to B) \equiv \mathcal{O}(\mathcal{H}^A \to$*

$\mathcal{H}^B) \subset \mathcal{Q}(A \to B)$. *Sia* $\mathcal{F}$ *la mappa indotta* $\mathcal{F}(\mathcal{H}) \coloneqq \mathcal{O}(\mathbb{C} \to \mathcal{H})$, *dove* $\mathcal{H}$ *è uno spazio di Hilbert arbitrario. Allora la coppia* $\mathcal{R} = (\mathcal{F}, \mathcal{O})$ *è chiamata* ***teoria quantistica delle risorse (QRT)*** *se valgono le 2 seguenti condizioni:*

- *Per ogni sistema fisico* A *il set* $\mathcal{O}(A) \coloneqq \mathcal{O}(A \to A)$ *contiene la mappa identità* id^A.
- *Per ogni tre sistemi fisici* A, B *e* C, *se* $\Phi \in \mathcal{O}(A \to B)$ *e* $\Lambda \in \mathcal{O}(B \to C)$, *allora* $\Lambda \circ \Phi \in \mathcal{O}(A \to C)$.

L'insieme $\mathcal{F}(\mathcal{H}) \subset \mathcal{S}(\mathcal{H})$ definisce l'insieme degli stati liberi agenti su $\mathcal{H}$ e gli elementi di $\mathcal{S}(\mathcal{H}) \setminus \mathcal{F}(\mathcal{H})$ sono invece gli stati risorsa. Analogamente le mappe CPTP appartenenti a $\mathcal{O}(A \to B)$ sono dette operazioni libere e quelle che non ci appartengono vengono dette risorse dinamiche.
In analogia con la notazione che stiamo utilizzando indicheremo $\mathcal{F}(A) \coloneqq \mathcal{F}(\mathcal{H}^A)$ e $\mathcal{F}(AB) \coloneqq \mathcal{F}(\mathcal{H}^A \otimes \mathcal{H}^B)$.
Quindi, dalla definizione 2.1, una QRT modella cosa, le parti che possiedono il sistema fisico, possano realizzare fisicamente date limitazioni e vincoli dovuti a limitazioni tecniche, limiti sperimentali o anche dalle leggi della fisica. Quali operazioni possono essere fatte dagli agenti è descritto matematicamente da $\mathcal{O}(A \to B)$, che è tipicamente molto più piccolo dell'insieme di tutti i canali quantistici.

La prima condizione dice che l'identità deve sempre essere un'operazione libera. Mentre la seconda condizione dice che la composizione di due operazioni libere sarà anch'essa libera. Queste garantiscono che le operazioni libere appartenenti ad $\mathcal{O}$ siano effettivamente libere, nel senso che possono essere eseguite liberamente, quante volte si vuole e in qualsiasi ordine. Una conseguenza della seconda condizione è che un'operazione libera non può convertire uno stato libero in uno non libero, o più formalmente:

Proposizione 2.1. ***(Regola d'oro della QRT)*** *Per ogni 2 sistemi fisici* A *e* B, *se* $\Phi \in \mathcal{O}(A \to B)$ *e* $\rho \in \mathcal{F}(A)$ *allora* $\Phi(\rho) \in \mathcal{F}(B)$.

Quindi le operazioni libere sono più fondamentali degli stati liberi. Questi ultimi sono infatti oggetti speciali che devono poter essere ottenuti liberamente. La loro preparazione sarà individuata dalle operazioni $\mathcal{O}(\mathbb{C} \to \mathcal{H}^A)$. Se però fissiamo l'insieme degli stati liberi possiamo ottenere diverse QRT. Quindi considereremo l'insieme degli stati liberi come una componente della QRT, anche se emergono dalla definizione di operazione libera.

La regola d'oro della QRT non implica che gli stati risorsa non abbiano ruolo nella QRT. Possono infatti essere usati per eludere, almeno parzialmente, la restrizione sulle operazioni permesse. Per esempio per un qualche $\sigma \notin \mathcal{F}(B)$ potrebbero esistere le mappe $\Phi \in \mathcal{O}(AB)$ e $\Lambda \notin \mathcal{O}(A)$ tali che $\Phi(\sigma \otimes \rho) = \Lambda(\rho)$ per ogni $\rho \in \mathcal{S}(A)$. In questo caso la risorsa σ permette di simulare una operazione Λ che sarebbe, negli altri casi, ristretta.

2.2 Struttura di prodotto tensoriale

Mentre la definizione 2.1 stipula i requisiti matematici minimi, nella pratica ci sono altre proprietà naturali che si possono desiderare in una QRT. Le più ovvie possono essere messe insieme in quella che è chiamata struttura di prodotto tensoriale:

Definizione 2.2. *Si dice che una QRT $\mathcal{R} = (\mathcal{F}, \mathcal{O})$ ammette una struttura di prodotto tensoriale se valgono le tre seguenti condizioni:*

1. *Le operazioni libere sono "completamente libere", cioè per ogni tre sistemi fisici A, B, C se $\Phi \in \mathcal{O}(A \to B)$ allora $id^C \otimes \Phi \in \mathcal{O}(CA \to CB)$.*

2. *Apporre stati liberi è un'operazione libera, cioè per ogni dato stato libero $\sigma \in \mathcal{F}(B)$, la mappa CPTP $\Phi_\sigma(\rho) \coloneqq \rho \otimes \sigma$ è una mappa libera, cioè appartiene a $\mathcal{O}(A \to AB)$.*

3. *Scartare un sistema è una operazione libera, cioè per ogni spazio di Hilbert $\mathcal{H}$, l'insieme $\mathcal{O}(\mathcal{H} \to \mathbb{R})$ non è vuoto.*

Osservazione 2.1. *$\mathcal{B}(\mathcal{H} \to \mathbb{R})$ contiene una sola mappa CPTP, la traccia. Quindi la condizione 3 equivale a dire che per ogni $\mathcal{H}$ l'insieme $\mathcal{O}(\mathcal{H} \to \mathbb{R})$ contiene la traccia.*

La prima condizione dice che le operazioni libere rimangono libere anche quando agiscono su una sola parte di un sistema composto. Tali mappe vengono dette completamente libere (in analogia con le mappe CP). Come conseguenza della prima condizione abbiamo che se $\Phi \in \mathcal{O}(A \to B)$ e $\Phi' \in \mathcal{O}(A' \to B')$, allora $\Phi \otimes \Phi' \in \mathcal{O}(AA' \to BB')$, essendo quest'ultima composizione di operazioni libere: $\Phi \otimes \Phi' = (id^B \otimes \Phi') \circ (\Phi \otimes id^{A'})$. La seconda e terza condizioni dicono invece che apporre o scartare un sistema è una operazione libera. Entrambe sono condizioni naturali per una QRT, in particolare l'abilità di apporre stati liberi arbitrari a qualsiasi sistema riflette la situazione dove gli stati liberi sono veramente liberi da generare.

Queste condizioni non sono completamente indipendenti, e portano a interessanti conseguenze:

Proposizione 2.2. *Per una QRT con struttura di prodotto tensoriale abbiamo che:*

1. *La traccia parziale $id \otimes Tr$ è una operazione libera.*

2. *Ogni canale di rimpiazzo $\Lambda_\sigma \in \mathcal{Q}(A \to B)$ della forma $\Lambda_\sigma(X) \coloneqq Tr(X)\sigma$, con $\sigma \in \mathcal{F}(B)$ fissato, è libero.*

3. *Se $\rho \in \mathcal{F}(A)$ e $\sigma \in \mathcal{F}(B)$ allora $\rho \otimes \sigma \in \mathcal{F}(AB)$.*

Dimostrazione. La prima conseguenza segue immediatamente dalle condizioni 1 e 3 della definizione 2.2.
Per la seconda conseguenza abbiamo che $\Lambda_\sigma(X) = \mathrm{Tr}(X)\sigma = (\mathrm{Tr} \circ \Phi_\sigma)(X)$, con $\Phi_\sigma(\rho) = \rho \otimes \sigma$ libera per la condizione 2 della definizione 2.2. Quindi Λ_σ è libera perché composizione di operazioni libere.
Inoltre, essendo $\Phi_\sigma(\rho) = \rho \otimes \sigma \in \mathcal{O}(A \to AB)$ e $\rho \in \mathcal{F}(A)$ per la proposizione 2.1 $\rho \otimes \sigma \in \mathcal{F}(AB)$, che dimostra la terza conseguenza. □

L'intuizione dietro quest'ultima proprietà è che se ρ e σ sono libere da preparare separatamente, allora anche lo stato composto $\rho \otimes \sigma$ deve esserlo. Questo implica anche che $\mathcal{F}(A) \otimes \mathcal{F}(B) \subset \mathcal{F}(AB)$ per ogni 2 sistemi fisici A e B, mentre il contrario vale solo parzialmente. Cioè se $\rho^{AB} \in \mathcal{F}(AB)$ allora $\rho^A \in \mathcal{F}(A)$ e $\rho^B \in \mathcal{F}(B)$, essendo la traccia parziale un'operazione libera.

2.3 QRT consistente

Nel modellare sistemi fisici con la QRT si hanno i vincoli fisici che ci danno o l'insieme delle operazioni libere o quello degli stati liberi, ma come abbiamo visto in precedenza si possono ricavare gli stati liberi dalle operazioni libere. È quindi necessario, nella costruzione del modello, definire una QRT consistente.

2.3.1 QRT consistente per un dato insieme di operazioni libere

Supponiamo che le operazioni libere di un sistema fisico A siano fissate dai vincoli fisici. Vogliamo costruire una QRT consistente con queste operazioni libere $\mathcal{O}(A)$. Per prima cosa vediamo che l'insieme $\mathcal{O}(A)$ impone un preordine(vedi Definizione 2.6) sull'insieme delle matrici densità $\mathcal{S}(A)$. Dati infatti due stati arbitrari $\rho, \sigma \in \mathcal{S}(A)$ possiamo scrivere:

$$\rho \xrightarrow{\mathcal{O}} \sigma \qquad \text{se} \quad \exists \Phi \in \mathcal{O}(A) \quad \text{tale che} \quad \sigma = \Phi(\rho). \tag{2.1}$$

Se $\rho \xrightarrow{\mathcal{O}} \sigma$ e $\sigma \xrightarrow{\mathcal{O}} \rho$ scriveremo $\rho \overset{\mathcal{O}}{\approx} \sigma$. Esso è chiaramente un preordine. Vale infatti la proprietà transitiva: se $\rho \xrightarrow{\mathcal{O}} \sigma$ e $\sigma \xrightarrow{\mathcal{O}} \gamma$ allora $\rho \xrightarrow{\mathcal{O}} \sigma$.
Possiamo quindi definire un insieme minimo di stati liberi per ogni insieme di operazioni $\mathcal{O}(A)$:

Definizione 2.3. *L'insieme minimo di stati liberi associati all'insieme di operazione libere $\mathcal{O}(A)$ è definito come:*

$$\mathcal{F}_{min}(A) = \{\rho \in \mathcal{S}(A) \,:\, \forall \sigma \in \mathcal{S}(A)\ \exists \Phi \in \mathcal{O}(A) \,:\, \rho = \Phi(\sigma)\}. \tag{2.2}$$

In altre parole $\rho \in \mathcal{F}_{min}(A)$ se può essere liberamente generato partendo da ogni altro stato. Se inoltre consideriamo una QRT consistente con l'insieme di stati liberi $\mathcal{F}(A)$ dobbiamo avere $\mathcal{F}_{min}(A) \subseteq \mathcal{F}(A)$. Infatti se $\sigma \in \mathcal{F}(A)$ e $\rho \in \mathcal{F}_{min}(A)$, per definizione di $\mathcal{F}_{min}$, abbiamo che $\sigma \xrightarrow{\mathcal{O}} \rho$ e per Proposizione 2.1 $\rho \in \mathcal{F}(A)$, che dà senso al termine "minimo".

Quindi se supponiamo che tutti gli stati liberi siano convertibili fra di loro tramite operazioni libere avremo che $\mathcal{F}_{min}(A) = \mathcal{F}(A)$, più formalmente:

Proposizione 2.3. *Sia $\mathcal{F}(A)$ un insieme di stati liberi consistenti con $\mathcal{O}(A)$, se per ogni $\rho, \sigma \in \mathcal{F}(A)$ vale $\rho \overset{\mathcal{O}}{\approx} \sigma$ allora $\mathcal{F}_{min}(A) = \mathcal{F}(A)$.*

Dimostrazione. Siano $\sigma \in \mathcal{F}(A)$ e $\rho \in \mathcal{F}_{min}(A)$. Essendo $\mathcal{F}_{min}(A) \subseteq \mathcal{F}(A)$ abbiamo che $\rho \in \mathcal{F}(A)$. Quindi per ipotesi deve essere $\rho \overset{\mathcal{O}}{\approx} \sigma$.
Per definizione di F_{min} abbiamo che $\forall \omega \in \mathcal{S}(A)$, $\omega \xrightarrow{\mathcal{O}} \sigma$. Per la proprietà transitiva $\omega \xrightarrow{\mathcal{O}} \sigma$ e quindi $\mathcal{F}(A) \subseteq \mathcal{F}_{min}(A)$.

□

Un tipo di QRT per cui vale questa proprietà sono quelle con una struttura di prodotto tensoriale. Più in generale è sufficiente che la QRT permetta sia lo scarto di un sistema e sia la preparazione di ogni stato libero. Se infatti combino le due operazioni ottengo il canale di rimpiazzo $\Phi_\sigma(X) = \mathrm{Tr}(X)\sigma$ per qualche stato libero σ. Quindi l'insieme degli stati liberi deve essere $\mathcal{F}_{min}(A)$.

In conclusione, dato un insieme di operazioni libere $\mathcal{O}(A)$, se uno desidera una QRT in cui gli stati liberi sono tra loro liberamente convertibili e dove scartare un sistema è permesso, allora $\mathcal{F}_{min}(A)$ è l'unico insieme di stati liberi permesso.

2.4 QRT convessa

La definizione 2.1 impone una piccola struttura matematica sulla teoria. Successivamente abbiamo introdotto la struttura di prodotto tensoriale, che accorpa una collezione di proprietà naturali possedute da quasi tutte le QRT in letteratura. Esistono però altri tipi di strutture matematiche che si possono venire fuori in una QRT, indipendentemente dalla struttura di prodotto tensoriale. In particolare a noi interessano le teorie delle risorse convesse.

Definizione 2.4. *Una QRT $\mathcal{R} = (\mathcal{F}, \mathcal{O})$ è detta convessa se $\mathcal{O}(A \to B)$ è convesso per ogni scelta di spazi di Hilbert $\mathcal{H}^A$, $\mathcal{H}^B$, cioè:*

$$p\Phi + (1-p)\Lambda \in \mathcal{O}(A \to B) \qquad \forall \Phi, \Lambda \in \mathcal{O}(A \to B),\, p \in [0,1] \quad \forall \mathcal{H}^A, \mathcal{H}^B. \tag{2.3}$$

Nella nostra formulazione di QRT gli stati liberi $\mathcal{F}(\mathcal{H}) = \mathcal{O}(A \to B)$ sono definiti come un caso speciale delle operazioni libere. Quindi in una QRT convessa anche $\mathcal{F}(A)$

è convesso. Il contrario non è però vero in generale. La convessità è una proprietà importante perché permette di fare uso dell'analisi convessa.

2.5 Quantificare le risorse

L'approccio utilizzato con la QRT permette di definire modi precisi e operazionalmente utili per quantificare le risorse. Una QRT è definita su un qualunque spazio di Hilbert $\mathcal{H}$. Perciò la misura deve poter agire su tutti gli stati di un qualsiasi spazio. Si possono quindi considerare funzioni non negative della forma: $f : \cup_{\mathcal{H}} \mathcal{S}(\mathcal{H}) \to \mathbb{R}_0^+$. In pratica si può anche considerare un dominio più ristretto, limitandosi a un solo spazio di Hilbert $\mathcal{H}$.

La proprietà più fondamentale di una misura delle risorse è la monotonia. In particolare definiamo:

Definizione 2.5. *Una funzione non negativa $f : \cup_{\mathcal{H}} \mathcal{S}(\mathcal{H}) \to \mathbb{R}_0^+$ è chiamata funzione monotona se, per ogni $\Phi \in \mathcal{O}(A \to B)$ e $\rho \in \mathcal{S}(A)$ vale:*

$$f(\rho) \geq f(\Phi(\rho)). \tag{2.4}$$

Questa definizione acquisisce significato se ci si ricorda che, in una QRT, le operazioni libere non possono generare risorse. Se nella QRT considerata gli stati liberi sono convertibili l'uno con l'altro, allora la monotonia implica che per ρ, σ liberi abbiamo $f(\rho) = f(\sigma)$. Possiamo quindi porre per comodità $f(\rho) = f(\sigma) = 0$, imponendo che si annulli per gli stati liberi. Vi sono altre proprietà che possono caratterizzare una misura delle risorse, che però esulano dagli obbiettivi di questa tesi, e vengono quindi omesse.

2.6 Teoria quantistica delle risorse dell'entanglement

L'entanglement è un fenomeno prettamente quantistico, non esistente nella meccanica classica e che viene fuori quando si ha a che fare con sistemi composti da più sottosistemi. Esistono infatti stati del sistema composto che non possono essere espressi come prodotto di stati dei sottosistemi individuali. La teoria dell'entanglement è l'applicazione più nota della QRT, vediamo ora come.

2.6.1 Il protocollo LOCC

Nella teoria delle risorse dell'entanglement le operazioni libere derivano dallo scenario fisico dove sistemi spazialmente separati si scambiano tra di loro informazione classica liberamente, ma l'informazione quantistica viene processata solo localmente, tramite mappe CPTP agenti sui sottosistemi individuali. Si parla quindi di protocollo LOCC,

che sta per"local operations classical communication". Le mappe globali che possono essere applicate sotto queste restrizioni formeranno quindi la classe delle operazioni libere sotto LOCC. Ogni operazione LOCC è formata da round strutturati come:

1. Misura locale di una delle parti.
2. Broadcast globale del risultato della misura.

Se quindi vogliamo ottenere una forma matematica dobbiamo concatenare gli operatori di Kraus delle operazioni locali:

$$\Lambda(\rho) = \sum_k (\otimes_{i=1}^N M_{k,i}^{A_i}) \rho (\otimes_{i=1}^N M_{k,i}^{A_i})^\dagger \tag{2.5}$$

dove $M_{k,i}^{A_i}$ agiscono sul sottosistema A_i. Ogni operatore LOCC avrà quindi questa forma, ma non vale l'inverso. La classe delle mappe con forma (2.5) è infatti chiamata delle operazioni separabili, e le operazione LOCC sono solo un loro sottoinsieme. Questo rende lo studio delle operazioni LOCC molto complicato e non è ancora possibile capire se una operazione qualsiasi Λ sia implementabile tramite LOCC. Lo studio delle loro proprietà è quindi fatto lavorando su classi più "ampie" che contengono le operazioni LOCC, le cui proprietà saranno quindi anche valide per le operazioni LOCC.

2.6.2 Stati separabili

Vogliamo ora costruire l'insieme di stati liberi per le operazioni LOCC.

Proposizione 2.4. *Gli stati liberi per LOCC su uno spazio di stati N-partito* $\mathcal{H} = \otimes_{i=1}^N \mathcal{H}_i$ *hanno la forma:*

$$\rho^{A_1,A_2,\dots,A_N} = \sum_k p_k \rho_{1,k}^{A_1} \otimes \rho_{2,k}^{A_2} \otimes \cdots \otimes \rho_{N,k}^{A_N}. \tag{2.6}$$

Dimostrazione. La trasformazione $\sigma^{A_1,A_2,\dots,A_N} \xrightarrow{\mathcal{O}} \rho^{A_1,A_2,\dots,A_N}$ per ogni stato $\sigma^{A_1,A_2,\dots,A_N}$ è ottenibile scartando prima lo stato $\sigma^{A_1,A_2,\dots,A_N}$ e generando localmente i vari stati $\rho_{i,k}^{A_i}$ secondo la distribuzione p_k. □

Questi stati sono detti separabili e possiamo definire l'insieme che li contiene come SEP($\mathcal{H}$), possiamo inoltre vedere che:

Proposizione 2.5. *Per LOCC abbiamo che:*

$$SEP(\mathcal{H}) = \mathcal{F}_{min}(\mathcal{H}). \tag{2.7}$$

Dimostrazione. Segue direttamente da prop 2.4. □

Gli stati non appartenenti a SEP($\mathcal{H}$) vengono chiamati stati entangled, e sono gli stati risorsa della QRT. Quindi l'entanglement viene definito indirettamente dalle trasformazioni LOCC, come risorsa che quest'ultime non possono generare.

Risulta però molto complesso capire se uno stato è separabile o entangled, per ovviare a questo problema si sono cercati dei criteri di separabilità, cioè condizione necessarie (ma non sufficienti) per la separabilità di uno stato.

2.6.3 Entanglement bipartito e relazioni d'ordine

Il caso più semplice di entanglement è quello bipartito, dove abbiamo solo due sottosistemi individuali del sistema composto. Per comodità sfruttiamo lo stesso formalismo usato nel superdense coding, avremo cioè Alice e Bob che possono agire rispettivamente sui sottosistemi A e B. In questo caso abbiamo quindi che uno stato ρ di $\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$ è separabile se si può scrivere come:

$$\rho = \sum_k p_k \rho_k^A \otimes \rho_k^B \tag{2.8}$$

dove ρ_k^A è definito su $\mathcal{H}^A$ e ρ_k^B su $\mathcal{H}^B$. In particolare se è uno stato puro si può scrivere $\rho = \rho^A \otimes \rho^B$ dove ρ^A, ρ^B sono stati puri, in quest'ultimo caso possiamo anche esprimerlo in forma vettoriale:

$$|\psi\rangle = |\psi^A\rangle \otimes |\psi^B\rangle \tag{2.9}$$

con $|\psi\rangle \in \mathcal{H}^{AB}$, $|\phi^A\rangle \in \mathcal{H}^{\mathcal{A}}$ e $\psi^B \in \mathcal{H}^{\mathcal{B}}$.

Vogliamo ora definire delle relazioni d'ordine all'entanglement bipartito, esse possono infatti essere usate per confrontare le risorse, senza dover definire una misura su di esse. Diamo per prima cosa una definizione di relazione d'ordine parziale e di preordine.

Definizione 2.6. *Sia P un insieme e $\leq$ una relazione binaria su P, allora $\leq$ è detta relazione d'ordine parziale se valgono le seguenti proprietà:*

1. *$a \leq a \quad a \in P$ (riflessività).*
2. *Se $a \leq b$ e $b \leq c$ con $a, b, c \in P$, allora $a \leq c$ (transitività).*
3. *Se $a \leq b$ e $b \leq a$ con $a, b \in P$, allora $a = b$ (antisimmetria).*

Se valgono solo le prime due proprietà viene invece chiamata preordine.

dove il termine "parziale" è dovuto al fatto che non venga richiesto che due qualsiasi elementi di P siano in relazione fra loro.

È possibile definire un preordine sfruttando la convertibilità degli stati fra di loro. Abbiamo infatti già definito un preordine in precedenza, quando abbiamo costruito l'insieme minimo degli stati liberi, dove erano le operazioni libere a generarlo.

Possiamo in questo modo confrontare il "grado" di risorsa di uno stato, a noi in particolare interessa poter confrontare l'entanglement fra due stati. Per capire ciò ci basta guardare come abbiamo definito gli stati separabili. Essi infatti sono gli stati che possono essere ottenuti da un qualsiasi altro stato, entangled o non, tramite LOCC. Si intuisce quindi che se possiamo trasformare lo stato $|\psi\rangle$ in $|\phi\rangle$ tramite LOCC ma non possiamo fare l'inverso, allora $|\phi\rangle$ sarà meno entangled di $|\psi\rangle$. Se invece potessimo trasformare l'uno nell'altro saranno ugualmente entangled. Questo è coerente col concetto di risorsa, sarebbe infatti assurdo, per costruzione della QRT, poter generare risorse tramite operazioni libere. Lo studio della convertibilità tramite LOCC per stati puri sarà proprio l'argomento centrale del prossimo capitolo.

Sfortunatamente l'obbligo che le trasformazioni avvengano con certezza è solitamente troppo restringente. In generale, nelle QRT più interessanti, non sarà possibile trasformare perfettamente uno stato dato, o viceversa, in un altro tramite le operazioni libere. In particolare più è grande la dimensione dei sottosistemi più sarà difficile che due stati qualsiasi siano comparabili. Per ovviare a questo problema si può rilassare la condizione che $\rho \to \sigma$ debba avvenire con certezza. Si dice quindi che σ è ottenibile tramite una trasformazione stocastica da ρ, e si scrive $\rho \xrightarrow{SO} \sigma$ se σ è ottenibile da ρ, con una probabilità non nulla, tramite LOCC. Questa classe di trasformazioni è chiamata SLOCC, e ne vedremo l'utilità più avanti.

Capitolo 3

Teorema di Nielsen

Vogliamo ora concentrarci sulle trasformazioni dell'entanglement, in particolare vogliamo capire quando possiamo trasformare lo stato puro $|\psi\rangle$ in $|\phi\rangle$ tramite LOCC. Questa domanda fu risposta da Nielsen in un articolo del 1999 [15], la cui dimostrazione venne raffinata da Nielsen e Chuang [16]. In questo capitolo vogliamo arrivare alla dimostrazione di questo risultato.

3.1 Preliminari matematici

La convertibilità tra stati puri entangled bipartiti è strettamente legata a un'area di ricerca in algebra lineare abbastanza attiva, la teoria della maggiorazione, che introdurremo più avanti. Vedremo che essa è legata alle matrici stocastiche e alla convessità. Inoltre tratteremo due strumenti molto utili nello studio dell'entanglement bipartito: la decomposizione di Schmidt e la purificazione.

3.1.1 Convessità

Abbiamo già visto il concetto di convessità quando abbiamo trattato la QRT. Diamo ora la definizione di insieme convesso:

Definizione 3.1. *Sia V spazio vettoriale, l'insieme $A \subseteq V$ si dice convesso se:*

$$\forall x, y \in A \quad \{(1-t)x + ty \,:\, t \in]0,1[\} \subseteq A.$$

È inoltre utile dare la definizione di combinazione convessa, che sfrutteremo più volte, avendo a che fare con distribuzioni di probabilità:

Definizione 3.2. *Una combinazione convessa è una combinazione lineare(di vettori, scalari, ecc.) dove tutti i coefficienti sono non-negativi e hanno come somma 1:*

$$\sum_j \alpha_j x_j \quad con \quad \sum_j \alpha_j = 1 \quad e \quad \alpha_j \geq 0 \quad \forall j.$$

Un esempio già visto di combinazioni convesse sono gli stati misti.

3.1.2 Matrici stocastiche

Diamo quindi le definizioni di matrice stocastica e di matrice doppiamente stocastica:

Definizione 3.3. *Una matrice $n \times n$ A è detta stocastica se i suoi elementi sono tutti non negativi e se la somma su ogni riga è 1, cioè:*

$$A_{ij} \geq 0 \quad per \quad i, j = 1, \ldots, n, \tag{3.1}$$

$$\sum_{j=1}^{n} A_{ij} = 1 \quad per \quad i = 1, \ldots, n. \tag{3.2}$$

Definizione 3.4. *Una matrice $n \times n$ A stocastica è detta doppiamente stocastica se la somma su ogni colonna è 1, cioè:*

$$\sum_{i=1}^{n} A_{ij} = 1 \quad per \quad j = 1, \ldots, n. \tag{3.3}$$

Il nome di queste matrici deriva dal ruolo che coprono nella teoria delle catene di Markov discrete. Le matrici doppiamente stocastiche possono essere chiamate anche *trasformazionidi Schur* o *bistocastiche*. Caso particolare di matrici doppiamente stocastiche è quello delle matrici di permutazione, che possiamo definire come:

Definizione 3.5. *Sia $\pi : \{1, \ldots, m\} \to \{1, \ldots, m\}$ una permutazione di m elementi. Sia $\vec{e}_j$ la base canonica di lunghezza m, allora la matrice di permutazione $m \times m$ associata a π è definita come:*

$$P_\pi = \begin{pmatrix} \vec{e}_{\pi(1)} \\ \vec{e}_{\pi(2)} \\ \cdots \\ \vec{e}_{\pi(m)} \end{pmatrix}. \tag{3.4}$$

Esse hanno un unico elemento unitario per ogni riga e per ogni colonna, è quindi evidente che siano doppiamente stocastiche.
Risultato importante sulle matrici stocastiche è il Teorema di Birkhoff, che dice:

Teorema 3.1. *(**Teorema di Birkhoff**) Una matrice $d \times d$ D è doppiamente stocastica se e solo se può essere scritta come combinazione convessa di matrici di permutazione, cioè*

$$D = \sum_j p_j P_j \qquad con \quad \sum_j p_j = 1 \quad e \quad P_j \text{ matrici di permutazione.} \tag{3.5}$$

Questo Teorema, che non dimostriamo, è importante perché mostreremo che connette il concetto di maggiorazione con le matrici doppiamente stocastiche, permettendoci di allargare il concetto di maggiorazione anche agli operatori.

3.1.3 Decomposizione di matrici

Nella meccanica quantistica si ha a che fare con operatori lineari. Risulta quindi molto utile trovare dei modi per separare questi operatori in parti più semplici. In particolare le seguenti decomposizioni ci permettono di esprimere un operatore lineare come prodotto di operatori unitari e positivi.

Teorema 3.2. *(**Decomposizione polare**) Sia A un operatore lineare su uno spazio vettoriale V, allora esistono U operatore unitario e J, K operatori positivi tali che:*

$$A = UJ = KU \tag{3.6}$$

dove gli operatori positivi unici J e k che soddisfano l'equazione sono definiti da:

$$J \equiv \sqrt{A^\dagger A}, \quad K \equiv \sqrt{AA^\dagger}. \tag{3.7}$$

Inoltre se A è invertibile allora U è unica.

Dimostrazione. Consideriamo $J \equiv \sqrt{A^\dagger A}$, che è positivo e quindi hermitiano per definizione, possiamo quindi scrivere:

$$J = \sum_i \lambda_i |i\rangle\langle i| \quad \text{con} \quad \lambda_i \geq 0 \tag{3.8}$$

dove $|i\rangle$ è la base ortonormale che diagonalizza J. Definiamo poi $|\psi_i\rangle = A|i\rangle$ da cui si vede che:

$$\langle \psi_i \,|\, \psi_i \rangle = \langle i|A^\dagger A|i\rangle = \langle i|J^2|i\rangle = \lambda_i^2. \tag{3.9}$$

Consideriamo ora solo gli i con $\lambda_i \neq 0$ per i quali definiamo $|e_i\rangle = \frac{1}{\lambda_i}|\psi_i\rangle$, che formano un sistema ortonormale, infatti:

$$\langle e_i \,|\, e_j \rangle = \frac{1}{\lambda_i \lambda_j}\langle i|J^2|j\rangle = \frac{\lambda_i \lambda_j}{\lambda_i \lambda_j}\langle i \,|\, j\rangle = \delta_{ij}. \tag{3.10}$$

Si usa poi il metodo di Gram-Schmidt per completare $|e_i\rangle$ a una base ortonormale. Definiamo quindi l'operatore $U = \sum_i |e_i\rangle\langle i|$, che è unitario, infatti:

$$U^\dagger U = \sum_{i,j} |j\rangle\langle e_j \,|\, e_i\rangle\langle i| = \sum_i |i\rangle\langle i| = \mathbb{I}. \tag{3.11}$$

Inoltre abbiamo che:

$$\text{con } \lambda_i \neq 0 \qquad UJ|i\rangle = \sum_k |e_k\rangle\langle k|J|i\rangle = \lambda_i |e_i\rangle = |\psi_i\rangle = A|i\rangle, \tag{3.12}$$

$$\text{con } \lambda_i = 0 \qquad UJ|i\rangle = 0 = A|i\rangle. \tag{3.13}$$

Abbiamo mostrato che $A = UJ$ sui vettori della base. Quindi, essendo A lineare, risulta definita su tutto lo spazio. Si può vedere poi che J risulta unica, infatti:

$$A^\dagger A = JU^\dagger UJ = J^2 \Rightarrow J = \sqrt{A^\dagger A} \quad \text{in modo unico.} \tag{3.14}$$

Se A è invertibile allora lo è anche J e possiamo scrivere:

$$A^{-1} = (UJ)^{-1} = j^{-1}U^{-1} \Rightarrow U = AJ^{-1} \tag{3.15}$$

e quindi, dall'unicità di J, risulta unica anche U. Per l'altra decomposizione scriviamo:

$$A = UJ = UJU^\dagger U = KU \Rightarrow K = UJU^\dagger, \tag{3.16}$$

$$AA^\dagger = KUU^\dagger K = K^2 \Rightarrow K = \sqrt{AA^\dagger}. \tag{3.17}$$

□

Se combiniamo la decomposizione polare con il Teorema spettrale, otteniamo la seguente decomposizione:

Teorema 3.3. *(**Decomposizione ai valori singolari**) Sia A una matrice quadrata. Allora esistono le matrici unitarie U e V, e una matrice diagonale D con elementi non negativi tali che $A = UDV$.*
Gli elementi diagonali di D sono chiamati valori singolari di A.

Dimostrazione. Da Teorema 3.2 posso scrivere $A = SJ$, con S unitaria e J positiva. Dal Teorema spettrale si ha che esistono la matrice unitaria T e la matrice diagonale D tali che $J = TDT^\dagger$, dove gli elementi di D sono non negativi perché J è positiva. Ponendo $U = ST$ e $V = T^\dagger$ dimostriamo la tesi.

□

3.1.4 Decomposizione di Schmidt

Introduciamo ora un importante strumento nello studio dei sistemi composti, in particolare nello studio dell'entanglement bipartito:

Teorema 3.4. *(**Decomposizione di Schmidt**) Sia $|\psi\rangle$ uno stato puro di un sistema composto AB, allora esistono stati ortonormali $|i_A\rangle$ per A e $|i_B\rangle$ per B tali che:*

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle \qquad con \quad \lambda_i \geq 0 \quad tali\ che \quad \sum_i \lambda_i^2 = 1. \tag{3.18}$$

Inoltre i valori dei λ_i sono unici.

Dimostrazione. Dimostriamo prima il caso $\dim(A) = \dim(B) = n$. Siano $|j\rangle$ e $|k\rangle$ basi ortonormali rispettivamente di A e B, si può quindi scrivere:

$$|\psi\rangle = \sum_{j,k} a_{jk} |j\rangle |k\rangle \qquad \text{con } a \text{ matrice complessa.} \tag{3.19}$$

Decomponendo poi a ai valori singolari (Teorema 3.3) si ottiene $a = udv$, con u, v matrici unitarie e d matrice diagonale a valori non-negativi. Abbiamo quindi:

$$a_{jk} = \sum_{i=1}^{n} u_{ji} d_{ii} v_{ik} \Rightarrow |\psi\rangle = \sum_{i,j,k} u_{ji} d_{ii} v_{ik} |j\rangle |k\rangle \tag{3.20}$$

se definiamo $|i_A\rangle \sum_j u_{ji} |j\rangle$ e $|i_B\rangle = \sum_k v_{ik} |k\rangle$ e $\lambda_i = d_{ii} \geq 0$ otteniamo $|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$. Rimane solo da verificare che $|i_A\rangle$ e $|i_B\rangle$ sono ortonormali:

$$\langle l_A \,|\, i_A \rangle = \sum_{j,m} u^*_{ml} u_{ji} \langle m \,|\, j \rangle = \sum_j u^*_{jl} u_{ji} = \delta_{il} \tag{3.21}$$

dove nell'ultima uguaglianza viene sfruttata l'unitarietà di u. Per $|i_B\rangle$ i calcoli sono analoghi. Si può espandere anche al caso $\dim(A) \neq \dim(B)$, con una dimostrazione analoga, usando però il caso più generale della decomposizione ai valori singolari. □

Le basi $|i_A\rangle$ e $|i_B\rangle$ sono chiamate *basi di Schmidt* rispettivamente per i sistemi A e B. Il numero n_ψ dei λ_i non nulli è chiamato *numero di Schmidt* per lo stato $|\psi\rangle$. Il numero di Schmidt assume un ruolo importante per un sistema quantistico bipartito. Vedremo che distingue qualitativamente l'entanglement degli stati puri. In particolare uno stato puro è separabile solo se ha $n_\psi = 1$.
La dimostrazione della decomposizione mostra che essa non è che un'altra forma della decomposizione ai valori singolari. Ciò mostra l'utilità delle decomposizioni degli operatori lineari, che ci permettono di capire tante proprietà dei sistemi quantistici.
Una conseguenza di questo Teorema, che ne mostra anche l'utilità, si ha considerando le

matrici densità ridotte. Sia $|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle$ la decomposizione di Schmidt per $|\psi\rangle$. Allora le matrici ridotte devono avere la forma $\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$ e $\rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$. Hanno quindi gli stessi autovalori λ_i^2. Inoltre i ranghi di ρ^A e ρ^B sono uguali al numero di Schmidt. Molte proprietà dei sistemi composti sono determinate dagli autovalori della matrice densità. Sono quindi le stesse per entrambi i sottosistemi.

Un risultato di particolare importanza, che mette in relazione stati con coefficienti di Schmidt identici, è il seguente:

Proposizione 3.5. *Se due stati puri $|\psi\rangle$ e $|\phi\rangle$, dello stesso sistema composto dai sottosistemi A e B, hanno gli stessi coefficienti di Schmidt, allora esistono due trasformazioni unitarie U, sul sottosistema A, e V, sul sottosistema B, tali che $|\psi\rangle = (U \otimes V)|\phi\rangle$.*

Dimostrazione. Abbiamo che:

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle \quad \text{e} \quad |\phi\rangle = \sum_i \lambda_i |i'_A\rangle|i'_B\rangle$$

con $|i_A\rangle$ e $|i'_A\rangle$ basi di A e $|i_B\rangle$ e $|i'_B\rangle$ basi di B.
Possiamo quindi definire le trasformazioni unitarie U e V sulle basi come:

$$U|i'_A\rangle = |i_A\rangle \quad \text{e} \quad V|i'_B\rangle = |i_B\rangle$$

e la tesi è immediatamente dimostrata. □

Quindi possiamo dire che due stati puri che hanno stessi coefficienti di Schmidt sono equivalenti a meno di operazioni unitarie locali. Quindi per lo studio dell'entanglement bipartito degli stati puri ci interessano solo questi coefficienti

3.1.5 Purificazione

Come visto prima la matrice ridotta dello stato puro $|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_A\rangle$ ha la forma $\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$. Abbiamo quindi che ρ^A è uno stato puro(misto) solo se $|\psi\rangle$ è separabile(entangled). Ci vogliamo quindi chiedere se sia possibile, partendo da uno stato misto, introdurre un nuovo sistema fisico per avere come stato del sistema composto uno stato puro. Il seguente risultato risponde a questa domanda.

Teorema 3.6. *Sia ρ^A lo stato del sistema quantistico A, allora è possibile introdurre un sistema R e definire lo stato puro $|AR\rangle$ per il sistema composto AR tale che soddisfi:*

$$\rho^A = Tr_R(|AR\rangle\langle AR|). \tag{3.22}$$

Dimostrazione. Consideriamo la decomposizione ortonormale $\rho^A = \sum_i p_i |i_A\rangle\langle i_A|$, con $|i_A\rangle$ base ortonormale di A e introduciamo R tale che $\dim(\mathbb{H}^A) = \dim(\mathbb{H}^R)$ con $|i_R\rangle$ base ortonormale di R. Possiamo definire:

$$|AR\rangle \equiv \sum_i \sqrt{p_i} |i_A\rangle|i_R\rangle \tag{3.23}$$

che ridotto al sistema A diventa:

$$\begin{aligned}\mathrm{Tr}_R(|AR\rangle\langle AR|) &= \sum_k \langle k_R|(\sum_i \sqrt{p_i}|i_A\rangle|i_R\rangle)(\sum_j \sqrt{p_j}\langle j_A|\langle j_R|)|k_R\rangle \\ &= \sum_{i,k,j} \sqrt{p_i p_j} k_R i_R |i_A\rangle\langle j_A| j_R k_R = \sum_k p_k |k_A\rangle\langle k_A| = \rho^A.\end{aligned}$$

□

In questa dimostrazione abbiamo anche mostrato come ottenere una purificazione, tramite l'eq. (3.23). Si può inoltre notare come la purificazione e la decomposizione di Schmidt siano strettamente legate. La procedura di purificazione consiste infatti nel definire uno stato puro la cui base di Schmidt per il sistema A è la base in cui lo stato misto è diagonale, dove i coefficienti di Schmidt sono uguali alle radici quadrate degli autovalori dell'operatore densità che viene purificato.

È inoltre facile vedere che la purificazione non è unica, basta infatti scegliere una base ortonormale diversa per R per avere purificazioni diverse. Si può però facilmente passare da una purificazione all'altra, come mostra il seguente risultato.

Proposizione 3.7. *Siano $|AR_1\rangle$ e $|AR_2\rangle$ due diverse purificazioni di uno stato ridotto ρ^A del sistema composto AR, allora esiste un operatore unitario U_R, agente sul sottosistema R, tale che $|AR_1\rangle = (\mathbf{I}_A \otimes U_R)|AR_2\rangle$.*

Dimostrazione. Per decomposizione ortonormale abbiamo che $\rho^A = \sum_i p_i |i_A\rangle\langle i_A|$. Quindi, usando la decomposizione di Schmidt le due purificazioni $|AR_1\rangle$ e $|AR_2\rangle$ di ρ^A sono date da:

$$|AR_1\rangle = \sum_i \sqrt{p_i}|i_A\rangle|i_{R_1}\rangle, \qquad |AR_2\rangle = \sum_i \sqrt{p_i}|i_A\rangle|i_{R_2}\rangle \tag{3.24}$$

dove $|i_{R_1}\rangle$ e $|i_{R_2}\rangle$ sono basi ortonormali diverse di R. Ci basta quindi definire l'operatore U_R tale che $U_R|i_{R_2}\rangle = |i_{R_1}\rangle$ per dimostrare la tesi. □

3.1.6 Maggiorazione

Introduciamo ora il concetto di maggiorazione, essa è un ordinamento su vettori reali di dimensione d. Utilizzeremo la notazione $x^\downarrow$ per indicare un vettore riordinato con le componenti in ordine decrescente, cioè tale che $x^\downarrow_j \geq x^\downarrow_{j+1}$. Diamo così la definizione di maggiorazione:

Definizione 3.6. *Siano $x, y \in V$, spazio vettoriale reale con $\dim(V) = d$, allora diciamo che x è maggiorato da y, scritto $x \prec y$, se valgono:*

$$\sum_{j=1}^{k} x_j^{\downarrow} \leq \sum_{j=1}^{k} y_j^{\downarrow} \quad per \quad 1 \leq k \leq d-1, \tag{3.25}$$

$$\sum_{j=1}^{d} x_j^{\downarrow} = \sum_{j=1}^{d} y_j^{\downarrow}. \tag{3.26}$$

Verificare questa definizione può però risultare molto complicato, è utile quindi la seguente condizione per la maggiorazione fra due vettori:

Proposizione 3.8. *Siano $x, y \in V$, spazio vettoriale reale con $\dim(V) = d$, allora abbiamo che $x \prec y$ se e solo se valgono:*

$$\sum_{j=1}^{d} \max(x_j - t, 0) \leq \sum_{j=1}^{d} \max(y_j - t, 0) \quad \forall t \in \mathbb{R}, \tag{3.27}$$

$$\sum_{j=1}^{d} x_j = \sum_{j=1}^{d} y_j. \tag{3.28}$$

Dimostrazione. La condizione (3.28) è immediata dalla Definizione 3.6 per $k = d$. Supponiamo $x \prec y$ e fissiamo $t \in \mathbb{R}$, notiamo che:

$$x \prec y \Leftrightarrow \sum_{j=1}^{k} x_j^{\downarrow} \leq \sum_{j=1}^{k} y_j^{\downarrow} \Leftrightarrow \sum_{j=1}^{k} (x_j^{\downarrow} - t) \leq \sum_{j=1}^{k} (y_j^{\downarrow} - t) \tag{3.29}$$

se $t \leq \min_j(x_j, y_j)$ allora la condizione (3.27) è facilmente verificata perché $\max(x_j - t, 0) = x_j - t$ e $\max(y_j - t, 0) = y_j - t$. Anche se $t \geq \max_j(x_j, y_j)$ abbiamo che la condizione è facilmente verificata perché $\max(x_j - t, 0) = 0$ e $\max(y_j - t, 0) = 0$.

Consideriamo ora i valori restanti, cioè $\min_j(x_j, y_j) \leq t \leq \max_j(x_j, y_j)$, in questo caso definiamo $\tilde{x}_j = x_j^{\downarrow} - t$ e $\tilde{y}_j = y_j^{\downarrow} - t$ è quindi vale, come abbiamo visto in eq. (3.29), $\tilde{x} \prec \tilde{y}$. Definiamo anche $\overline{n}_x, \overline{n}_y \in \mathbb{N}$ tali che $\tilde{x}_{\overline{n}_x+1} < 0$ e $\tilde{y}_{\overline{n}_y+1} < 0$ dove, per le condizioni su t, abbiamo che $1 \leq \overline{n}_x \leq d$ e $1 \leq \overline{n}_y \leq d$. Possiamo quindi scrivere:

$$\sum_{j=1}^{k} \tilde{x}_j \leq \sum_{j=1}^{\overline{n}_x} \tilde{x}_j = \sum_{j=1}^{d} \max(x_j - t, 0) \quad \text{per} \quad k = 1, \ldots, d, \tag{3.30}$$

$$\sum_{j=1}^{k} \tilde{y}_j \leq \sum_{j=1}^{\overline{n}_y} \tilde{y}_j = \sum_{j=1}^{d} \max(y_j - t, 0) \quad \text{per} \quad k = 1, \ldots, d. \tag{3.31}$$

Poniamo quindi $k = \overline{n}_x$ e sfruttando $\tilde{x} \prec \tilde{y}$ otteniamo:

$$\sum_{j=1}^{\overline{n}_x} \tilde{x}_j \leq \sum_{j=1}^{\overline{n}_x} \tilde{y}_j \leq \sum_{j=1}^{\overline{n}_y} \tilde{y}_j, \Rightarrow \sum_{j=1}^{d} \max(x_j - t, 0) \leq \sum_{j=1}^{d} \max(y_j - t, 0). \tag{3.32}$$

Per dimostrare l'inversa procediamo in modo analogo. Consideriamo $\min_j(x_j, y_j) \leq t \leq \max_j(x_j, y_j)$ e definiamo $\tilde{x}_j = x_j^{\downarrow} - t$ e $\tilde{y}_j = y_j^{\downarrow} - t$. Definiamo poi $\overline{n}_x, \overline{n}_y \in \mathbb{N}$ tali che $\tilde{x}_{\overline{n}_x+1} < 0$ e $\tilde{y}_{\overline{n}_y+1} < 0$, che, in funzione di t, possono valere $\overline{n}_x = 1, \ldots, d$, $\overline{n}_y = 1, \ldots, d$. Quindi avremo che:

$$\sum_{j=1}^{\overline{n}_y} \tilde{x}_j \leq \sum_{j=1}^{\overline{n}_x} \tilde{x}_j = \sum_{j=1}^{d} \max(x_j - t, 0) \leq \sum_{j=1}^{d} \max(y_j - t, 0) = \sum_{j=1}^{\overline{n}_y} \tilde{y}_j. \tag{3.33}$$

Che dimostra $\tilde{x} \prec \tilde{y}$ e quindi, per eq. (3.29), la tesi.

□

Grazie a questo criterio si può verificare una proprietà importante della maggiorazione:

Proposizione 3.9. *Siano $x, y \in V$, spazio vettoriale reale con $\dim(V) = d$, allora l'insieme degli x tali che $x \prec y$ è convesso.*

Dimostrazione. Ci basta mostrare che, se prendiamo $x, z \in V$ tali che $x \prec y$ e $z \prec y$, abbiamo $(1-t)x + tz \prec y$ per $t \in]0, 1[$. Sfruttiamo ora la Proposizione 3.8 e, per prima cosa, verifichiamo la seconda condizione:

$$\sum_{j=1}^{d}((1-t)x_j + tz_j) = (1-t)\sum_{j=1}^{d} x_j + t\sum_{j=1}^{d} z_j = (1-t)\sum_{j=1}^{d} y_j + t\sum_{j=1}^{d} y_j = \sum_{j=1}^{d} y_j.$$

Vediamo poi che, per ogni $s \in \mathbb{R}$, vale:

$$\sum_{j=1}^{d} \max((1-t)x_j + tz_j - s, 0) \leq \sum_{j=1}^{d} \max((1-t)x_j - (1-t)s, 0) + \sum_{j=1}^{d} \max(tz_j - ts, 0) =$$
$$= (1-t)\sum_{j=1}^{d} \max(x_j - s, 0) + t\sum_{j=1}^{d} \max(z_j - s, 0) \leq \sum_{j=1}^{d} \max(y_j - s, 0).$$

È quindi verificata anche la prima condizione e di conseguenza la tesi.

□

Questi sono solo pochi dei tanti risultati relativi alla teoria della maggiorazioni, ma bastano per evidenziare il legame che ha con le matrici stocastiche e la convertibilità sotto LOCC.

3.2 Risultati preliminari

Mettiamo ora insieme le definizioni e i risultati che abbiamo dato. In particolare vogliamo mostrare il legame tra la teoria della maggiorazione e le matrici stocastiche. Questo primo risultato lega il concetto di maggiorazione alle permutazioni, e ci permette di comprendere meglio il significato della maggiorazione.

Proposizione 3.10. *Siano $x, y \in V$, spazio vettoriale reale con $\dim(V) = d$, allora:*

$$x \prec y \Leftrightarrow x = \sum_j p_j P_j y \tag{3.34}$$

con p_j una qualche distribuzione di probabilità e P_j una qualche matrice di permutazione

Dimostrazione. Supponiamo $x \prec y$. Senza perdita di generalità possiamo supporre che $x = x^{\downarrow}$ e $y = y^{\downarrow}$ e procediamo per induzione su $d = \dim(V)$.

Caso $d = 1$: abbiamo $x \prec y$ che per definizione, con $k = d = 1$, implica $x = y$. È sufficiente quindi prendere $p = 1$ e $P = \mathbb{I}$ e il risultato è verificato.

Caso $d = n + 1$: abbiamo che $x \prec y \Rightarrow x_1 \leq y_1$. Scegliamo quindi m tale che $y_m \leq y_{m-1}$ e definiamo $t \in [0, 1]$ tale che $x_1 = ty_1 + (1 - t)y_m$. Definiamo quindi una combinazione convessa di matrici di permutazione $D \equiv t\mathbb{I} + (1-t)T$, dove T è la matrice di permutazione che scambia tra loro primo e m-esimo elemento. Avremo quindi:

$$Dy = (x_1, y_2, \ldots, y_{m-1}, (1 - t)y_1 + ty_m, y_{m+1}, \ldots, y_{n+1}). \tag{3.35}$$

Definiamo ora $x' \equiv (x_2, \ldots, x_{n+1})$ e $y' = (y_2, \ldots, y_{m-1}, (1 - t)y_1 + ty_m, y_{m+1}, \ldots, y_{n+1})$ e vogliamo mostrare che $x' \prec y'$. Avremo, per come li abbiamo definiti, che $x' = x'^{\downarrow}$ e $y' = y'^{\downarrow}$. Per prima cosa verifichiamo la condizione in eq. (3.25). Consideriamo il caso $k \leq m - 2$. Da $x \prec y$, tenendo conto delle definizioni di x' e y', abbiamo che:

$$\sum_{j=1}^{k} x'_j \leq \sum_{j=1}^{k} y'_j \quad \text{per} \quad 1 \leq k \leq m - 2.$$

Il caso per $m - 1 \leq k \leq n$ è più delicato, ma abbastanza chiaro se si esplicitano le sommatorie. Da $x \prec y$ abbiamo che:

$$x_1 + x_2 + \cdots + x_k \leq y_1 + y_2 + \cdots + y_{m-1} + y_m + y_{m+1} + \cdots + y_k \tag{3.36}$$

e possiamo sfruttare il fatto che $y_1 + y_m - x_1 = (1 - t)y_1 + ty_m = y'_{m-1}$ ottenendo:

$$x_2 + \cdots + x_k \leq y_2 + \cdots + y_{m-1} + (1 - t)y_1 + ty_m + y_{m+1} + \cdots + y_k \tag{3.37}$$

$$\Rightarrow \sum_{j=1}^{k} x'_j \leq \sum_{j_1}^{k} y'_j \quad \text{per} \quad m - 1 \leq k \leq d - 1. \tag{3.38}$$

Il caso per $k = d$ si mostra in modo analogo.

Abbiamo quindi mostrato che $x' \prec y'$ e, essendo il caso per d = n vero per l'ipotesi di induzione, abbiamo che $x' = \sum_{j=1}^{s} p'_j P'_j y'$. Estendendo trivialmente P'_j a n + 1 dimensioni possiamo scrivere:

$$x = \sum_{j=1}^{s} p'_j P'_j D y = \sum_{j=1}^{s} t p'_j P'_j \mathbb{I} y + \sum_{j=1}^{s} (1-t) p'_j P'_j T y \tag{3.39}$$

definiamo quindi:

$$\begin{aligned} p_l &= t p'_l, & P_l &= P'_l, & &\text{per} \quad 1 \le l \le s, \\ p_l &= (1-t) p'_{l-m}, & P_l &= P'_{l-m} T, & &\text{per} \quad m+1 \le l \le 2s, \end{aligned}$$

dove p_l è una distribuzione di probabilità e P_l sono matrici di permutazione perché prodotti di matrici di permutazione, ottenendo quindi $x = \sum_l p_l P_l y$ come volevamo.

Per dimostrare l'inverso supponiamo $x = \sum_j p_j P_j y$. Abbiamo che $P_j y \prec y$ perché la matrice di permutazione scambia l'ordine delle coordinate di y, che è ininfluente per Definizione 3.6. Essendo p_j una distribuzione di probabilità allora $\sum_j p_j P_j y$ è una combinazione convessa e quindi, per Proposizione 3.9, abbiamo $x \prec y$.

□

In altre parole questa proposizione ci dice che $x \prec y$ se e solo se possiamo esprimere x come combinazione convessa di permutazioni y. Intuitivamente x è più disordinata di y nel senso che può essere ottenuta mischiando e sommando gli elementi di y. Questo è uno dei risultati più utili della teoria della maggiorazione.

Abbiamo una combinazione convessa di matrici di permutazione, possiamo sfruttare il Teorema di Birkhoff e riesprimere la proposizione in termini di matrici doppiamente stocastiche:

Proposizione 3.11. *$x \prec y$ se e solo se $x = Dy$ per una qualche matrice doppiamente stocastica D.*

Dimostrazione. Per Proposizione 3.10 $x \prec y \Leftrightarrow x = \sum_j p_j P_j y$. Per dimostrare la proposizione ci basta definire $D = \sum_j p_j P_j$ che sarà, per il Teorema 3.1, doppiamente stocastica. □

Questa forma è utile nell'estendere la Proposizione 3.10 agli operatori hermitiani. Possiamo infatti estendere il concetto di maggiorazione agli operatori se consideriamo il vettore dei loro autovalori.

Definizione 3.7. *Siano A e B due operatori hermitiani, diciamo allora che $A \prec B$ se $\lambda(A) \prec \lambda(B)$ dove $\lambda(A)$ e $\lambda(B)$ sono i vettori degli autovalori di A e B.*

E quindi la Proposizione 3.10 diventa per gli operatori hermitiani:

Teorema 3.12. *Siano A e B due operatori hermitiani, allora $A \prec B$ se e solo se esistono p_j distribuzione di probabilità e U_j insieme di matrici unitarie tali che $A = \sum_j p_j U_j B U_j^\dagger$.*

Dimostrazione. Supponiamo $A \prec B$, allora per definizione $\lambda(A) \prec (B)$ e quindi, per Proposizione 3.10, abbiamo $\lambda(A) = \sum_j p_j P_j \lambda(B)$ con p_j una qualche distribuzione di probabilità e P_j una qualche matrice di permutazione. Sia $\Lambda(A)$ la matrice diagonale con elementi gli autovalori in $\lambda(A)$, allora possiamo scrivere:

$$\Lambda(A) = \sum_j p_j P_j \Lambda(B) P_j^\dagger. \tag{3.40}$$

Ma abbiamo, per il Teorema spettrale, $A = V\lambda(A)V^\dagger$ e $\lambda(B) = WBW^\dagger$, con V e W matrici unitarie. Possiamo perciò scrivere:

$$A = V(\sum_j p_j P_j \Lambda(B) P_j^\dagger)V^\dagger = \sum_j p_j (VP_jW) B (VP_jW)^\dagger. \tag{3.41}$$

Definendo $U_j = VP_jW$ otteniamo $A = \sum_j U_j B U_j^\dagger$.
Per dimostrare l'inversa supponiamo $A = \sum_j U_j B U_j^\dagger$, con ragionamenti analoghi a prima arriviamo a $\Lambda(A) = \sum_j V_j \Lambda(B) V_j^\dagger$, con V_j unitarie. Lavoriamo ora sulle componenti:

$$\lambda_k(A) = \Lambda_{kk}(A) = \sum_{j,l} p_j V_{j,kl} \Lambda_{ll}(B) V_{j,kl}^* = \sum_{j,l} p_j |V_{j,kl}|^2 \lambda_l(B). \tag{3.42}$$

Definiamo la matrice D tale che $D_{kl} = \sum_j p_j |V_{j,kl}|^2$ e quindi abbiamo:

$$\lambda_k(A) = \sum_l D_{kl} \lambda_l(B) \Rightarrow \lambda(A) = D\lambda(B). \tag{3.43}$$

Abbiamo inoltre che $D_{kl} \geq 0$ per $k, l = 1, \ldots, n$ e

$$\sum_k D_{kl} = \sum_{k,j} p_j |V_{j,kl}|^2 = \sum_j p_j (\sum_k |V_{j,kl}|^2) = \sum_j p_j = 1, \tag{3.44}$$

$$\sum_l D_{kl} = \sum_{k,j} p_j |V_{j,kl}|^2 = \sum_j p_j (\sum_l |V_{j,kl}|^2) = \sum_j p_j = 1 \tag{3.45}$$

dove $\sum_k |V_{j,kl}|^2 = 1$ e $\sum_l |V_{j,kl}|^2 = 1$ perché V è unitaria. Quindi D è doppiamente stocastica e, per il corollario 3.11 e l'eq. (3.43), abbiamo $\lambda(A) \prec \lambda(B)$. □

3.3 Semplificazione del protocollo LOCC

Abbiamo ottenuto tutti i risultati sulla maggiorazione necessari per lo studio dell'entanglement bipartito, l'ostacolo più grosso sono ora le trasformazioni LOCC. Come abbiamo visto in precedenza consistono in diversi round dove può essere coinvolto un protocollo di comunicazione classica bidirezionale. Fortunatamente si può dimostrare che esse possono essere semplificate in una trasformazione di un solo round che coinvolge un protocollo di comunicazione classica mono-direzionale.

Proposizione 3.13. *Supponiamo che $|\psi\rangle$ possa essere trasformato in $|\phi\rangle$ da LOCC. Questa trasformazione può essere ottenuta da un protocollo che coinvolge i seguenti step:*

1. *Alice fa una misura singola descritta dall'operatore di misura M_j.*
2. *Manda il risultato a Bob.*
3. *Bob applica un operatore U_j al suo sistema, dipendente dal risultato della misura.*

Dimostrazione. Senza perdita di generalità possiamo supporre che il protocollo LOCC consista in:

1. Alice fa una misura e manda il risultato a Bob.
2. Bob fa una misura, che può dipendere dal risultato di Alice, e manda il risultato ad Alice.
3. Alice fa una misura, che può dipendere dal risultato di Bob, e manda il risultato a Bob.
4. Ecc.. (Si procede fino a che necessario).

Si vuole mostrare che l'effetto di ogni misura che Bob può fare può essere simulato da Alice, quindi le azioni di Bob possono essere rimpiazzate da azioni di Alice. Per vedere ciò immaginiamo che Bob faccia una misura, descritta dall'operatore M_j, sullo stato puro $|\psi\rangle$, che ha decomposizione di Schmidt $|\psi\rangle = \sum_l \sqrt{\lambda_l}|l_A\rangle|l_B\rangle$. Definiamo l'operatore N_j sul sistema di Alice in modo che abbia, come rappresentazione matriciale sulla base $|l_A\rangle$, la stessa che ha M_j sulla base $|l_B\rangle$. Se quindi M_j ha la rappresentazione:

$$M_j = \sum_{k,l} M_{j,kl}|k_B\rangle\langle l_B| \tag{3.46}$$

allora N_j ha rappresentazione:

$$N_j = \sum_{k,l} M_{j,kl}|k_A\rangle\langle l_A|. \tag{3.47}$$

Supponiamo ora che Bob applichi M_j sul proprio sottosistema, lo stato dopo la misura è:

$$|\psi_j\rangle \propto M_j|\psi\rangle = \sum_{k,l,m} M_{j,kl}\sqrt{\lambda_m}|k_B\rangle\langle l_B\,|\,m_B\rangle|m_A\rangle = \sum_{k,l} M_{j,kl}\sqrt{\lambda_l}|k_B\rangle|l_A\rangle \tag{3.48}$$

con probabilità $p_j = \langle\psi|M_j^\dagger M_j|\psi\rangle = \sum_{k,l}\lambda_l|M_{j,kl}|^2$.
Se invece fosse stata Alice a fare la misura N_j sul proprio sottosistema lo stato dopo la misura sarebbe:

$$|\phi_j\rangle \propto N_j|\psi\rangle = \sum_{k,l,m} M_{j,kl}\sqrt{\lambda_m}|k_A\rangle\langle l_A\,|\,m_A\rangle|m_B\rangle = \sum_{k,l} M_{j,kl}\sqrt{\lambda_l}|k_A\rangle|l_B\rangle \tag{3.49}$$

con probabilità $p_j = \langle\psi|N_j^\dagger N_j|\psi\rangle = \sum_{k,l}\lambda_l|M_{j,kl}|^2$.
I due stati $|\psi_j\rangle$ e $|\phi_j\rangle$ sono quindi lo stesso stato a meno di scambiare il sistema di Alice con quello di Bob tramite la mappa $|k_A\rangle \leftrightarrow |k_B\rangle$. Hanno quindi le stesse componenti di Schmidt. Segue quindi dalla Proposizione 3.5 che esistono U_j, matrici unitarie sul sistema di Alice, e V_j, matrici unitarie sul sistema di Bob, tali che $|\psi_j\rangle = (U_j \otimes V_j)|\phi_j\rangle$. Quindi Bob che fa una misura con M_j equivale ad Alice che fa una misura con $U_j M_j$ seguita da Bob che fa l'operazione V_j. Tutte le misure di Bob quindi possono essere sostituite da misure di Alice, e visto che, per la Proposizione 1.2, ogni sequenza di misure equivale a una misura singola, abbiamo ristretto il protocollo LOCC come nella tesi. □

3.4 Teorema di Nielsen

Possiamo ora enunciare e dimostrare il Teorema di Nielsen, che evidenzia lo stretto legame fra entanglement bipartito e maggiorazione. Per fare ciò definiamo prima $\rho_\psi \equiv \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$ e $\rho_\phi \equiv \mathrm{Tr}_B(|\phi\rangle\langle\phi|)$, che sono le matrici ridotte del sistema di Alice, indicheremo allora con λ_ψ e λ_ϕ gli autovalori delle due matrici. In questo modo la formulazione del Teorema è:

Teorema 3.14. ***(Teorema di Nielsen)*** *Uno stato puro bipartito $|\psi\rangle$ può essere trasformato in un altro stato puro $|\phi\rangle$ da LOCC se e solo se $\lambda_\psi \prec \lambda_\phi$.*

Dimostrazione. Supponiamo che $|\psi\rangle \to |\phi\rangle$ sia possibile con certezza via LOCC. Da Proposizione 3.13 possiamo assumere che consista in: Alice fa una misura con l'operatore M_j e manda il risultato a Bob che applica l'operatore U_j, che può dipendere dal risultato della misura. Quindi dal punto di vista di Alice abbiamo che inizia con lo stato ρ_ψ e finisce con lo stato ρ_ϕ indipendentemente dal risultato della misura, quindi dobbiamo avere:

$$M_j\rho_\psi M_j^\dagger = p_j\rho_\phi \quad \text{con} \quad p_j = \langle\psi|M_j^\dagger M_j|\psi\rangle. \tag{3.50}$$

Facciamo ora la decomposizione polare di $M_j\sqrt{\rho_\phi}$:

$$M_j\sqrt{\rho_\psi} = \sqrt{M_j\sqrt{\rho_\psi}(M_j\sqrt{\rho_\psi}^\dagger)}V_j = \sqrt{M_j\sqrt{\rho_\psi}M_j^\dagger}V_j = \sqrt{p_j\rho_\phi}V_j \tag{3.51}$$

dove V_j è una operazione unitaria. Moltiplichiamo ora a sinistra per il suo aggiunto:

$$(M_j\sqrt{\rho_\psi})^\dagger(M_j\sqrt{\rho_\psi}) = \sqrt{\rho_\psi}M_j^\dagger M_j\sqrt{\rho_\psi} = p_j V_j^\dagger\rho_\phi V_j. \tag{3.52}$$

Sommiamo su tutti i j:

$$\sum_j \sqrt{\rho_\psi}M_j^\dagger M_j\sqrt{\rho_\psi} = \sqrt{\rho_\psi}(\sum_j M_j^\dagger M_j)\sqrt{\rho_\psi} = \rho_\psi = \sum_j p_j V_j^\dagger\rho_\phi V_j \tag{3.53}$$

dove abbiamo sfruttato la proprietà delle misure $\sum_j M_j^\dagger M_j = \mathbf{I}$. Quindi per il Teorema 3.12 abbiamo $\rho_\psi \prec \rho_\phi$ che implica per definizione $\lambda_\psi \prec \lambda_\phi$.

Per provare l'inversa supponiamo $\lambda_\psi \prec \lambda_\phi$, per Teorema 3.12 esiste una qualche distribuzione di probabilità p_j e matrici U_j unitarie tali che:

$$\rho_\psi = \sum_j p_j U_j^\dagger\rho_\psi U_j. \tag{3.54}$$

Supponiamo ora che ρ_ψ sia invertibile (il caso non invertibile è fatto dopo), e definiamo l'operatore M_j tale che:

$$M_j\sqrt{\rho_\psi} \equiv \sqrt{p_j\rho_\phi}U_j^\dagger. \tag{3.55}$$

Abbiamo quindi che:

$$\sum_j M_j^\dagger M_j = \rho_\psi^{-\frac{1}{2}}(\sum_j p_j U_j\rho_\phi U_j^\dagger)\rho_\psi^{-\frac{1}{2}} = \rho_\psi^{-\frac{1}{2}}\rho_\psi\rho_\psi^{-\frac{1}{2}} = \mathbb{I}. \tag{3.56}$$

Quindi gli M_j formano una famiglia di operatori di misura.

Supponiamo ora che ρ_ψ non sia invertibile, avremo allora che il $\ker(\rho_\psi)$ non è più banale. Per prima cosa vediamo che:

$$|v\rangle \in \ker(\rho_\psi) \Rightarrow \langle w|\rho_\psi|v\rangle = \sum_j p_j\langle w|U_j\rho_\phi U_j^\dagger|v\rangle = 0 \quad \forall|w\rangle \tag{3.57}$$

$$\Rightarrow U_j\rho_\phi U_j^\dagger|v\rangle = 0 \Rightarrow |v\rangle \in \ker(U_j\rho_\phi U_j^\dagger) \tag{3.58}$$

dove abbiamo sfruttato la non negatività dei p_j. Notiamo inoltre che, sempre per $|v\rangle \in \ker(\rho_\psi)$:

$$\langle v|U_j\rho_\phi U_j^\dagger|v\rangle = (\sqrt{\rho_\phi}U_j^\dagger|v\rangle)^\dagger(\sqrt{\rho_\phi}U_j^\dagger|v\rangle) = |\sqrt{\rho_\phi}U_j^\dagger|v\rangle|^2 = 0 \tag{3.59}$$

$$\Rightarrow |v\rangle \in \ker(\sqrt{\rho_\phi}U_j^\dagger). \tag{3.60}$$

Sappiamo inoltre che lo spazio di Hilbert può essere scritto come $\mathcal{H} = \ker(\rho_\psi) \oplus \text{supp}(\rho_\psi)$ Prendiamo poi $\{|v_1\rangle, \ldots, |v_m\rangle\}$ e $\{|w_1\rangle, \ldots, |w_s\rangle\}$, basi ortonormali rispettivamente di $\ker(\rho_\psi)$ e di $\text{supp}(\rho_\psi)$, allora avremo che $\{|v_1\rangle, \ldots, |v_m\rangle, |w_1\rangle, \ldots, |w_s\rangle\}$ è base di $\mathcal{H}$ e quindi la rappresentazione matriciale a blocchi di $\sqrt{\rho_\psi}$ sarà:

$$\sqrt{\rho_\psi} = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & A \end{array}\right), \qquad \text{con } A : \text{supp}(\rho_\psi) \to \text{supp}(\rho_\psi). \tag{3.61}$$

Come visto prima, $\ker(\rho_\psi) \subseteq \ker(\sqrt{\rho_\phi} U_j^\dagger)$ e quindi la rappresentazione matriciale di $\sqrt{\rho_\phi} U_j^\dagger$ deve essere:

$$\sqrt{\rho_\phi} U_j^\dagger = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & B \end{array}\right), \qquad \text{con } B : \text{supp}(\rho_\psi) \to \text{supp}(\rho_\psi). \tag{3.62}$$

Abbiamo poi che A è invertibile, possiamo quindi definire l'operatore M'_j come in eq. (3.55):

$$M'_j A \sqrt{p_j} B, \qquad \text{con } M'_j : \text{supp}(\rho_\psi) \to \text{supp}(\rho_\psi) \tag{3.63}$$

e, come visto prima, abbiamo che $\sum_j M'^\dagger_j M'_j = \mathbb{I}$. Se ora definiamo M_j come:

$$M_j = \left(\begin{array}{c|c} \sqrt{p_j}\,\mathbb{I} & 0 \\ \hline 0 & M'_j \end{array}\right) \tag{3.64}$$

allora soddisfa eq. (3.55), essendo $\ker(\rho_p si) \subseteq \ker(\sqrt{p_j} U_j^\dagger)$, e:

$$\sum_j M_j^\dagger M_j = \sum_j \left(\begin{array}{c|c} p_j \mathbb{I} & 0 \\ \hline 0 & M'^\dagger_j M'_j \end{array}\right) = \left(\begin{array}{c|c} \mathbb{I} & 0 \\ \hline 0 & \mathbb{I} \end{array}\right) = \mathbb{I}. \tag{3.65}$$

Quindi è anch'essa una famiglia di operatori di misura.

Supponiamo ora che Alice faccia la misura M_j ottenendo il risultato j e lo stato corrispondente $|\psi_j\rangle \propto M_j|\psi\rangle$. Sia ρ_j la matrice ridotta di Alice corrispondente a $|\psi_j\rangle$ abbiamo:

$$\rho_j \propto M_j \rho_\psi M_j^\dagger = M_j \sqrt{\rho_\psi}\sqrt{\rho_\psi} M_j^\dagger = p_j \sqrt{\rho_\phi} U_j^\dagger U_j \sqrt{\rho_\phi} = p_j \rho_\phi. \tag{3.66}$$

Rinormalizzando si ottiene $\rho_j = \rho_\phi$. Quindi da Proposizione 3.7 Bob può convertire $|\psi_j\rangle$ in $|\phi\rangle$ tramite una certa trasformazione unitaria V_j

□

3.4.1 Esempio con due qubit

Un esempio semplice dove si può applicare il Teorema è quello in cui consideriamo solo due qubit. Supponiamo che Alice e Bob condividano una coppia di qubit nello stato $|\psi\rangle$, abbiamo allora due possibili forme della decomposizione di Schmidt:

1. se è separabile abbiamo$|\psi\rangle = |1_A\rangle|1_B\rangle$,
2. se è entangled abbiamo $|\psi\rangle = \sqrt{\lambda_1}|1_A\rangle|1_B\rangle + \sqrt{\lambda_2}|2_A\rangle|2_B\rangle$, con $\lambda_1 + \lambda_2 = 1$.

Dove in entrambi i casi le basi $|i_A\rangle$ e $|i_B\rangle$ sono le rispettive basi di Schmidt. Il vettore degli autovalori è quindi molto semplice, avendo la forma $\lambda = (\lambda_1, \lambda_2)$, dove assumo, senza perdità di generalità, $\lambda_1 \geq \lambda_2$. È quindi evidente che ogni stato entangled può essere trasformato in uno stato separato tramite LOCC, ma ciò non ci stupisce, avendoli definiti in questo modo quando abbiamo trattato la teoria delle risorse.

Decisamente più interessante è il fatto che, tramite il Teorema di Nielsen, possiamo individuare una preordine totale su tutti gli stati, così da confrontare quale stato sia più o meno entangled. È immediato, dalla definizione di maggiorazione, vedere che $(\frac{1}{2}, \frac{1}{2})$ è maggiorato da tutti gli altri possibili vettori di autovalori, gli stati individuati da questo vettore potranno quindi essere trasformati in un qualsiasi altro tramite LOCC, sono perciò gli stati massimamente entangled, e coincidono proprio con gli stati di Bell. Notiamo inoltre che $(1-a, a) \prec (1-b, b)$ per $\frac{1}{2} \geq a \geq b \geq 0$, cioè più ci si allontana da $(\frac{1}{2}, \frac{1}{2})$(stati massimamente entangled) avvicinandosi a $(1, 0)$(stati separabili), più diminuisce l'entanglement, fino ad arrivare agli stati separabili.

3.4.2 Stati incomparabili

Il caso che abbiamo appena visto con 2 qubit è però fuorviante, in esso siamo infatti riusciti a definire un preordine totale, cioè presi due stati qualsiasi allora è sempre possibile compararli. Ciò non è però possibile in generale, per esempio se consideriamo in $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^3$ i due stati:

$$|\psi\rangle = \sqrt{\frac{1}{2}}|11\rangle + \sqrt{\frac{2}{5}}|22\rangle + \sqrt{\frac{1}{10}}|33\rangle, \tag{3.67}$$

$$|\phi\rangle = \sqrt{\frac{3}{5}}|11\rangle + \sqrt{\frac{1}{5}}|22\rangle + \sqrt{\frac{1}{5}}|33\rangle. \tag{3.68}$$

Abbiamo che nè $|\psi\rangle \to |\phi\rangle$ nè $|\phi\rangle \to |\psi\rangle$ sono possibili, non possiamo quindi confrontare l'entanglement dei due stati, in questo caso si dice che essi sono *incomparabili*. Si può quindi pensare che essi rappresentino due diversi tipi di entanglement. Più però aumenta $N = \min(\dim A, \dim B)$, cioè più aumenta il numero dei coefficienti di Schmidt, più aumenta il numero di tipi di entanglement diversi. Nel limite per N grande quasi tutte le coppie di stati puri $|\psi\rangle$ e $|\phi\rangle$ saranno incomparabili. Si sono quindi sviluppate altre classi di operazioni libere più potenti di LOCC.

3.4.3 Quantificare l'entanglement bipartito

Ci chiediamo ora se sia possibile quantificare l'entanglement di uno stato puro bipartito sfruttando il Teorema d Nielsen. La risposta a questa domanda è positiva, è infatti possibile in due modi, che danno lo stesso risultato.

Supponiamo di voler quantificare l'entanglement dello stato $|\psi\rangle$ condiviso da Alice e Bob. L'idea è quella di associare l'entanglement allo stato $|\psi\rangle$ come associamo la massa a un oggetto. Se per bilanciare una bilancia a due bracci, dove in un braccio abbiamo una massa di 1kg, dobbiamo mettere nell'altro braccio 25 palline, allora ogni pallina deve avere massa (1/25)kg. Se invece ogni pallina ha massa (1/25.3)kg allora dobbiamo bilanciare 10 masse da una parte e 253 palline dall'altra. Cioè, se n masse vengono bilanciate da m palline allora la massa delle palline è (n/m) per $n, m \to \infty$.

Se quindi prendiamo come unità per misurare l'entanglement lo stato di bell $(|00\rangle + |11\rangle)/\left(\sqrt{2}\right)$ abbiamo due tipi di trasformazioni che possono essere usate per quantificare l'entanglement.

- *Distillazione di entanglement*: Alice e Bob convertono m copie di uno stato puro $|\psi\rangle$ in n copie dello stato di Bell $(|00\rangle + |11\rangle)/\left(\sqrt{2}\right)$ tramite LOCC.
- *Diluizione di Entanglement*: Alice e Bob convertono n copie dello stato di Bell $(|00\rangle + |11\rangle)/\left(\sqrt{2}\right)$ in m copie dello stato puro $|\psi\rangle$.

Dove in entrambi i casi si richiede non che le trasformazioni avvengano con esattezza, ma con alta fedeltà. La fedeltà è una distanza tra due stati definita come $F(\rho, \phi) \equiv \mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)$. Essa misura quindi quanto siano "vicini" due stati, in particolare $F(\rho, \sigma) = 1 \Leftrightarrow \rho = \sigma$. Quindi con alta fedeltà intendiamo che la fedeltà tra lo stato che otteniamo con LOCC e quello che volevamo ottenere deve tendere a 1 per $m \to \infty$.
Chiameremo il rapporto $E_D = n/m$ per $n, m \to \infty$ *entanglement distillabile* nel primo caso, ed *entanglement di formazione* E_F nel secondo. Non è affatto ovvio che le due definizioni diano lo stesso numero, si può però dimostrare che per stati puri lo danno. Il risultato più importante è che l'entanglement di formazione(o l'entanglement distillabile) E_F di $|\psi\rangle$ è uguale a $S(\rho_\psi)$, cioè all'entropia di Von Neumann dello stato ridotto per un suo sottosistema. Ricordiamo che l'entropia di Von Neumann per uno stato ρ è definita come $S(\rho) = -\mathrm{Tr}\left(\rho \log(\rho)\right)$. Possiamo quindi definire l'ammontare dell'entanglement per sistemi puri bipartiti come $E_F = S(\rho_\psi)$.

Questo genere di trasformazioni appena utilizzate, dove viene richiesto di ottenere stati con altà fedeltà e non con esattezza, sono chiamate trasformazioni asintotiche. Il loro utilizzo è fisicamente giustificato dal fatto che, se per esempio consideriamo i seguenti coefficienti di Schmidt:

$$\mathrm{I}: (0.5, 0.49, 0.01), \quad \mathrm{II}: \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right), \quad \mathrm{III}: (0.5, 0.5, 0).$$

Abbiamo che per trasformazioni esatte I e II sono comparabili, mentre III è incomparabile ad entrambe, anche se è evidente che I e III abbiano molto più in comune fra di loro che con II. Per ignorare quindi le piccole differenze fra gli stati si devono usare limiti asintotici. Inoltre abbiamo che le trasformazioni asintotiche sono tutte invertibili, ed è per questo che $E_D = E_F$.

Capitolo 4

Generalizzazione e domande aperte

Il metodo per quantificare l'entanglement di uno stato puro bipartito che abbiamo appena visto non è pienamente soddisfacente, poiché necessità di un numero infinito di copie degli stati, condizione impossibile nelle situazioni reali. Vogliamo quindi trovare un modo per quantificare l'entanglement nel caso di un numero finito di copie. Un primo risultato fu trovato da Guifré Vidal nel 1999 [20].

4.1 Entanglement monotone

Le misure E_D e E_F sono state costruite per descrivere l'entanglement in termini di qualche operazione. Quindi vengono fuori dall'ottimizzazione di qualche protocollo che agisce sullo stato. Possiamo però anche usare un punto di vista assiomatico per permettere a ogni funzione, che soddisfi certi postulati, di essere una misura per l'entanglement. È lo stesso già visto in precedenza nella sezione 2.5. Chiamiamo quindi come *entanglement monotone* una funzione E monotona sotto LOCC, che quindi soddisfa:

$$E\left(\Lambda(\rho)\right) \leq E(\rho) \tag{4.1}$$

dove Λ è una trasformazione LOCC. Questa condizione è stata individuata da Vidal [19] come l'unica necessaria per una misura dell'entanglement. Gli stati separabili sono convertibili l'uno con l'altro sotto LOCC. Quindi, in analogia con quanto fatto con le funzione monotone, poniamo $E(\sigma) = 0$ per ogni stato separabile σ.

Solitamente le misure dell'entanglement soddisfano anche una condizione più forte, quella che E non aumenti in media, cioè:

$$\sum_i p_i E(\sigma_i) \leq E(\rho) \tag{4.2}$$

dove $\{p_i, \sigma_i\}$ è l'ensemble ottenuto da ρ tramite operazioni LOCC. Questa condizione non è necessaria, ma spesso più semplice da provare.

4.2 Probabilità di transizione come misura dell'entanglement bipartito

La domanda che si pose Vidal nel suo articolo fu: supponiamo che Alice e Bob condividano lo stato puro $|\psi\rangle$ e vogliono convertirlo in un altro stato puro $|\phi\rangle$, qual è la massima probabilità di successo se si possono usare solo trasformazioni LOCC?

Alice e Bob possono compiere operazioni unitarie locali, ci interessano quindi solo i coefficienti di Schmidt. Avremo le due decomposizioni:

$$|\psi\rangle = \sum_i \sqrt{\alpha_i}|i_A\rangle|i_B\rangle \qquad \text{dove } \alpha_i \geq \alpha_{i+1} \geq 0, \quad \sum_i \alpha_i = 1, \tag{4.3}$$

$$|\phi\rangle = \sum_i \sqrt{\beta_i}|i_A\rangle|i_B\rangle \qquad \text{dove } \beta_i \geq \beta_{i+1} \geq 0, \quad \sum_i \beta_i = 1. \tag{4.4}$$

Definiamo quindi sull'insieme degli stati puri una famiglia di entanglement monotone $E_k(\rho)$ con $k = 1, 2, \ldots, n$ come:

$$E_k(|\psi\rangle) = \sum_{i=k}^{n} \alpha_i. \tag{4.5}$$

Da cui si può mostrare che la probabilità massima di transizione $P(|\psi\rangle \to |\phi\rangle)$ vale:

$$P(|\psi\rangle \to |\phi\rangle) = \min_{l\in[1,n]} \frac{E_l(|\psi\rangle)}{E_l(|\phi\rangle} = \min_{l\in[1,n]} \frac{\sum_{i=l}^{n} \alpha_i}{\sum_{i=l}^{n} \beta_i}. \tag{4.6}$$

Possiamo vedere questo risultato come una prima generalizzazione del Teorema di Nielsen, dove studiamo anche i casi in cui la conversione dello stato non avviene con certezza.

In analogia con quello che abbiamo fatto con Nielsen può venire l'idea di costruire una relazione d'ordine parziale partendo da questo risultato, si potrebbe essere tentati di porre come criterio che lo stato $|\psi_1\rangle$ è più entangled dello stato $|\psi_2\rangle$ se e solo se $P(|\psi_1\rangle \to |\psi_2\rangle) > P(|\psi_2\rangle \to |\psi_1\rangle)$, ma essa è mal definita. Infatti se consideriamo i tre stati $|\psi_k\rangle \in \mathbb{C}^4 \otimes \mathbb{C}^4$, con $\vec{\alpha}_k$ il vettore del quadrato dei coefficienti di Schmidt dove:

$$\vec{\alpha}_1 \equiv \frac{1}{130}(100, 10, 10, 10),$$
$$\vec{\alpha}_2 \equiv \frac{1}{130}(60, 60, 5, 5),$$
$$\vec{\alpha}_3 \equiv \frac{1}{130}(43, 43, 43, 1).$$

Tale relazione d'ordine porta alla seguente contraddizione: $\psi_1 < \psi_2 < \psi_3 < \psi_1$.

Traiamo ora le conclusioni riguardanti la quantificazione dell'entanglement. Esse ci interessano particolarmente perché non è ancora chiaro, con le tecnologie attuali,

come fare certe trasformazioni locali nello spazio di un gran numero di copie, elemento necessario per le trasformazioni asintotiche. Ma anche se quest'ultime fossero facilmente implementabili, lo scenario finito rimane comunque importante per trarre conclusioni per il caso di un numero finito di copie di uno stato puro. Dall'eq (4.6) possiamo ricavare i seguenti fatti qualitativi:

- La conversione locale ottimale tra due stati con coefficienti di Schmidt diversi è sempre un processo irreversibile. Cioè non si può convertire localmente con certezza uno stato in un altro, e poi riottenere lo stato iniziale. Questo risultato non vale però nel caso di trasformazioni asintotiche.

- La quantificazione dell'entanglement richiede più di una misura. Per gli stati puri in $\mathcal{H} = \mathbb{C}^n \otimes \mathbb{C}$ gli $n-1$ entanglement monotone $E_k(k = 2, \ldots, n)$ definiti in (4.5), sono una famiglia minima di parametri che descrivono in modo dettagliato e immediato le loro risorse non locali. Possono essere considerate come le misure dell'entanglement.

- Le risorse non locali dell'entanglement non sono additive in generale, cioè spesso si possono estrarre più informazioni da una coppia dello stesso stato $|\psi\rangle \otimes |\psi\rangle$ che due volte quella che possono estrarre dallo stato singolo $|\psi\rangle$, per esempio se considero:

  $$|\psi\rangle = \frac{1}{\sqrt{2}}(|11\rangle + |22\rangle) \quad \text{e} \quad |\phi\rangle = \frac{1}{\sqrt{3}}(|11\rangle + |22\rangle + |33\rangle)$$

  abbiamo che $1 = P(|\psi\rangle \otimes |\psi\rangle \to |\phi\rangle) > 2P(|\psi\rangle \to |\phi\rangle) = 0$.
  L'additività è quindi una condizione artificiale per ottenere una buona misura dell'entanglement. Nel caso asintotico l'additività è quindi una proprietà interessante, che viene dall'additività dell'entropia e dalla reversibilità delle trasformazioni.

4.3 Classi di equivalenza dell'entanglement

Come visto in precedenza nel caso bipartito possiamo distinguere diversi tipi di entanglement fra stati puri in base alla convertibilità tramite LOCC. Abbiamo però visto che, eccetto che nel caso con due qubit, molti stati sono tra loro incomparabili. Si può imporre una condizione ancora più stringente, l'interconvertibilità tramite LOCC, possiamo cioè definire una classe di equivalenza, dove due stati sono equivalenti se $|\psi\rangle \leftrightarrow |\phi\rangle$ tramite LOCC. Questa definizione è molto comoda perché nella teoria dell'informazione quantistica possiamo usare indistintamente gli stati appartenenti alla stessa classe per svolgere un compito. Ma dal Teorema 3.14 ciò è possibile solo se i due stati hanno gli stessi coefficienti di Schmidt. Esistono quindi un'infinità non numerabile di queste classi di equivalenza nel caso bipartito. Questa classificazione non risulta quindi molto utile.

Una classificazione più semplice, ma molto più utile, venne data da Dür, Vidal e Cirac [9]. Essi studiarono il caso bipartito, sfruttando il risultato di Vidal precedentemente discusso. Il caso tripartito è un problema di più difficile risoluzione, ma fu risolto, sempre nello stesso articolo, nel caso con tre qubit. Riportiamo quì di seguito quello che hanno trovato.

4.3.1 SLOCC

Una classificazione semplice si può fare con le *stochastic local operation and classical communication*, dette SLOCC, cioè tramite LOCC ma senza imporre che avvenga con certezza, solo con una probabilità non nulla. Possiamo così stabilire una relazione di equivalenza dove due stati $|\psi\rangle$ e $|\phi\rangle$ sono equivalenti se sono convertibili l'uno con l'altro tramite SLOCC. Questa equivalenza significa che i due stati possono implementare lo stesso compito, seppur con diverse probabilità di successo.

Questa classificazione rimarrebbe però inutile se non fossimo in grado di sapere quali stati sono in relazione fra loro tramite SLOCC. Come visto in precedenza è difficile capire quando una qualunque trasformazione è implementabile tramite LOCC. Ricordiamo che una qualunque trasformazione LOCC Λ deve avere la forma riportata in eq. (2.5), ma per la SLOCC ci interessa solo una parte di questa sommatoria. Se infatti supponiamo che $|\psi\rangle$ possa essere convertito in $|\phi\rangle$ tramite SLOCC, allora almeno uno dei termini della sommatoria in eq. (2.5) deve fare la conversione. Per esempio nel caso con tre qubit avremo che se $|\phi\rangle \to |\phi\rangle$ tramite SLOCC allora esistono tre operatori locali A, B, C tali che:

$$|\phi\rangle = (A \otimes B \otimes C)\,|\psi\rangle. \tag{4.7}$$

Si può inoltre dimostrare che questi operatori devono essere invertibili, questo tipo di operatore $A \otimes B \otimes C$ è chiamato ILO("invertible local operator"). Ovviamente anche l'inversa è valida, se cioè è possibile la conversione $|\psi\rangle \to |\phi\rangle$ tramite ILO, allora lo è anche tramite SLOCC. Riassumendo:

Proposizione 4.1. *Gli stati $|\psi\rangle$ e $|\phi\rangle$ sono equivalenti tramite SLOCC se e solo se esiste un operatore V ILO tale che:*

$$|\phi\rangle = V|\psi\rangle. \tag{4.8}$$

Possiamo sfruttare i risultati precedentemente studiati ottenuti da Vidal [20] per analizzare il caso bipartito. Dall'eq. (4.6) vediamo che:

$$P(|\psi\rangle \to |\phi\rangle) = 0 \quad \text{se } n_\psi < n_\phi, \tag{4.9}$$
$$P(|\psi\rangle \to |\phi\rangle) > 0 \quad \text{se } n_\psi \geq n_\phi, \tag{4.10}$$

da cui segue che due stati puri bipartiti appartengono alla stessa classe di equivalenza se e solo se $n_\psi = n_\phi$. In tutti gli altri casi si avrebbe una tra le due probabilità, $P(|\psi\rangle \to |\phi\rangle)$ e $P(|\phi\rangle \to |\psi\rangle)$, uguale a zero. Quindi se si ha $\mathcal{H} = \mathbb{C}^n \otimes \mathbb{C}^m$ con $n \leq m$, avremo n classi di equivalenza. Si può anche definire una relazione d'ordine fra classi, da (4.10) si deduce che l'operazione SLOCC è possibile solo se il numero di Schmitd o rimane lo stesso, o diminuisce. Quindi maggiore è il numero di Schmidt della classe, maggiore l'entanglement, infatti per $n_\psi = 1$ si hanno gli stati separabili.

4.3.2 Entanglement con tre qubit

Per ora si è studiato in dettaglio solo il caso di entanglement bipartito. L'entanglement multipartito è molto più complesso da analizzare, non possiamo infatti fare la decomposizione di Schmidt per stati tripartiti e oltre. Questo limita molto le nostre capacità di studiarlo. Studiamo ora l'entanglement degli stati puri in un sistema con tre qubit, dove incontreremo il più semplice caso di entanglement tripartito.

Abbiamo come spazio di Hilbert $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$, dove chiamiamo i tre sistemi di ogni qubit come A, B, C. Di particolare interesse sono i ranghi $r(\rho^A), r(\rho^B), r(\rho^C)$ delle matrici ridotte, e il range $R(\rho^{BC})$ di ρ^{BC}, che sono i principali strumenti matematici che sfrutteremo per classificare i vari tipi di entanglement.

Analizziamo ora i possibili casi:

Stati separabili ed entanglement bipartito

Partiamo prima con una semplice osservazione, se il rango di una delle matrici ridotte $r(\rho^A), r(\rho^B)$ o $r(\rho^C)$ è uno, allora è possibile riscrivere lo stato puro dei tre qubit come prodotto di due stati puri. Basta ricordarsi che il rango della matrice ridotta è uguale al suo numero di Schmidt. Quindi il qubit, che ha rango della sua matrice ridotta uguale a uno, è non correlato agli altri. Possiamo quindi individuare quattro classi possibili:

- **Classe A-B-C**: si ha quando $r(\rho^A) = r(\rho^B) = r(\rho^C) = 1$. È il caso degli stati separabili, applicando appropriate operazioni locali unitarie si può sempre arrivare allo stato:

$$|\psi_{A-B-C}\rangle = |0\rangle|0\rangle|0\rangle. \tag{4.11}$$

- **Classi A-BC, AB-C e C-AB**: sono le tre classi che contengono entanglement bipartito. Si hanno quando solo uno dei ranghi delle matrici ridotte del sistema è uguale a uno. Per esempio se abbiamo $r(\rho^B) = r(\rho^C) = 2$ e $r(\rho^A) = 1$ allora lo stato appartiene alla classe A-BC, e tramite delle operazioni unitarie locali si può arrivare allo stato:

$$|\psi_{A-BC}\rangle = |0\rangle \left(\cos\theta|0\rangle|0\rangle + \sin\theta|1\rangle|1\rangle\right). \tag{4.12}$$

Scegliamo come rappresentativo di questa classe lo stato massimamente entangled $|0\rangle\left(|0\rangle|0\rangle+|1\rangle|1\rangle\right)/\sqrt{2}$, possiamo infatti ottenere da esso tramite LOCC, cioè con certezza, tutti gli altri stati.

Queste classi non sono equivalenti fra di loro tramite SLOCC perché le trasformazioni ILO mantengono i ranghi delle matrici ridotte invariati [9].

Entanglement tripartito

Studiamo ora il caso con $r(\rho^A) = r(\rho^B) = r(\rho^C) = 2$. Notiamo che c'è una stretta correlazione fra la convertibilità tramite SLOCC e il modo in cui gli stati entangled possano essere espressi come combinazione lineare minima di stati prodotto. Infatti il numero di stati prodotto della decomposizione rimane invariato sotto SLOCC, per esempio se applichiamo una generica operazione ILO al seguente stato:

$$(A\otimes B\otimes C)\left(\frac{|000\rangle+|111\rangle}{\sqrt{2}}\right)=\frac{|A_0\rangle|B_0\rangle|C_0\rangle+|A_1\rangle|B_1\rangle|C_1\rangle}{\sqrt{2}} \tag{4.13}$$

abbiamo che, dall'invertibilità dell'operatore A, $|A_0\rangle$ e $|A_1\rangle$ devono essere linearmente indipendenti (ragionamento analogo per B e C). Viene quindi conservato il numero di termini nella decomposizione minima. Ciò ci permette di dire che esistono almeno due classi di entanglement tripartito, rappresentate dai seguenti stati:

$$|GHZ\rangle=\frac{|000\rangle+|111\rangle}{\sqrt{2}},\qquad |W\rangle=\frac{|100\rangle+|010\rangle+|001\rangle}{\sqrt{3}}.$$

Un modo per capire se uno stato appartiene alla classe GHZ o alla classe W è tramite lo studio del range di ρ^{BC}, $R(\rho^{BC})$. Per vedere ciò serve il seguente risultato:

Proposizione 4.2. *Sia $\sum_{i=1}^{l}|e_i\rangle|f_i\rangle$ una decomposizione dello stato $|\eta\rangle\in\mathcal{H}^E\otimes\mathcal{H}^F$, allora gli stati $\{e_i\}_{i=1}^{l}$ generano il range di $\rho^E\equiv Tr_E|\eta\rangle\langle\eta|$.*

Dimostrazione. Da una parte abbiamo che:

$$\rho^E=\sum_{i,j=1}^{l}\langle f_i\,|\,f_j\rangle|e_j\rangle\langle e_i|.$$

Dall'altra parte abbiamo che per definizione $|\nu\rangle\in R(\rho^E)$ se e solo se esiste $|\mu\rangle$ tale che: $|\nu\rangle=\rho^E|\mu\rangle$, e quindi

$$|\nu\rangle=\sum_{i,j=1}^{l}\langle f_i\,|\,f_j\rangle\langle e_i\,|\,\mu\rangle|e_j\rangle.$$

□

Abbiamo che $r(\rho^A) = 2$ quindi sono necessari almeno due termini prodotto per espandere $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$, se no sarebbe separabile. Se supponiamo che sia possibile una decomposizione a due termini, della forma:

$$|\psi\rangle = |a_1\rangle|b_1\rangle|c_1\rangle + |a_2\rangle|b_2\rangle|c_2\rangle \tag{4.14}$$

allora per la Proposizione 4.2 abbiamo che $|b_1\rangle|c_1\rangle$ e $|b_2\rangle|c_2\rangle$ generano il range di ρ^{BC}. Sappiamo inoltre che $R(\rho^{BC})$ è un sottospazio bidimensionale di $\mathcal{C}^2 \otimes \mathcal{C}^2$ e quindi contiene o solo uno o solo due stati prodotto [9]. Abbiamo quindi mostrato che, per uno stato della classe GHZ, $R(\rho^{BC})$ contiene due stati prodotto. Per il caso dove $R(\rho^{BC})$ contiene solo uno stato prodotto non possiamo scrivere lo stato nella forma (4.14), ma lo possiamo scrivere come:

$$|\psi\rangle = |a_1\rangle|b_1\rangle|c_1\rangle + |a_2\rangle|\phi_{BC}\rangle \tag{4.15}$$

e, tramite operazioni locali unitarie, si può mostrare che appartiene alla classe W [9].

Ordine fra classi

Vogliamo ora studiare le relazioni gerarchiche tra le sei classi, per fare ciò studiamo se esistono operatori locali non invertibili che trasformano uno stato di una classe in un'altra. Considero quindi un operatore locale non invertibile che trasforma $|\psi\rangle$ in $|\phi\rangle$ come:

$$|\phi\rangle = (A \otimes B \otimes C)|\psi\rangle$$

dove, per la non invertibilità, almeno uno tra gli operatori A, B, C deve avere rango uno. Quindi deve diminuire almeno uno dei ranghi delle matrici ridotte. Se $|\psi\rangle$ appartiene o alla classe GHZ o alla classe W, allora $|\psi\rangle$ può appartenere solo o alle classi di entanglement bipartito o a quella degli stati separabili. Uno stato della classe GHZ non potrà mai essere convertito in uno della classe W e viceversa. Per ragionamenti analoghi uno stato bipartito potrà essere trasformato solo in un uno stato separabile, e non in uno stato di un'altra classe di entanglement bipartito, perché dovrebbe aumentare il rango di una delle matrici ridotte, che è impossibile per trasformazioni locali [9]. In Fig. 4.1 sono schematizzate le possibili conversioni.

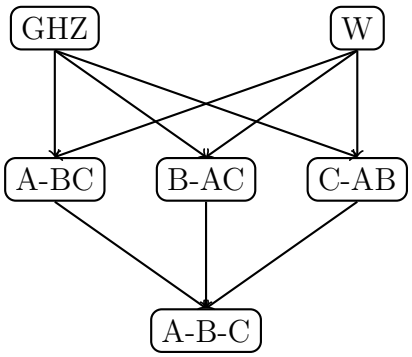

Figura 4.1: Nello schema sono visualizzate le diverse classi per un sistema a tre qubit. Le direzioni delle freccie indicano quali operazioni locali non invertibili si possono fare.

Bibliografia

[1] A. Aspect, J. Dalibard e G. Roger. "Experimental Test of Bell's Inequalities Using Time-Varying Analyzers". In: *Phys. Rev. Lett.* 49 (25 dic. 1982), pp. 1804–1807. DOI: 10.1103/PhysRevLett.49.1804. URL: https://link.aps.org/doi/10.1103/PhysRevLett.49.1804.

[2] A. Aspect, P. Grangier e G. Roger. "Experimental Tests of Realistic Local Theories via Bell's Theorem". In: *Phys. Rev. Lett.* 47 (7 ago. 1981), pp. 460–463. DOI: 10.1103/PhysRevLett.47.460. URL: https://link.aps.org/doi/10.1103/PhysRevLett.47.460.

[3] S. D. Bartlett, T. Rudolph e R. W. Spekkens. "Reference frames, superselection rules, and quantum information". In: *Reviews of Modern Physics* 79.2 (apr. 2007), pp. 555–609. DOI: 10.1103/revmodphys.79.555. URL: https://doi.org/10.1103%2Frevmodphys.79.555.

[4] J. S. Bell. "On the Einstein Podolsky Rosen paradox". In: *Physics Physique Fizika* 1 (3 nov. 1964), pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195. URL: https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195.

[5] C. H. Bennett e S. J. Wiesner. "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". In: *Phys. Rev. Lett.* 69 (20 nov. 1992), pp. 2881–2884. DOI: 10.1103/PhysRevLett.69.2881. URL: https://link.aps.org/doi/10.1103/PhysRevLett.69.2881.

[6] C. H. Bennett et al. "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels". In: *Physical Review Letters* 76.5 (gen. 1996), pp. 722–725. DOI: 10.1103/physrevlett.76.722. URL: https://doi.org/10.1103%2Fphysrevlett.76.722.

[7] C. H. Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Phys. Rev. Lett.* 70 (13 mar. 1993), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895. URL: https://link.aps.org/doi/10.1103/PhysRevLett.70.1895.

[8] E. Chitambar e G. Gour. "Quantum resource theories". In: *Reviews of Modern Physics* 91.2 (apr. 2019). DOI: 10.1103/revmodphys.91.025001. URL: https://doi.org/10.1103%2Frevmodphys.91.025001.

[9] W. Dür, G. Vidal e J. I. Cirac. "Three qubits can be entangled in two inequivalent ways". In: *Physical Review A* 62.6 (nov. 2000). DOI: 10.1103/physreva.62.062314. URL: https://doi.org/10.1103%2Fphysreva.62.062314.

[10] A. Einstein, B. Podolsky e N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Phys. Rev.* 47 (10 mag. 1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777. URL: https://link.aps.org/doi/10.1103/PhysRev.47.777.

[11] S. J. Freedman e J. F. Clauser. "Experimental Test of Local Hidden-Variable Theories". In: *Phys. Rev. Lett.* 28 (14 apr. 1972), pp. 938–941. DOI: 10.1103/PhysRevLett.28.938. URL: https://link.aps.org/doi/10.1103/PhysRevLett.28.938.

[12] G. Gour et al. "The resource theory of informational nonequilibrium in thermodynamics". In: *Physics Reports* 583 (lug. 2015), pp. 1–58. DOI: 10.1016/j.physrep.2015.04.003. URL: https://doi.org/10.1016%2Fj.physrep.2015.04.003.

[13] R. Horodecki et al. "Quantum entanglement". In: *Reviews of Modern Physics* 81.2 (giu. 2009), pp. 865–942. DOI: 10.1103/revmodphys.81.865. URL: https://doi.org/10.1103%2Frevmodphys.81.865.

[14] M. Kumar. *Quantum: Einstein, Bohr and the Greate Debate About the Nature of Reality*. A cura di I. Books. 2009, p. 313.

[15] M. A. Nielsen. "Conditions for a Class of Entanglement Transformations". In: *Physical Review Letters* 83.2 (lug. 1999), pp. 436–439. DOI: 10.1103/physrevlett.83.436. URL: https://doi.org/10.1103%2Fphysrevlett.83.436.

[16] M. A. Nielsen e I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010, pp. 571–581. DOI: 10.1017/CBO9780511976667.

[17] M. B. Plenio e S. Virmani. *An introduction to entanglement measures*. 2006. arXiv: quant-ph/0504163 [quant-ph].

[18] E. Schrödinger. "Discussion of Probability Relations between Separated Systems". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 31.4 (1935), pp. 555–563. DOI: 10.1017/S0305004100013554.

[19] G. Vidal. "Entanglement monotones". In: *Journal of Modern Optics* 47.2-3 (feb. 2000), pp. 355–376. DOI: 10.1080/09500340008244048. URL: https://doi.org/10.1080%2F09500340008244048.

[20] G. Vidal. “Entanglement of Pure States for a Single Copy”. In: *Physical Review Letters* 83.5 (ago. 1999), pp. 1046–1049. DOI: 10.1103/physrevlett.83.1046. URL: https://doi.org/10.1103%2Fphysrevlett.83.1046.

[21] C. Weedbrook et al. “Gaussian quantum information”. In: *Rev. Mod. Phys.* 84 (2 mag. 2012), pp. 621–669. DOI: 10.1103/RevModPhys.84.621. URL: https://link.aps.org/doi/10.1103/RevModPhys.84.621.