Indice

Introduzione

La Quantum Information è il ramo della fisica che consiste nello studio dei sistemi quantistici come mezzi per la codifica e l'elaborazione di informazione. Negli ultimi anni questo campo ha destato crescente interesse grazie alla risonanza ottenuta da alcuni risultati. Sfruttando effetti strettamente quantistici, quali l'*entanglement*, il principio di sovrapposizione, e le relazioni di indeterminazione, è stato infatti possibile progettare algoritmi molto più efficienti dei loro corrispondenti classici e realizzare in laboratorio, tra gli altri, sistemi crittografici la cui inviolabilità è garantita dai principi della meccanica quantistica, canali di comunicazione che codificano due unità fondamentali di informazione classica in una sola di informazione quantistica (*codifica superdensa*), o il trasferimento senza interazione diretta dello stato di un sistema su di un secondo sistema identico (*teletrasporto*).

Studiare efficacemente gli stati quantistici come portatori di informazione significa, essenzialmente, studiare come l'informazione possa essere codificata, decodificata ed elaborata su di un sistema quantistico. Questo porta necessariamente a porsi problemi di carattere più propriamente fisico che applicativo: decodificare l'informazione, cioè estrarla dal sistema fisico, corrisponde ad effettuare delle misurazioni, per cui interesserà approfondire la teoria della misura; mentre per analizzare le possibili codifiche ed elaborazioni è necessario classificare le possibili operazioni su di un sistema. Per entrambi i problemi sono stati sviluppati approcci prima che l'informazione quantistica prendesse forma come campo di studio; mostrandone però l'utilità al fine di

applicazioni pratiche, quest'ultima ha risvegliato l'interesse nei confronti di questi due tipi di problemi e ne ha incoraggiato l'approfondimento.

Già negli anni '70 erano stati sviluppati due modelli matematici per le misure e le macchine quantistiche completi e più generali delle misurazioni di osservabili autoaggiunte e delle evoluzioni unitarie che si è abituati a prendere in considerazione: si tratta rispettivamente delle *POVM* (*Positive Operator-Valued Measure*) e delle *Quantum Operation*. Questi due oggetti matematici astraggono dalla struttura interna degli strumenti che rappresentano, focalizzandosi sulla relazione tra lo stato del sistema in ingresso e la distribuzione di probabilità sullo spazio dei risultati della misurazione (per le POVM), o lo stato del sistema in uscita (per le Quantum Operation). Conoscere il meccanismo interno di uno strumento di misura, o di qualsiasi altro apparecchio che agisca su un sistema quantistico, permette di ricavare la POVM o la Quantum Operation associata; ma a partire dalla scrittura formale di una POVM o di una Quantum Operation si possono solo ottenere indizi su una delle molteplici realizzazioni pensabili. Un simile grado di astrazione non rende sterile un modello: ricordiamo che è ad esempio condiviso dalla nota e fruttuosa trattazione delle macchine termiche tramite cicli termodinamici, la quale ha portato a risultati di notevole interesse come il teorema di Carnot, oltre a molteplici applicazioni pratiche in tecnologie oggi di uso quotidiano. Analogamente, queste scritture astratte permettono di ricavare enunciati generalmente validi riguardo alla possibilità o impossibilità di principio di compiere certe operazioni (di misura o trasformazione) e di trovare i limiti ideali della loro efficienza.

Nel presente lavoro si è affrontato un problema di questo tipo. Si è presa in considerazione l'operazione consistente nel costruire a partire da N stati ortogonali inizialmente ignoti uno stato che sia loro sovrapposizione ad ampiezze e fasi relative fissate. Una macchina del genere avrebbe diverse

possibili applicazioni, di cui la più evidente è la creazione di entanglement; tuttavia non è possibile realizzarla esattamente, e si sono cercate, partendo da casi particolari e via via generalizzando, le Quantum Operation che meglio la approssimano. Non risultano studi del genere in letteratura, e nel corso di quello svolto qui sono emersi alcuni risultati inaspettati. Il metodo con cui si è ottenuto il risultato più generale, che contempla anche i casi in cui si richiedano copie multiplein ingresso o in uscita, è stato generalizzato in un teorema applicabile anche in diversi contesti

La tesi è organizzata come segue:

Nel **primo capitolo** si introdurrà il formalismo delle Quantum Operation. Si partirà dal modello fisico generale di macchina quantistica per ricavarne, deduttivamente, tre caratterizzazioni diverse ma equivalenti, e le si utilizzerà per dimostrarne alcune proprietà salienti. Si concluderà il capitolo con alcuni esempi di Quantum Operation semplici ma significative, di cui si calcolerà la rappresentazione in tutte le caratterizzazioni esaminate.

Nel **secondo capitolo** si introdurranno i concetti necessari alla formulazione e risoluzione del problema del sovrappositore come problema di ottimizzazione covariante. Si definirà il concetto di Quantum Operation covariante, e se ne fornirà una completa classificazione in termini di operatori invarianti. Si introdurrà poi il concetto di distanza tra due Quantum Operation, ai fini di affrontare problemi di approssimazione ottima. Successivamente, si introdurranno le Quantum Operation come strutture convesse semplificando in tal modo problemi di ottimizzazione. Infine si introdurrà il concetto di covarianza forte, definito per operazioni quantistiche da m stati in n stati di sistemi identici, e si presenteranno alcuni risultati originali trovati in tale contesto.

Nell **terzo capitolo** si imposterà innanzitutto in maniera generale il problema dell'approssimazione di un sovrappositore di due stati ortogonali con pari ampiezza per la covarianza universale. La soluzione esplicita sarà presentata sia nel caso di sistemi a due dimensioni (*qubit*), che nel caso più generale di generica dimensione finita. Si studierà quindi l'approssimazione di una macchina che sovrappone più stati, a partire da un numero generico di copie degli stati da sovrapporre e producendo u numero generico di sovrapposizioni. Studiandone il caso covariante in fase per input invarianti, si ricaverà un risultato che si troverà valere in generale per il caso universalmente covariante e che generalizza quanto trovato per il sovrappositore semplice. Si imposterà poi l'ottimizzazione del sovrappositore da copia singola in copia singola covariante in fase per il qubit. Si concluderà presentando una ulteriore generalizzazione del risultato, applicabile anche a macchine diverse dal sovrappositore e a gruppi di simmetria diversi dalla fase o da quello universale.

Convenzioni matematiche

Nel presente lavoro gli spazi di Hilbert sono da intendersi a dimensione finita. Anche se diversi ragionamenti possono probabilmente essere estesi a generici spazi separabili in modo banale, la trattazione di spazi a dimensione infinita esula da questa tesi.

Insiemi e superoperatori si sono rappresentati in carattere calligrafico, cercando di evitare per tutto il testo sovrapposizioni nell'uso delle lettere. Dove non specificato diversamente, si può assumere che $\mathcal{H}, \mathcal{J}, \mathcal{K}, \mathcal{A}$ siano spazi di Hilbert, $\mathcal{S}$ sia un insieme, $\mathcal{E}, \mathcal{F}, \mathcal{I}$ siano funzioni da operatori in operatori, $\mathcal{G}$ sia un gruppo. $\mathcal{B}(\mathcal{H}, \mathcal{K})$ indica l'insieme gli operatori limitati da $\mathcal{H}$ in $\mathcal{K}$. Per spazi di Hilbert a dimensione finita, coincide con l'insieme degli operatori lineari;per brevità l'insieme degli operatori da uno spazio in sé sarà indicato da $\mathcal{B}(\cdot)$. Eccezione all'uso del carattere calligrafico faranno le strutture $\mathbb{N}, \mathbb{R}, \mathbb{C}$ dei numeri naturali, reali, e complessi rispettivamente.

Si sono usate lettere maiuscole per gli operatori lineari, cercando di riservare U, V, W ad operatori unitari, P a proiettori. Le lettere minuscole si sono utilizzate invece per i numeri, e per i vettori su spazi vettoriali reali nel capitolo 2.

Per non appesantire la notazione, siè preferito sottointendere gli insiemi su cui corrono gli indici qualora fosse chiaro dal contesto.

Isomorfismo tra operatori e vettori

Siano $\mathcal{H}$,$\mathcal{K}$ spazi di Hilbert; sia $E : \mathcal{H} \to \mathcal{K}$ un operatore lineare. Scelte due basi $\{|k_i\rangle\} \subset \mathcal{K}$ e $\{|h_j\rangle\} \subset \mathcal{H}$. Si può costruire un'applicazione che mappi

$$E = \sum_{i,j} \langle k_i|E|h_j\rangle \ |k_j\rangle\langle h_j|$$

in

$$|E\rangle\!\rangle = \sum_{i,j} \langle k_i|E|h_j\rangle \ |k_j\rangle \otimes |h_j\rangle.$$

È evidente che tale applicazione è lineare e biiettiva, e quindi costituisce un isomorfismo di spazi vettoriali tra $\mathcal{B}(\mathcal{H}, \mathcal{K})$ e $\mathcal{K}\otimes\mathcal{H}$. Si noti che la costruzione della mappa dipende dalla scelta di una base su $\mathcal{H}$.

Posti $D \in \mathcal{B}(\mathcal{K})$ e $F \in \mathcal{B}(\mathcal{H})$, tramite il calcolo matriciale si trova facilmente che

$$D \otimes F|E\rangle\!\rangle = |DEF^T\rangle\!\rangle,$$

in cui l'operazione di trasposizione è definita sulla stessa base di $\mathcal{H}$ su cui si è costruito l'isomorfismo.

Si può inoltre notare che, definito su $\mathcal{B}(\mathcal{H}, \mathcal{K})$ il prodotto Hermitiano di Hilbert-Schmidt $(A, B)_{HS} \doteq \mathrm{Tr}\left[A^\dagger B\right]$ si trova $(A, B)_{HS} = \langle\!\langle A|B\rangle\!\rangle$, cioè la mappa $E \mapsto |E\rangle\!\rangle$ costituisce un isomorfismo tra spazi di Hilbert.

Capitolo 1

Macchine Quantistiche e Quantum Operation

Gli assiomi della meccanica quantistica stabiliscono che gli stati ρ_1 e ρ_2 ai tempi t_1 e t_2 di un sistema chiuso siano connessi secondo la relazione $\rho_1 = U\rho_2 U^\dagger$ da un operatore unitario U, funzione unicamente della differenza tra t_1 e t_2 e della fisica del sistema espressa tramite l'operatore hamiltoniano H.

L'evoluzione libera e unitaria non è tuttavia l'unica a cui un sistema possa sottostare: evoluzioni di sistemi aperti sono state prese in considerazione per casi particolari sin dai primi tempi della teoria, nell'affrontare problemi importanti come la descrizione degli spettri atomici (teoria semiclassica della radiazione) o il collasso della funzione d'onda (misura alla Von Neumann[2]). Nella Quantum Information, trattando gli stati quantistici come portatori di informazione, si è interessati alle trasformazioni che è possibile operare *fisicamente* sullo stato di un sistema (che saranno, in generale, un sottoinsieme di quelle applicabili matematicamente) non solo tramite un'opportuna dinamica chiusa, ma anche eventualmente guidandone l'evoluzione per mezzo di qualche apparato. Le applicazioni che descrivono lo stato in uscita in funzione dello stato in ingresso a macchine quantistiche siffatte o di forma

più generale sono dette **Quantum Operation**.

Nel presente capitolo si partirà da modelli fisci generali delle macchine quantistiche per dare tre caratterizzazioni diverse (ma equivalenti) delle Quantum Operation, e si useranno questi strumenti per una discussione preliminare delle loro proprietà. Il capitolo sarà chiuso da alcuni esempi di operazione di operazione quantistica, di cui si calcoleranno le espressioni esplicite.

1.1 Modelli e Forma di Kraus

1.1.1 Evoluzione guidata di un sistema

Si consideri un generico macchinario che posto in contatto con un sistema quantistico ne guidi l'evoluzione. Sistema e apparato saranno lasciati interagire per un tempo fissato. Si desidera conoscere la relazione tra gli stati del sistema prima e dopo l'interazione.

Nel linguaggio della meccanica quantistica, si descriverà il tutto come segue: all'apparato andrà associato lo spazio di Hilbert $\mathcal{A}$, mentre si rappresenterà il sistema da evolvere sullo spazio di Hilbert $\mathcal{H}$. La scelta della descrizione dell'apparato sarà operata in modo che il sistema composto $\mathcal{H}\otimes\mathcal{A}$ si possa considerare chiuso con buona approssimazione per tutto l'arco dell'interazione. L'apparato viene preparato prima di ogni uso in uno stato fissato, detto stato di pronto; pertanto non ci saranno correlazioni[1], e lo stato del sistema composto sarà scrivibile nella forma fattorizzata:

$$\rho = \rho_{\mathcal{H}} \otimes \rho_{\mathcal{A}} \tag{1.1}$$

con ovvio significato dei pedici. L'interazione tra apparato e sistema è

[1]La presenza di eventuali correlazioni rendenderebbe l'evoluzione non univocamente determinata dallo stato locale di partenza $\rho_{\mathcal{H}}$, anche a dinamica fissata. Una trattazione formale del problema si può trovare in [8].

adeguatamente rappresentata dall'evoluzione libera, sotto una Hamiltoniana opportuna, del sistema composto. Esisterà quindi un operatore unitario su $\mathcal{H} \otimes \mathcal{A}$, che chiameremo U, tale per cui lo stato del sistema composto al termine dell'operazione si possa scrivere $\rho' = U\rho_{\mathcal{H}} \otimes \rho_{\mathcal{A}} U^\dagger$. Lo stato finale del sistema di cui si è guidato l'evoluzione si troverà tracciando ρ' su $\mathcal{A}$:

$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathcal{A}} \left[U\rho_{\mathcal{H}} \otimes \rho_{\mathcal{A}} U^\dagger \right] \tag{1.2}$$

Scegliendo una base ortonormale $\{|i\rangle_{\mathcal{A}}\} \subset \mathcal{A}$ che diagonalizzi $\rho_{\mathcal{A}}$ (per cui, dunque, si possa scrivere $\rho_{\mathcal{A}} = \sum_i p_i |i\rangle_{\mathcal{A}} \, {}_{\mathcal{A}}\langle i|$), la precedente si riscrive:

$$\mathcal{E}(\rho) = \sum_{i,j} \, {}_{\mathcal{A}}\langle j|U \, \rho_{\mathcal{H}} \otimes p_i |i\rangle_{\mathcal{A}} \, {}_{\mathcal{A}}\langle i| \, U^\dagger |j\rangle_{\mathcal{A}}$$

o equivalentemente:

$$\mathcal{E}(\rho) = \sum_{i,j} p_i \, {}_{\mathcal{A}}\langle j|U|i\rangle_{\mathcal{A}} \, \rho_{\mathcal{H}} \, \, {}_{\mathcal{A}}\langle i|U^\dagger|j\rangle_{\mathcal{A}} \tag{1.3}$$

In cui gli elementi di matrice parziali ${}_{\mathcal{A}}\langle j|U|i\rangle_{\mathcal{A}}$ dell'operatore $U \in \mathcal{B}(\mathcal{H} \otimes \mathcal{A})$ sono chiaramente operatori su $\mathcal{H}$. Etichettandoli uno a uno e riscalandoli opportunamente, ossia ponendo

$$E_{ij} \doteq \sqrt{p_i} \, {}_{\mathcal{A}}\langle j|U|i\rangle_{\mathcal{A}} \in \mathcal{B}(\mathcal{H}) \tag{1.4}$$

la (1.3) si può riscrivere

$$\mathcal{E}(\rho_{\mathcal{H}}) = \sum_{i,j} E_{ij} \rho_{\mathcal{H}} E_{ij}^\dagger \tag{1.5}$$

o meglio, rinumerando con un indice singolo k le E_{ij} non nulle

$$\mathcal{E}(\rho) = \sum_k E_k \rho_{\mathcal{H}} E_k^\dagger \tag{1.6}$$

Una scrittura come questa è detta *operator-sum representation* o *decomposizione di Kraus* dell'operazione quantistica.[5] Gli operatori E_k sono detti *elementi* dell'operazione.

Proposizione 1.1 *Sia $\{E_k\} \subset \mathcal{B}(\mathcal{H})$ l'insieme degli elementi in rappresentazione di Kraus di un'operazione quantistica su uno spazio di Hilbert $\mathcal{H}$. Allora si ha*

$$\sum_k E_k^\dagger E_k = I_{\mathcal{H}} \tag{1.7}$$

dove $I_{\mathcal{H}}$ denota l'operatore identico su $\mathcal{H}$.

Dimostrazione. Se gli E_k sono gli elementi di un'operazione quantistica, per ogni ρ stato di $\mathcal{H}$ soddisfano una relazione della forma (1.6), in cui $\mathcal{E}(\rho_{\mathcal{H}})$ è ancora uno stato di $\mathcal{H}$. Tracciandone entrambi i membri si ottiene

$$\mathrm{Tr}\left[\sum_k E_k \rho_{\mathcal{H}} E_k^\dagger\right] = 1$$

che per la proprietà ciclica della traccia si può riscrivere

$$\mathrm{Tr}\left[\sum_k E_k^\dagger E_k \rho_{\mathcal{H}}\right] = 1 \tag{1.8}$$

La richiesta che la precedente equazione sia verificata per ogni $\rho_{\mathcal{H}}$ a traccia unitaria implica la tesi. Infatti se la (1.8) vale per tutti gli stati su $\mathcal{H}$, varrà in particolare per tutti gli stati puri; cioè si avrà:

$$\mathrm{Tr}\left[\sum_k E_k^\dagger E_k |\psi\rangle\langle\psi|\right] = 1 \qquad \forall |\psi\rangle \in \mathcal{H}$$

Ma $\mathrm{Tr}\left[\sum_k E_k^\dagger E_k |\psi\rangle\langle\psi|\right] = \langle\psi| \sum_k E_k^\dagger E_k |\psi\rangle$, e l'unico operatore ad avere valore d'aspettazione 1 su tutti i vettori di $\mathcal{H}$ è l'identità. □

Abbiamo fin qui dimostrato che per ogni evoluzione aperta che si possa scrivere nella forma (1.2), fissati lo stato di partenza dell'apparato e l'interazione fisica tra questo e il sistema in studio, esiste un insieme di operatori $\{E_k\}$ vincolati da una relazione di completezza della forma (1.7) e tali che si possa rappresentare la dipendenza dell'evoluto dallo stato di partenza nella forma (1.6).

Dimostreremo ora il risultato opposto: cioè che a qualunque insieme di operatori che soddisfi la (1.7) si può associare un'evoluzione aperta della forma (1.2).

Proposizione 1.2 *Sia* $\{E_k\} \subset \mathcal{B}(\mathcal{H})$*, con* $\sum_k E_k^\dagger E_k = I_\mathcal{H}$*. Allora esistono uno spazio di Hilbert* $\mathcal{A}$*, una matrice densità* $\rho_\mathcal{A} \in \mathcal{B}(A)$ *e un operatore unitario* $U \in \mathcal{B}(\mathcal{H} \otimes \mathcal{A})$ *tali che*

$$\sum_k E_k \rho_\mathcal{H} E_k^\dagger = \mathrm{Tr}_\mathcal{A}\left[U(\rho_\mathcal{H} \otimes \rho_\mathcal{A})U^\dagger\right] \tag{1.9}$$

per ogni $\rho_\mathcal{H}$ *stato in* $\mathcal{B}(\mathcal{H})$*.*

Dimostrazione. Scegliamo $\mathcal{A}$ tale che $\dim \mathcal{A} \geq \#\{E_k\}$, e fissiamo in $\mathcal{A}$ una base ortonormale $\mathcal{B}_\mathcal{A} = \{|i\rangle_\mathcal{A}, \quad 1 \leq i \leq \dim \mathcal{A}\}$.

Consideriamo ora l'applicazione da $\mathcal{H} \otimes |1\rangle_\mathcal{A}$ in $\mathcal{H} \otimes \mathcal{A}$:

$$|\psi\rangle|1\rangle_\mathcal{A} \mapsto \sum_k E_k|\psi\rangle|k\rangle_\mathcal{A} \tag{1.10}$$

Essa è manifestamente lineare; inoltre, la relazione di completezza per gli E_k implica che sia isometrica, infatti

$$\sum_{j,k} \langle\phi|E_j^\dagger E_k|\psi\rangle \ {}_\mathcal{A}\langle j|k\rangle_\mathcal{A} = \sum_k \langle\phi|E_k^\dagger E_k|\psi\rangle = \langle\phi|\psi\rangle = \langle\phi|\psi\rangle \ {}_\mathcal{A}\langle 1|1\rangle_\mathcal{A}$$

Il fatto che la (1.10) sia lineare ed isometrica garantisce che possa essere estesa ad un operatore unitario $U \in \mathcal{B}(\mathcal{H} \otimes \mathcal{A})$. Tracciando sull'apparato $U(\rho_\mathcal{H} \otimes |1\rangle_\mathcal{A} \ {}_\mathcal{A}\langle 1|)U^\dagger$ si conclude la dimostrazione; infatti per ogni $\rho_\mathcal{H} \in \mathcal{B}(\mathcal{H})$ si ottiene:

$$\mathrm{Tr}_\mathcal{A}\left[U(\rho_\mathcal{H} \otimes |1\rangle_\mathcal{A} \ {}_\mathcal{A}\langle 1|)U^\dagger\right] = \mathrm{Tr}_\mathcal{A}\left[\sum_{j,k} E_j \rho_\mathcal{H} E_k^\dagger \otimes |j\rangle_\mathcal{A} \ {}_\mathcal{A}\langle k|\right] = \sum_k E_k \rho_\mathcal{H} E_k^\dagger$$

che verifica la tesi. □

Abbiamo fin qui mostrato prima di tutto come ogni operazione quantistica fisicamente realizzabile su un sistema ammetta una decomposizione di Kraus, e successivamente come ogni $\mathcal{F}(\rho) = \sum_k E_k \rho E_k^\dagger$ con $\{E_k\}$ tale che $\sum_k E_k^\dagger E_k = I$ sia la decomposizione di Kraus di una quantum operation. Da questo consegue che l'insieme delle funzioni da $\mathcal{B}(\mathcal{H})$ in $\mathcal{B}(\mathcal{H})$ scrivibili nella forma di Kraus (1.6) per cui gli elementi della decomposizione soddisfano la relazione di completezza (1.7) coincide con quello delle quantum operation su $\mathcal{H}$.

Le scritture come la (1.2) sono dette *realizzazioni unitarie* della quantum operation associata. Le corrispondenze fra Quantum Operation e decomposizioni di Kraus e fra Quantum Operation e realizzazioni non sono biunivoche; ma prima di dimostrare questo enunciato attenderemo di poterlo fare nel caso più generale.

1.1.2 Macchine quantistiche

Per semplicità nella sezione precedente abbiamo preso in considerazione solo macchine quantistiche che agiscano in maniera fissata su di un sistema. In realtà ogni altro schema pensabile si può ricondurre ad un caso non molto più complesso, che passiamo ad analizzare.

L'apparato della macchina è anche in questo caso un sistema quantistico (eventualmente composto) rappresentabile sullo spazio di Hilbert $\mathcal{A}$ e inizialmente preparato nello stato di pronto fissato $\rho_{\mathcal{A}}$; questo sistema viene fatto interagire per un tempo fissato con uno stato arbitrario $\rho_{\mathcal{H}}$ di un altro sistema quantistico (eventualmente composto) $\mathcal{H}$, detto **sistema di input**; coerentemente ai postulati della meccanica quantistica, al termine dell'interazione il sistema composto apparato+input si troverà nello stato $U(\rho_{\mathcal{H}} \otimes \rho_{\mathcal{A}})U^\dagger$, dove U è un opportuno operatore unitario in $\mathcal{B}(\mathcal{H} \otimes \mathcal{A})$. Vogliamo prendere in considerazione lo stato di un sottosistema, che chiameremo **sistema di output** e rappresenteremo sullo spazio di Hilbert $\mathcal{K}$, del sistema totale appara-

to+input; se l'output è sottosistema di apparato+input, allora per gli assiomi della meccanica quantistica e le proprietà del prodotto tensore esisterà uno spazio di Hilbert $\mathcal{J}$ tale per cui $\mathcal{H}\otimes\mathcal{A}\simeq\mathcal{J}\otimes\mathcal{K}$, e di conseguenza lo stato di output sarà dato da $\mathrm{Tr}_{\mathcal{J}}\left[U(\rho_{\mathcal{H}}\otimes\rho_{\mathcal{A}})U^{\dagger}\right]$. Si vede subito che questo schema è una generalizzazione di quello dato nella sezione precedente, che si ritrova immediatamente ponendo $\mathcal{K}=\mathcal{H}$. Andiamo ora a generalizzare anche i risultati trovati sulle decomposizioni di Kraus come caratterizzazione delle quantum operation:

Proposizione 1.3 *Siano $\mathcal{H}$, $\mathcal{A}$ spazi di Hilbert, $\rho_{\mathcal{A}}\in\mathcal{B}(\mathcal{A})$ stato fissato, $U\in\mathcal{B}(\mathcal{H}\otimes\mathcal{A})$ unitario fissato; siano $\mathcal{J},\mathcal{K}$ spazi di Hilbert tali che $\mathcal{J}\otimes\mathcal{K}=\mathcal{H}\otimes\mathcal{A}$. Allora, posta*

$$\mathcal{E}:\mathcal{B}(\mathcal{H})\to\mathcal{B}(\mathcal{K})\quad,\qquad\rho\mapsto\mathrm{Tr}_{\mathcal{J}}\left[U(\rho\otimes\rho_{\mathcal{A}})U^{\dagger}\right]$$

si ha che esiste un insieme ordinato $\{E_k\}\subset\mathcal{B}(\mathcal{H},\mathcal{K})$ tale che:

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

e

$$\sum_k E_k E_k=I_{\mathcal{H}}\tag{1.11}$$

Dimostrazione. Si è seguito lo stesso percorso logico della sezione precedente, con piccolissime modifiche.

Fissate due basi ortogonali $\{|i\rangle_{\mathcal{A}}\}\subset\mathcal{A}$ e $\{|j\rangle_{\mathcal{J}}\}\subset\mathcal{J}$ rispettivamente per $\mathcal{A}$ e $\mathcal{J}$, se si è posto $\{|i\rangle_{\mathcal{A}}\}$ tale che $\rho_{\mathcal{A}}=\sum_i p_i|i\rangle_{\mathcal{A}}\,{}_{\mathcal{A}}\langle i|$ si può scrivere:

$$\mathcal{E}(\rho)=\sum_{i,j}{}_{\mathcal{J}}\langle j|U(\rho\otimes p_i|i\rangle_{\mathcal{A}}\,{}_{\mathcal{A}}\langle i|)U^{\dagger}|j\rangle_{\mathcal{J}},$$

ossia

$$\mathcal{E}(\rho)=\sum_{i,j}p_i\,{}_{\mathcal{J}}\langle j|U|i\rangle_{\mathcal{A}}\rho\,{}_{\mathcal{A}}\langle i|U^{\dagger}|j\rangle_{\mathcal{J}}$$

Fissando

$$E_{j,i} \doteq \sqrt{p_i}\ {}_{\mathcal{J}}\langle j|U|i\rangle_{\mathcal{A}}$$

e rinumerando gli $E_{j,i}$ non nulli su di un unico indice k, l'espressione diventa

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger,$$

che costituisce proprio la prima parte della tesi.

Per la seconda parte si veda la dimostrazione della proposizione 1.1. □

Proposizione 1.4 *Sia* $\{E_k\} \subset \mathcal{B}(\mathcal{H}, \mathcal{K})$*, con* $\sum_k E_k^\dagger E_k = I_{\mathcal{H}}$*. Allora esistono due spazi di Hilbert,* $\mathcal{A}$ *e* $\mathcal{J}$*, una matrice densità* $\rho_{\mathcal{A}} \in \mathcal{B}(A)$ *e un operatore unitario* $U \in \mathcal{B}(\mathcal{H} \otimes \mathcal{A})$ *tali che*

$$\sum_k E_k \rho_{\mathcal{H}} E_k^\dagger = \mathrm{Tr}_{\mathcal{J}} \left[U(\rho_{\mathcal{H}} \otimes \rho_{\mathcal{A}}) U^\dagger \right] \tag{1.12}$$

per ogni $\rho_{\mathcal{H}}$ *stato in* $\mathcal{B}(\mathcal{H})$*.*

Dimostrazione. Si scelga $\mathcal{J}$ in modo tale che $\dim \mathcal{J} = \#\{E_k\}$, $\mathcal{A}$ tale che $\mathcal{H} \otimes \mathcal{A} = \mathcal{K} \otimes \mathcal{J}$. Fissata una base ortonormale $\{|j\rangle_{\mathcal{J}}\}$ per $\mathcal{J}$ e un vettore normalizzato $|A\rangle \in \mathcal{A}$, si consideri la seguente applicazione lineare da $\mathcal{H} \otimes |A\rangle$ in $\mathcal{H} \otimes \mathcal{A} = \mathcal{K} \otimes \mathcal{J}$:

$$|\psi\rangle|A\rangle \mapsto \sum_k E_k|\psi\rangle|k\rangle_{\mathcal{J}} \tag{1.13}$$

e si proseegua come nella dimostrazione della proposizione 1.2, sostituendo questa applicazione alla (1.10) e $\mathrm{Tr}_{\mathcal{J}}$ a $\mathrm{Tr}_{\mathcal{A}}$.□

1.1.3 Proprietà della forma di Kraus

Scrivere le quantum operation in forma di Kraus permette di dimostrarne alcune proprietà di semplice interpretazione fisica.

Proposizione 1.5 *La composizione di due Quantum Operation è ancora una Quantum Operation.*

Dimostrazione. Siano $\mathcal{H}, \mathcal{J}, \mathcal{K}$ spazi di Hilbert. Se $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{J})$, $\mathcal{F} : \mathcal{B}(\mathcal{J}) \to \mathcal{B}(\mathcal{K})$ sono quantum operation, possono essere scritte in forma di Kraus, cioè si ha

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \qquad , \qquad \mathcal{F}(\sigma) = \sum_j F_j \sigma F_j^\dagger$$

per opportuni $\{F_j\} \subset \mathcal{B}(\mathcal{J}, \mathcal{K}), \{E_k\} \subset \mathcal{B}(\mathcal{H}, \mathcal{J})$ che verificano la relazione di completezza. La mappa composta $\mathcal{F} \circ \mathcal{E}$ si può allora scrivere:

$$\mathcal{F} \circ \mathcal{E}(\rho) = \mathcal{F}(\mathcal{E}(\rho)) = \mathcal{F}(\sum_k E_k \rho E_k^\dagger) = \sum_{j,k} F_j E_k \rho E_k^\dagger F_j^\dagger$$

In cui l'ultimo membro è manifestamente una rappresentazione in forma di Kraus, con insieme degli elementi $\{F_j E_k\}$. Infatti

$$\sum_{j,k} E_k^\dagger F_j^\dagger F_j E_k = \sum_k E_k^\dagger \left(\sum_j F_j^\dagger F_j \right) E_k = \sum_k E_k^\dagger E_k = I_{\mathcal{H}}$$

□

Proposizione 1.6 *La combinazione convessa*

$$p\mathcal{E}(\rho) + (1-p)\mathcal{F}(\rho) \quad , \qquad 0 \leq p \leq 1$$

di due Quantum Operation è ancora una Quantum Operation.

Dimostrazione. Siano $\mathcal{E}$ e $\mathcal{F}$ due Quantum Operation da $\mathcal{B}(\mathcal{H})$ in $\mathcal{B}(\mathcal{K})$, $\{E_k\}, \{F_j\}$ decomposizioni di Kraus a loro associate, p reale positivo non maggiore di 1. Si ha:

$$p\mathcal{E}(\rho) + (1-p)\mathcal{F}(\rho) = \sum_k p E_k \rho E_j^\dagger + \sum_j (1-p) F_j \rho F_j^\dagger \tag{1.14}$$

Ponendo

$$G_i \doteq \sqrt{p} E_i \qquad \text{per} \qquad 1 \leq i \leq \#\{E_k\}$$
$$G_{\#\{E_k\}+l} \doteq \sqrt{1-p} F_l \qquad \text{per} \qquad 1 \leq l \leq \#\{F_j\}$$

si trova che $\{G_i\}$ è una decomposizione di Kraus, in quanto

$$\sum_i G_i^\dagger G_i = p\sum_k E_k^\dagger E_k + (1-p)\sum_j F_j^\dagger F_j = pI_{\mathcal{H}} + (1-p)I_{\mathcal{H}} = I_{\mathcal{H}}$$

e tramite la (1.14) si verifica facilmente che

$$\sum_i G_i \rho G_i^\dagger = p\mathcal{E}(\rho) + (1-p)\mathcal{F}(\rho)$$

□

Proposizione 1.7 *Siano $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$ e $\mathcal{F} : \mathcal{B}(\mathcal{J}) \to \mathcal{B}(\mathcal{L})$ due Quantum Operation. Allora il loro prodotto tensoriale*[2] *$\mathcal{E} \otimes \mathcal{F} : \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{J}) \to \mathcal{B}(\mathcal{K}) \otimes \mathcal{B}(\mathcal{L})$ è ancora una Quantum Operation.*

Dimostrazione. Fissate due decomposizioni di Kraus $\{E_k\}$, $\{F_j\}$ per $\mathcal{E}$ e $\mathcal{F}$ rispettivamente, dalla definizione di prodotto tensoriale discende in fretta:

$$\mathcal{E} \otimes \mathcal{F}(\rho) = \sum_{j,k} E_k \otimes F_j \rho E_k^\dagger \otimes F_j^\dagger$$

E inoltre si ha:

$$\sum_{j,k} E_k^\dagger \otimes F_j^\dagger \, E_k \otimes F_j = \sum_{j,k} E_k^\dagger E_k \otimes F_j^\dagger F_j \, =$$

$$= \sum_{j,k} E_k^\dagger E_k \otimes F_j^\dagger F_j \, = \sum_k E_k^\dagger E_k \otimes \sum_j F_j^\dagger F_j \, =$$

$$= I_{\mathcal{H}} \otimes I_{\mathcal{J}} = I_{\mathcal{H}\otimes\mathcal{J}}$$

Che completa la tesi. □

Le tre proposizioni appena dimostrate riguardano la formalizzazione di tre modi diversi di costruire una macchina quantistica a partire da altre due. La prima si interpreta fisicamente immaginando di fornire, come passaggio intermedio, l'uscita della prima macchina in ingresso alla seconda. In analogia

[2] Il prodotto tensoriale è ben definito, poichè $\mathcal{E}$ e $\mathcal{F}$ sono applicazioni lineari.

con l'elettronica, le due macchine si possono dire disposte *in serie*. La seconda descrive una macchina con una componente probabilistica: corrisponde ad applicare a ρ $\mathcal{E}$ con probabilità p e $\mathcal{F}$ con probabilità $(1-p)$. La terza consiste nel considerare un sistema di input che sia un sistema composto, nell'applicare una macchina ad un suo sottosistema ed un'altra al restante; gli output delle due macchine andranno a comporre l'output complessivo.

Queste dimostrazioni forniscono:

- La prova formale che, come ci si aspettava, le macchine così composte sono trattabili con il formalismo delle QO
- Il calcolo esplicito di una forma di Kraus della macchina composta a partire dalle forme di Kraus delle componenti.

I gradi di libertà nella scelta delle rappresentazioni di Kraus e delle realizzazioni unitarie associate ad una Quantum Operation suggeriscono la possibilità dell'esistenza di apparati che, pur non essendo fisicamente decomponibili in sottomacchine, come Quantum Operation sono del tutto equivalenti a macchine composte.

1.2 Forma operatoriale

Lemma 1.1 *$R \in \mathcal{B}(\mathcal{H}\otimes\mathcal{K})$ è un operatore positivo se e solo se esiste un insieme di vettori (non normalizzati) $\{|E_k\rangle\!\rangle\} \subset \mathcal{H}\otimes\mathcal{K}$ tale che $R = \sum_k |E_k\rangle\!\rangle\langle\!\langle E_k|$.*

Dimostrazione. (Se) Poniamo $R = \sum_k |E_k\rangle\!\rangle\langle\!\langle E_k|$.Allora per ogni $|\Psi\rangle\!\rangle \in \mathcal{H}\otimes\mathcal{K}$ si ha

$$\langle\!\langle\Psi|R|\Psi\rangle\!\rangle = \sum_k \langle\!\langle\Psi|E_k\rangle\!\rangle\langle\!\langle E_k|\Psi\rangle\!\rangle = \sum_k |\langle\!\langle E_k|\Psi\rangle\!\rangle|^2 \geq 0,$$

che equivale alla positività di R.

(Solo se) Se R è positivo, allora per il teorema spettrale è anche diagonalizzabile. Quindi esiste un set ortonormale $\{|R_i\rangle\rangle\} \subset \mathcal{H} \otimes \mathcal{K}$ tale che sia:

$$R = \sum_i r_i \, |R_i\rangle\rangle\langle\langle R_i|$$

Ponendo $|E_i\rangle\rangle \doteq \sqrt{r_i}|R_i\rangle\rangle$ la precedente si può riscrivere

$$R = \sum_i |E_i\rangle\rangle\langle\langle E_i|$$

□

Lemma 1.2 *Sia $R = \sum_k |E_k\rangle\rangle\langle\langle E_k|$. Allora vale:*

$$\mathrm{Tr}_{\mathcal{K}}[R] = \left(\sum_k E_k^\dagger E_k \right)^T \tag{1.15}$$

In cui l'operazione di trasposizione è effettuata sulla stessa base che si è usata per costruire l'isomorfismo che associa gli E_k ai $|E_k\rangle\rangle$.

Nota. Si fissi una base in $\mathcal{H}$. Per il resto del capitolo considereremo tutte le operazioni algebriche dipendenti dalla base (in particolare proprio l'operatore di trasposizione $\cdot^T$ e l'isomorfismo tra spazi vettoriali che mappa operatori appartenenti a $\mathcal{B}(\mathcal{K}, \mathcal{H})$ in vettori di $\mathcal{K} \otimes \mathcal{H}$) come riferite a questa, senza bisogno di ulteriori specificazioni.

Dimostrazione. Per definizione abbiamo

$$|E_k\rangle\rangle = \sum_{m,n} \langle m|E_k|n\rangle |m\rangle|n\rangle$$

Sostituendo

$$\mathrm{Tr}_{\mathcal{K}}[R] = \mathrm{Tr}_{\mathcal{K}} \left[\sum_{k,m,n,m',n'} \langle m|E_k|n\rangle \langle n'|E_k^\dagger|m'\rangle |m\rangle|n\rangle\langle m'|\langle n'| \right]$$

Esplicitando la traccia:

$$\mathrm{Tr}_{\mathcal{K}}[R] = \sum_{k,m,n,m',n',i} \langle m|E_k|n\rangle\langle n'|E_k^\dagger|m'\rangle|n\rangle\langle n'|\langle m'|i\rangle\langle i|m\rangle$$

Eseguendo la somma su i e su m'

$$\mathrm{Tr}_{\mathcal{K}}[R] = \sum_{k,m,n,n'} \langle m|E_k|n\rangle\langle n'|E_k^\dagger|m\rangle\,|n\rangle\langle n'|$$

Eseguendo ora quella su m

$$\mathrm{Tr}_{\mathcal{K}}[R] = \sum_{k,m,n,n'} \langle n|E_k^\dagger E_k|n'\rangle|n\rangle\langle n'| = \sum_k (E_k^\dagger E_k)^T$$

Dato che la trasposizione è distributiva rispetto alla somma, otteniamo

$$\mathrm{Tr}_{\mathcal{K}}[R] = \left(\sum_k E_k^\dagger E_k\right)^T,$$

soddisfacendo la tesi. □

Proposizione 1.8 *Ad ogni Quantum Operation $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$ si può associare un operatore $R_{\mathcal{E}} \in \mathcal{B}(\mathcal{K} \otimes \mathcal{H})$ tramite l'applicazione lineare*

$$R_{\mathcal{E}} = \mathcal{E} \otimes \mathcal{I}(|I\rangle\rangle\langle\langle I|) \tag{1.16}$$

in cui $\mathcal{I}$ è l'operatore identico in $\mathcal{B}(\mathcal{B}(\mathcal{H}))$, e I è l'identità su $\mathcal{H}$. $R_{\mathcal{E}}$ è positivo e soddisfa la condizione

$$\mathrm{Tr}_{\mathcal{K}}[R_{\mathcal{E}}] = I_{\mathcal{H}} \tag{1.17}$$

Dimostrazione. $\mathcal{E}$ ammette qualche decomposizione di Kraus $\{E_k\}$, mentre $\mathcal{I}$ si rappresenta sulla decomposizione banale data da $\{I_{\mathcal{H}}\}$. Questo permette di calcolare agevolmente $R_{\mathcal{E}}$; infatti si ha:

$$R_{\mathcal{E}} = \sum_k (E_k \otimes I_{\mathcal{H}})|I\rangle\rangle\langle\langle I|(E_k^\dagger \otimes I_{\mathcal{H}}) = \sum_k |E_k\rangle\rangle\langle\langle E_k| \tag{1.18}$$

. Da cui per il lemma 1.1 discende immediatamente la positività di R. Passiamo ora a dimostrare la (1.17). Per i lemma 1.2 $\mathrm{Tr}_{\mathcal{K}}\left[R_{\mathcal{E}}\right] = \left(\sum_k E_k^\dagger E_k\right)^T$, ma – costituendo una decomposizione di Kraus – $\{E_k\}$ verifica la relazione di completezza (1.11), e di conseguenza la (1.17). □

Proposizione 1.9 *L'applicazione* (1.16) *è suriettiva sul codominio*

$$\mathcal{R} \doteq \{R \in \mathcal{B}(\mathcal{K}\otimes\mathcal{H}) : \langle\phi|R|\phi\rangle \geq 0 \forall |\phi\rangle \in \mathcal{K}\otimes\mathcal{H}, \quad \mathrm{Tr}_{\mathcal{K}}\left[R\right] = I_{\mathcal{H}}\} \quad (1.19)$$

Dimostrazione. Se $R \in \mathcal{R}$, per i lemmi 1.1 e 1.2 esiste una decomposizione di Kraus $\{E_k\} \subset \mathcal{B}(\mathcal{H},\mathcal{K})$ tale che $R = \sum_k |E_k\rangle\rangle\langle\langle E_k|$. Se $\mathcal{E}$, definita da $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$, è la quantum operation a cui è associata la decomposizione $\{E_k\}$, è immediato verificare, tramite il procedimento che porta alla (1.18), che $R_{\mathcal{E}} = R$. □

Proposizione 1.10 *La mappa lineare da* $\mathcal{B}(\mathcal{K}\otimes\mathcal{H})$ *in* $\mathcal{B}(\mathcal{B}(\mathcal{H}),\mathcal{B}(\mathcal{K}))$ *definita come segue*

$$\mathcal{E}_R(\rho) = \mathrm{Tr}_{\mathcal{H}}\left[I\otimes\rho^T R\right] \quad (1.20)$$

costituisce un'inversa a sinistra dell'applicazione (1.16).

Dimostrazione. La tesi equivale a richiedere

$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathcal{H}}\left[I\otimes\rho^T R_{\mathcal{E}}\right]; \quad (1.21)$$

basterà quindi dimostrare che è sempre verificata. Cominciamo sostituendo l'espressione esplicita di $R_{\mathcal{E}}$ in funzione di $\mathcal{E}$:

$$\mathrm{Tr}_{\mathcal{H}}\left[I\otimes\rho^T R_{\mathcal{E}}\right] = \mathrm{Tr}_{\mathcal{H}}\left[I\otimes\rho^T\mathcal{E}\otimes\mathcal{I}(|I\rangle\rangle\langle\langle I|)\right];$$

espandendo $|I\rangle\rangle\langle\langle I|$ e $\rho = \rho_{ij}|i\rangle\langle j|$, ed eseguendo le dovute moltiplicazioni tra operatori si ottiene:

$$\mathrm{Tr}_{\mathcal{H}}\left[I\otimes\rho^T R_{\mathcal{E}}\right] = \mathrm{Tr}_{\mathcal{H}}\left[\sum_{i,j,m,n}\mathcal{E}(|m\rangle\langle n|)\otimes\rho_{ji}|i\rangle\langle j|m\rangle\langle n|\right];$$

Tracciando si ha infine:

$$\mathrm{Tr}_{\mathcal{H}}\left[I \otimes \rho^T R_{\mathcal{E}}\right] = \sum_{m,n} \mathcal{E}(|m\rangle\langle n|) \otimes \rho_{mn}$$

che ricordando la linearità di $\mathcal{E}$ diventa proprio la (1.21). □

Proposizione 1.11 *La* (1.16)*, intesa come applicazione dallo spazio delle operazioni quantistiche da* $\mathcal{B}(\mathcal{H})$ *in* $\mathcal{B}(\mathcal{K})$ *nello spazio* $\mathcal{R}$ *definito dalla* (1.19)*, è biiettiva.*

Dimostrazione. Una funzione che ammette inversa a sinistra è iniettiva[3]. Quindi la (1.16) è iniettiva per la proposizione 1.10, e suriettiva per la proposizione 1.9.□

Possiamo riassumere quanto dimostrato fin qui in questa sezione con il seguente enunciato:

Teorema 1.1 *Sia* $\mathcal{QO}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ *l'insieme delle quantum operation da* $\mathcal{B}(\mathcal{H})$ *in* $\mathcal{B}(\mathcal{K})$*. Allora la mappa*

$$R_\cdot : \mathcal{QO}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K})) \to \{R \in \mathcal{B}(\mathcal{K} \otimes \mathcal{H}) : \langle\phi|R|\phi\rangle \geq 0 \quad \forall|\phi\rangle \in \mathcal{K} \otimes \mathcal{H}, \mathrm{Tr}\,\mathcal{K}R = I_{\mathcal{H}}\}$$

definita da

$$R_{\mathcal{E}} = \mathcal{E} \otimes \mathcal{I}(|I\rangle\rangle\langle\langle I|) \tag{1.22}$$

(dove $\mathcal{I} \in \mathcal{EB}(\mathcal{H}), \mathcal{B}(\mathcal{H})$ *è la quantum operation identica su* $\mathcal{B}(\mathcal{H})$ *e* I *l'identità su* $\mathcal{H}$*) costituisce una corrispondenza biunivoca. Inoltre la sua inversa si scrive:*

$$\mathcal{E}_R(\rho) = \mathrm{Tr}_{\mathcal{H}}\left[(I \otimes \rho^T)R\right] \tag{1.23}$$

[3]Infatti, dati due insiemi A e B, siano $f : A \to B, g : B \to A$ tali che $\forall a \in A g(f(a)) = a$. Allora, posti $a, b \in A : f(a) = f(b)$, si ha $a = g(f(a)) = g(f(b)) = b$.

Questo risultato, noto da tempo in letteratura [6][7], è il più rilevante tra quelli presenti in questo capitolo, perchè fornisce una caratterizzazione delle QO particolarmente utile. Questo non solo per la biunivocità della corrispondenza, proprietà che del resto è condivisa anche dalla caratterizzazione tramite mappe completamente positive, di cui si tratterà nella prossima sezione, ma anche e soprattutto perchè particolarmente adatta allo studio di alcuni problemi significativi, quali quelli di ottimizzazione covariante.

1.3 Mappe CP

Definizione. Una mappa lineare $\mathcal{E} \in \mathcal{B}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ si dice **completamente positiva** se e solo se per qualsiasi spazio di Hilbert $\mathcal{J}$, l'applicazione $\mathcal{E} \otimes \mathcal{I}_{\mathcal{J}}$, dove $\mathcal{I}_{\mathcal{J}}$ è l'identità in $\mathcal{B}(\mathcal{B}(\mathcal{J}))$, mappa operatori positivi in operatori positivi. In letteratura si indicano le mappe completamente positive anche con le abbreviazioni di **CP-Map** o **Mappe CP**.

Definizione. Sia $\mathcal{E} \in \mathcal{B}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ una mappa completamente positiva. Se per ogni $\rho \in \mathcal{B}(\mathcal{H})$ vale $\mathrm{Tr}\left[\mathcal{E}(\rho)\right] = \mathrm{Tr}\left[\rho\right]$ diremo che $\mathcal{E}$ è **trace-preserving**, o che conserva la traccia.

Nota. In questa trattazione siamo interessati esclusivamente a mappe che conservano la traccia; quindi d'ora in poi sottointenderemo la proprietà di conservazione della traccia nel fare riferimento a mappe CP, salvo dove specificato diversamente.

Allo stesso modo, chiamiamo $\mathcal{CP}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ l'insieme delle CP-Map trace-preserving da $\mathcal{B}(\mathcal{H})$ in $\mathcal{B}(\mathcal{K})$.

Teorema 1.2 *Per $\mathcal{H}$, $\mathcal{K}$ spazi di Hilbert a dimensione finita, si ha*

$$\mathcal{CP}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K})) = \mathcal{QO}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$$

Dimostrazione. Poniamo per semplicità di notazione $\mathcal{CP} \doteq \mathcal{CP}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ e $\mathcal{QO} \doteq \mathcal{QO}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$.

Cominciamo col dimostrare che $\mathcal{QO} \subseteq \mathcal{CP}$. Se $\mathcal{E} \in \mathcal{B}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ è una Quantum Operation, la proposizione 1.7 ne garantisce la completa positività in senso stretto. Gli altri assiomi (la conservazione della traccia e, implicitamente, la linearità) delle mappe CP sono verificati dalle Quantum Operation per definizione.

Prendiamo ora in considerazione l'applicazione $\mathcal{E} \mapsto R_{\mathcal{E}}$ da $\mathcal{B}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ in $\mathcal{B}(\mathcal{K} \otimes \mathcal{H})$, definita dall'equazione (1.16). Essa costituisce per costruzione l'estensione a tutto $\mathcal{B}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ della corrispondenza biunivoca $\mathcal{QO} \leftrightarrow \mathcal{R}$ definita nella precedente sezione; è a sua volta biunivoca, con inversa data dalla (1.20) (si veda la dimostrazione della proposizione (1.10)), per cui dati due sottoinsiemi di $\mathcal{B}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ $\mathcal{R}$ e $\mathcal{S}$, si ha che $\mathcal{R}$ e $\mathcal{S}$ coincidono se e solo se coincidono le loro immagini tramite R. $R_{\mathcal{R}}$ e $R_{\mathcal{S}}$.

Andiamo a studiare l'immagine $R_{\mathcal{CP}}$ di $\mathcal{CP}$. Osserviamo subito che, data la positività di $|I\rangle\rangle\langle\langle I|$, $\mathcal{E} \in \mathcal{CP}$ implica che $R_{\mathcal{E}}$ sia positivo. Imponendo il vincolo di conservazione della traccia si trova:

$$\mathrm{Tr}\left[\rho\right] = \mathrm{Tr}\left[I_{\mathcal{K}} \otimes \rho^T R_{\mathcal{E}}\right] = \mathrm{Tr}_{\mathcal{H}}\left[\rho^T \,\mathrm{Tr}_{\mathcal{K}}\left[R_{\mathcal{E}}\right]\right]$$

che valendo per tutti i ρ impone su $R_{\mathcal{E}}$ il vincolo $\mathrm{Tr}_{\mathcal{K}}\left[R_{\mathcal{E}}\right] = I_{\mathcal{H}}$. Quindi abbiamo che $R_{\mathcal{CP}} \subseteq \mathcal{R} = R_{\mathcal{QO}}$. Ma visto che $\mathcal{QO} \subseteq \mathcal{CP}$, abbiamo anche $R_{\mathcal{QO}} \subseteq R_{\mathcal{CP}}$. Allora possiamo affermare $R_{\mathcal{QO}} = R_{\mathcal{CP}}$, il che implica la tesi. □

1.4 Alcune macchine quantistiche notevoli

1.4.1 Traccia parziale

Supponiamo di avere un sistema composto, rappresentato sullo spazio di Hilbert $\mathcal{H} \otimes \mathcal{K}$, e di scartare il sottosistema $\mathcal{H}$.

Un operazione quantistica che rappresenta un processo di questo tipo è:

$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathcal{H}}\left[\rho\right].$$

Notiamo come questa scrittura costituisca già di per sé una realizzazione unitaria di $\mathcal{E}$, con $\mathcal{A} \doteq \mathbb{C}$ e $U \doteq I_{\mathcal{H}\otimes\mathcal{K}}$.

Tenendo questo fatto in considerazione è semplice costruire la rappresentazione di Kraus. Fissata una base $\{|i\rangle\}$ in $\mathcal{H}$, basta porre gli elementi della rappresentazione:

$$E_i \doteq I_{\mathcal{K}} \otimes \langle i|$$

per i quali si trova subito $\sum_i E_i \rho E_i^\dagger = \sum_k I_{\mathcal{K}} \otimes \langle i|\rho|i\rangle \otimes I_{\mathcal{K}} = \mathrm{Tr}_{\mathcal{H}}\left[\rho\right] = 1$.

A partire dalla decomposizione di Kraus è immediato scrivere R:

$$R = \sum_i |E_i\rangle\rangle\langle\langle E_i| = |I_{\mathcal{K}}\rangle\rangle\langle\langle I_{\mathcal{K}}| \otimes \sum_i |i\rangle\langle i| = |I_{\mathcal{K}}\rangle\rangle\langle\langle I_{\mathcal{K}}| \otimes I_{\mathcal{H}}$$

1.4.2 Preparazione

La preparazione di un sistema in uno stato fissato σ è un processo fisico largamente praticato in laboratorio, senza il quale non sarebbero possibili molti esperimenti. Si rappresenta immediatamente, senza bisogno di costruzioni, come CP-Map da $\mathcal{B}(\mathcal{H})$ in $\mathcal{B}(\mathcal{K})$, scrivendo

$$\mathcal{E}(\rho) = \sigma \qquad \forall \rho \text{ stato in } \mathcal{B}(\mathcal{H}).$$

Si può costruire facilmente una rappresentazione di Kraus opportuna. In generale lo stato σ si diagonalizza in una combinazione convessa di stati puri; poniamo, fissata la solita base ortonormale $\{|i\rangle\}$ su $\mathcal{H}$:

$$E_{i,j} \doteq \sqrt{p_j}|\psi_j\rangle\langle i|, \tag{1.24}$$

con i p_j e $|\psi_j\rangle$ tali che $\sigma = \sum_j p_j|\psi_j\rangle\langle\psi_j|$. Si verifica immediatamente che $\{E_i\}$ è una decomposizione di Kraus per $\mathcal{E}$: $\sum_{i,j} E_{i,j}\rho E_{i,j}^\dagger = \sum_{i,j} p_j\langle i|\rho|i\rangle|\psi_j\rangle\langle\psi_j| = \left(\sum_j p_j|\psi_j\rangle\langle\psi_j|\right)\left(\sum_i\langle i|\rho|i\rangle\right) = \sigma$

Calcoliamo l'operatore R associato:

$$R = \sum_{i,j} |E_{i,j}\rangle\rangle\langle\langle E_{i,j}| = \sum_{i,j} p_j |\psi_j\rangle\langle\psi_j| \otimes |i\rangle\langle i| = \sigma \otimes I_{\mathcal{H}}.$$

1.4.3 Misura

Anche il processo di misurazione di un'osservabile, nonostante il suo carattere particolare[2][4][3], si può descrivere tramite una Quantum Operation. Sia O un osservabile su $\mathcal{H}$, $O = \sum_i o_i P_i$ una sua spettralizzazione, con $o_i = o_j \iff i = j$. Dalla meccanica statistica sappiamo che se il sistema rappresentato da $\mathcal{H}$ si trova in uno stato ρ, effettuare una misurazione di O lo porterà nello stato

$$\mathcal{E}(\rho) = \sum_i P_i \rho P_i.$$

Questa evoluzione è già scritta nella forma di Kraus! Infatti $\sum_i P_i^\dagger P_i = \sum_i P_i = I_{\mathcal{H}}$, perchè $\{P_i\}$ è per costruzione una risoluzione dell'identità.

L'operatore R associato si scrive:

$$R = \sum_i |P_i\rangle\rangle\langle\langle P_i|$$

Se scegliamo una base su cui O è diagonale per costruire la mappa $P_i \mapsto |P_i\rangle\rangle$, troviamo che ciascun $|P_i\rangle\rangle$ è proporzionale a un vettore massimamente entangled su $\mathcal{H}_i \otimes \mathcal{H}_i$, in cui con $\mathcal{H}_i$ si è designato l'autospazio corrispondente a o_i.

Abbiamo qua considerato solo il caso più semplice: esistono trattazioni più raffinate dei processi di misurazione tramite le Quantum Operation [4][3], che introducono il concetto di strumento e prendono in considerazione una classe di misurazioni più ampia di quella descritta dalle osservabili autoaggiunte. Estendendo il concetto di Quantum Operation a comprendere anche applicazioni che non conservano necessariamente la traccia, è possibile usare questo formalismo anche per trattare la *state-reduction*. Per le mac-

chine quantistiche però è sufficiente, come abbiamo visto, limitarsi al caso *trace-preserving*.

1.4.4 Teletrasporto

Un'applicazione molto nota della quantum information è il cosiddetto teletrasporto quantistico, teorizzato da Bennet, Brassard, Crépeau, Jozsa, Peres e Wootters nel 1993 [9] e realizzato sperimentalmente per la prima volta dalle équipe guidate da Zeilinger a Vienna e da De Martini a Roma tra il 1997 e il 1998 [10][11].

Il teletrasporto consiste nel trasferire lo stato di un sistema su di un altro sistema equivalente senza porli direttamente in interazione. A grandi linee, lo schema è questo: si fa opportunamente interagire lo stato del primo sistema con un membro di una coppia EPR, e si effettua una misura opportuna sul sistema composto dai due. A questo punto, effettuando una trasformazione unitaria dipendente dal risultato della misura sul secondo membro della coppia si ottiene lo stato di partenza. Descrizioni si possono trovare in [1][9][10][11].

A noi interessa andare a descrivere il teletrasporto nel formalismo delle QO. Sarà rappresentato da una CP-Map da $\mathcal{B}(\mathcal{H})$ in $\mathcal{B}(\mathcal{H})$ della forma

$$\mathcal{E}(\rho) = \rho.$$

Quella appena scritta è la CP-Map identica; ammette una decomposizione di Kraus banale $\{I_{\mathcal{H}}\}$, e in rappresentazione operatoriale si scrive $R = |I\rangle\rangle\langle\langle I|$.

Come abbiamo già accennato, la CP-Map identica rappresenta in modo molto intuitivo un altro processo fisico: il "processo nullo" che consiste nel lasciare semplicemente il sistema inalterato. Il fatto che due operazioni molto diverse, una delle quali tecnica, che si attua con tecniche sperimentali non banali, e che si fonda su effetti fisici prettamente quantistici come l'entanglement, mentre la seconda pensabile anche in fisica classica e realizzabile

senza nessun apparato, siano rappresentate dalla stessa Quantum Operation dovrebbe rendere chiaro il grado di astrazione introdotto da questo strumento concettuale.

Capitolo 2

Quantum Operation Covarianti

La presenza di simmetrie è una caratteristica diffusamente condivisa dalla maggior parte delle leggi fisiche. Lo studio di tali simmetrie si è rivelato particolarmente fruttuoso ed ad esso si possono ricondurre alcune tra le più fondamentali scoperte della fisica moderna, a cominciare dalla stessa relatività Galileiana.

Le leggi fisiche si esprimono tramite relazioni tra grandezze misurabili, permettendo di prevedere la statistica di esperimenti riguardanti tali grandezze. Si dice che una legge fisica presenta simmetria rispetto a una certa trasformazione quando descrive esperimenti i cui risultati non cambiano applicando questa trasformazione congiuntamente al sistema fisico misurato e all'osservatore. Una trasformazione che verifica questa proprietà si dice simmetria della legge in questione. A partire da questa definizione, è intuitivo vedere come l'insieme delle simmetrie di una data legge fisica abbia struttura di gruppo rispetto all'applicazione successiva di due trasformazioni. Una legge che ammette un gruppo di simmetria si dice *covariante* rispetto al gruppo in questione. Un singolo sistema fisico invece è simmetrico.

Le trasformazioni fisiche di cui si sta parlando ammetteranno ovviamente una descrizione matematica come endomorfismi dello spazio degli stati. Una Quantum Operation è un'applicazione da stati in stati: è facile vedere come

il concetto di covarianza si possa estendere anche alle Quantum Operation, che pure sono descrizioni di processi fisici specifici e non leggi universali. Nel presente capitolo le si descriverà matematicamente, e le si considererà come candidate all'approssimazione di macchine ideali.

Si può dimostrare che ad ogni macchina quantistica in cui la dinamica del sistema chiuso input+apparato+output ammetta un gruppo di simmetria si associa una Quantum Operation covariante rispetto allo stesso gruppo. Il principio di relatività si può esprimere come l'imposizione di opportuni[1] gruppi di simmetria per la dinamica di sistemi chiusi. Quindi, se si accetta una qualsiasi variante del principio di relatività, si devono assumere le quantum operation non covarianti come non fisiche.

2.1 Definizioni preliminari.

Gli strumenti matematici per trattare le simmetrie in meccanica quantistica si appoggiano alla teoria delle rappresentazioni dei gruppi sugli spazi di Hilbert. Trattandosi di un capitolo fondamentale della fisica matematica, i cui rudimenti sono oggi largamente conosciuti, non si è ritenuto necessario dilungarsi in una sua presentazione. Testi di riferimento molto diffusi sono il libro di Jones [12] e quello di Hammermesh [13].

Definizione. Sia $\mathcal{E} \in \mathcal{QOB}(\mathcal{H}), \mathcal{B}(\mathcal{K})$, e siano $\{U_g\}$, $\{V_g\}$ rappresentazioni unitarie di un medesimo gruppo $\mathcal{G}$ su $\mathcal{H}$ e $\mathcal{K}$, rispettivamente. Diremo che $\mathcal{E}$ è **covariante** rispetto a $\{U_g\}$ e $\{V_g\}$ se per ogni stato di $\mathcal{H}$ e per ogni elemento g del gruppo vale:

$$\mathcal{E}(U_g \rho U_g^\dagger) = V_g \mathcal{E}(\rho) V_g^\dagger$$

[1] Più precisamente, il gruppo di Galileo per la relatività Galileiana e quello di Poincaré per la relatività Einsteiniana speciale.

Teorema 2.1 *$\mathcal{E} \in \mathcal{QO}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}),)$ è covariante rispetto alle rappresentazioni unitarie $\{U_g\} \subset \mathcal{B}(\mathcal{H})$ e $\{V_g\} \subset \mathcal{B}(\mathcal{K})$ se e solo l'operatore positivo $R_\mathcal{E}$ ad essa associato è invariante rispetto alla rappresentazione $\left\{V_g \otimes U_g^*\right\}$, cioè se e solo se si ha*

$$[R_\mathcal{E}, V_g \otimes U_g^*] = 0$$

In cui l'operazione di coniugazione complessa è riferita alla stessa base su cui si è costruito R.

Dimostrazione. La condizione di covarianza su $\mathcal{E}$ si può riscrivere in termini di $R_\mathcal{E}$

$$\mathrm{Tr}_\mathcal{H}\left[I \otimes U_g^* \rho^T U_g^T R_\mathcal{E}\right] = V_g \,\mathrm{Tr}_\mathcal{H}\left[I \otimes \rho^T R_\mathcal{E}\right] V_g^\dagger \qquad \forall \rho$$

che equivale a

$$V_g^\dagger \,\mathrm{Tr}_\mathcal{H}\left[I \otimes U_g^* \rho^T U_g^T R_\mathcal{E}\right] V_g = \mathrm{Tr}_\mathcal{H}\left[I \otimes \rho^T R_\mathcal{E}\right] \qquad \forall \rho \tag{2.1}$$

Ricordando che $I \otimes U_g^* \rho^T U_g^T = (I \otimes U_g^*)(I \otimes \rho^T)(I \otimes U_g^T)$ e applicando la proprietà ciclica della traccia possiamo scrivere $\mathrm{Tr}_\mathcal{H}\left[I \otimes U_g^* \rho^T U_g^T R_\mathcal{E}\right] = \mathrm{Tr}_\mathcal{H}\left[(I \otimes \rho^T)(I \otimes U_g^T) R_\mathcal{E} I \otimes U_g^*\right]$. Sostituendo e portando i V_g e $V_g^\dagger$ dentro la traccia, la (2.1) si riscrive:

$$\mathrm{Tr}_\mathcal{H}\left[I \otimes \rho^T (V_g^\dagger \otimes U_g^T R_\mathcal{E} V_g \otimes U_g^*)\right] = \mathrm{Tr}_\mathcal{H}\left[I \otimes \rho^T R_\mathcal{E}\right] \qquad \forall \rho,$$

che per la biiettività della corrispondenza $\mathcal{E} \leftrightarrow R_\mathcal{E}$ è verificata se e solo se $V_g^\dagger \otimes U_g^T R_\mathcal{E} V_g \otimes U_g^* = R_\mathcal{E}$. Quest'ultima condizione si può anche scrivere (moltiplicando ambo i membri a sinistra per $V_g \otimes U_g^*$ e portando tutto al primo membro) $[R_\mathcal{E}, V_g \otimes U_g^*] = 0$. Tutti i passaggi eseguiti sono coimplicazioni. □

Questa forma della condizione di covarianza, espressa nei termini dell'invarianza di $R_\mathcal{E}$, risulta solitamente più semplice da verificare, data $\mathcal{E}$, di quella esposta nella definizione. La minore difficoltà è data non soltanto dal

fatto che la seconda condizione non richiede di essere verificata singolarmente per ogni $\rho \in \mathcal{B}(\mathcal{H})$, ma anche dal contenuto del seguente teorema:

Teorema 2.2 *Sia $\mathcal{H}$ uno spazio di Hilbert, R un operatore normale su $\mathcal{B}(\mathcal{H})$. R è invariante rispetto alla rappresentazione $U_g \subset \mathcal{B}(\mathcal{H})$ se e solo se i suoi autospazi sono spazi invarianti per U_g.*

Dimostrazione. (Solo se) Sia $\mathcal{H}_\lambda$ l'autospazio di R relativo all'autovalore λ. Allora, se R commuta con tutti gli U_g si trova:

$$\forall g \in \mathcal{G},\, \forall \lambda \in \sigma(R),\, \forall |\psi\rangle \in \mathcal{H}_\lambda \qquad RU_g|\psi\rangle) = U_g R|\psi\rangle = U_g \lambda|\psi\rangle = \lambda U_g|\psi\rangle$$

da cui consegue per definizione di $\mathcal{H}_\lambda$:

$$\forall \lambda \in \sigma(R),\, \forall g \in \mathcal{G} \qquad U_g \mathcal{H} = \mathcal{H}$$

(Se) Supponiamo che tutti gli autospazi di R siano invarianti per $\{U_g\}$. Sia $|\phi\rangle \in \mathcal{H}$ è un autovettore per l'autovalore λ. Banalmente si trova:

$$\forall g \in \mathcal{G} \qquad UR|\phi\rangle = U\lambda|\phi\rangle = \lambda U|\phi\rangle$$

Se supponiamo che tutti gli autospazi di R siano invarianti per $\{U_g\}$ si trova che $U|\phi\rangle$ è ancora autovettore di λ, da cui deduciamo:

$$\forall g \in \mathcal{G} RU_g|\phi\rangle = \lambda U_g|\phi\rangle$$

Per la proprietà transitiva dell'uguaglianza abbiamo quindi che per qualsiasi $|\phi\rangle$ autovettore di R e qualsiasi $g \in \mathcal{G}$ si ha $RU_g|\phi\rangle = U_g R|\phi\rangle$. Per il teorema spettrale esisterà una base $\{|\phi_i\rangle\}$ di autovettori di R; per cui, per ogni $|\psi\rangle \in \mathcal{H}$ posso scrivere:

$$RU_g|\psi\rangle = \sum_i \langle\phi_i|\psi\rangle RU_g|\phi_i\rangle = \sum_i \langle\phi_i|\psi\rangle U_g R|\phi_i\rangle = U_g R|\psi\rangle$$

che valendo per tutti i g equivale all'invarianza di R.□

Si deduce immediatamente che, nota la decomposizione di $\mathcal{K} \otimes \mathcal{H}$ in sottospazi invarianti per $V_g \otimes U_g^*$, diagonalizzare $R_\mathcal{E}$ sarà sufficiente a determinare se $\mathcal{E}$ sia o meno covariante rispetto a $\{U_g\}$ e $\{V_g\}$. Questa proprietà permette anche, fissate $\{U_g\}$ e $\{V_g\}$, di costruire una parametrizzazione degli $R_\mathcal{E}$ in termini di autovalori di $R_\mathcal{E}$ e di matrici unitarie sulle classi di equivalenza tra rappresentazioni irriducibili.

2.2 Massimizzazione covariante della fidelity.

2.2.1 Il problema dell'approssimazione ottimale

Sia $\mathcal{F}$ una generica applicazione tra stati in $\mathcal{B}(\mathcal{H})$ e stati in $\mathcal{B}(\mathcal{K})$. Nel precedente capitolo si sono viste tre diverse condizioni necessarie e sufficienti per la realizzabilità di $\mathcal{F}$:

- Esiste una decomposizione di Kraus $\{E_k\} \subset \mathcal{B}(\mathcal{H}, \mathcal{K})$ tale che $\mathcal{F}(\rho) = \sum_k E_k \rho E_k^\dagger$
- Esiste un operatore positivo $R \in \mathcal{B}(\mathcal{K} \otimes \mathcal{H})$ tale che $\mathrm{Tr}_\mathcal{K}[R] = I_\mathcal{H}$ e $\mathcal{F}(\rho) = \mathrm{Tr}_\mathcal{H}[(I_\mathcal{K} \otimes \rho)R]$
- Esiste una trace preserving CP-Map $\mathcal{E}$ da $\mathcal{B}(\mathcal{H})$ in $\mathcal{B}(\mathcal{K})$ tale che $\mathcal{E} = \mathcal{F}$

Se $\mathcal{F}$ non verifica esplicitamente nessuna delle tre condizioni, rimane comunque possibile cercare le quantum operation che meglio realizzano $\mathcal{F}$. Scelto un funzionale $E(\mathcal{E}, \mathcal{F})$ (non necessariamente lineare o bilineare) da $\mathcal{B}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ in $\mathbb{R}$ che misuri in qualche modo l' «efficienza» di $\mathcal{E}$ nell'approssimare $\mathcal{F}$, il problema si riduce a trovare i massimi globali di $E_\mathcal{F}(\mathcal{E}) \doteq E(\mathcal{E}, \mathcal{F})$. Inoltre, se si sceglie $E_\mathcal{F}$ in modo che $E_\mathcal{F} \leq 1$ e $E_\mathcal{F}(\mathcal{E}) = 1 \iff \mathcal{E} = \mathcal{F}$, una delle informazioni fornite dalla ricerca del massimo sarà l'appartenenza o meno di $\mathcal{F}$ all'insieme delle Quantum Operation.

In certe applicazioni non interessa che $\mathcal{E}$ approssimi bene $\mathcal{F}$ per tutti gli stati di input possibili, ma solo per un sottoinsieme $\mathcal{S} \subset \mathcal{B}(\mathcal{H})$ dato. Intuitivamente, questo introduce dei gradi di libertà ulteriori, dato che non ci interessa il valore di $\mathcal{E}$ fuori da $\mathcal{S}$, e si deve avere che l'efficienza ottimale rispetto alla richiesta più forte non sia maggiore di quella rispetto alla richiesta più debole. Bisognerà tenere conto anche di questo fattore nella scelta del funzionale appropriato.

2.2.2 Fidelity

Un funzionale adatto a descrivere l'efficienza con cui una quantum operation realizza un'applicazione tra stati è la cosiddetta fidelity tra mappe. Esistono diverse definizioni della fidelity tra mappe, non sempre equivalenti, ma tutte la costruiscono a partire da un funzionale analogo definito sugli stati.

Definizione. Sia $\mathcal{H}$ uno spazio di Hilbert. Chiameremo **fidelity** tra due stati $\rho, \sigma \in \mathcal{B}(\mathcal{H})$ il seguente funzionale:

$$F(\rho, \sigma) = \left(\mathrm{Tr} \left[\sqrt{\sigma^{\frac{1}{2}} \rho \sigma^{\frac{1}{2}}} \right] \right)^2$$

Per la fidelity tra stati valgono le seguenti proprietà. Per la loro dimostrazione si faccia riferimento al testo di Nielsen e Chuang [1].

- La fidelity tra due stati è compresa tra zero e uno:

$$\forall \rho, \sigma \text{ stati in } \mathcal{B}(\mathcal{H}) 0 \qquad \leq F(\rho, \sigma) \leq 1$$

- $$F(\rho, \sigma) = 1 \iff \rho = \sigma$$

- La fidelity tra stati è simmetrica in σ e ρ, ossia

$$\forall \rho, \sigma \text{ stati in } \mathcal{B}(\mathcal{H}) \qquad F(\rho, \sigma) = F(\sigma, \rho)$$

La fidelity tra stati è invariante per trasformazioni unitarie su $\mathcal{H}$. Cioè per ogni operatore unitario $U \in \mathcal{B}(\mathcal{H})$

$$\forall \rho, \sigma \text{ stati in } \mathcal{B}(\mathcal{H}) \qquad F(U\rho U\dagger, U\sigma U^\dagger) = F(\rho, \sigma)$$

enditemize

2.3 Covarianza forte

Consideriamo le Quantum Operation da m in n sistemi tra loro identici. Una trasformazione di simmetria che agisca sull'intero Sia $R : \mathcal{H}^{\otimes m} \otimes \mathcal{H}^{\otimes n} \to \mathcal{H}^{\otimes m} \otimes \mathcal{H}^{\otimes n}$ l'operatore positivo associato ad una Quantum Operation da $\mathcal{H}^{\otimes m}$ in $\mathcal{H}^{\otimes n}$, e sia $\{U_g : g \in \mathcal{G}\}$ una rappresentazione unitaria su $\mathcal{H}$ del gruppo $\mathcal{G}$. Diciamo che la Quantum Operation è **covariante**[2] rispetto a $\mathcal{G}$ se si ha:

$$\forall g \in \mathcal{G} \qquad U_g^{\otimes n} \otimes U_g^{*\otimes m} R = R\, U_g^{\otimes n} \otimes U_g^{*\otimes m} \tag{2.3}$$

Posto $M = \max(m, n)$, R si può invece dire **fortemente covariante** se ammette una purificazione $|\psi_R\rangle \in \mathcal{H}^{\otimes M} \otimes \mathcal{H}^{\otimes M}$ tale che

$$\forall g \in \mathcal{G} \qquad U_g^{\otimes M} \otimes U_g^{*\otimes M} |\psi_R\rangle = e^{i\theta(g)} |\psi_R\rangle. \tag{2.4}$$

Come suggerito dalla nomenclatura, la condizione di covarianza forte è sufficiente a garantire la covarianza, ma non è vero il viceversa. Infatti, detto $\mathcal{A}$ il sistema di ancilla per la purificazione e posta la (2.4), per ogni $g \in \mathcal{G}$ si ha:

$$R = \mathrm{Tr}_{\mathcal{A}}\left[|\psi_R\rangle\langle\psi_R|\right] = \mathrm{Tr}_{\mathcal{A}}[U_g^{*\otimes M} \otimes U_g^{\otimes M} |\psi_R\rangle\langle\psi_R| U_g^{T\otimes M} \otimes U_g^{\dagger\otimes M}] \tag{2.5}$$

[2]Senza avere informazioni particolari sulla struttura del suo spazio di definizione e della rappresentazione $\{U_g\}$ di $\mathcal{G}$ agente su di esso, un generico operatore O [hermitiano] si dice **covariante** rispetto a $\{U_g\}$ se vale

$$\forall g \in \mathcal{G} \qquad U_g\, O = O\, U_g \tag{2.2}$$

Separando il contributo dell'ancilla, la rappresentazione totale si riscrive

$$U_g^{*\otimes M} \otimes U_g^{\otimes M} = U_g^{*\otimes m} \otimes U_g^{\otimes n} \otimes U_g^{*\otimes M-m} \otimes U_g^{\otimes M-n}$$

Sostituendo questo risultato nella (2.5) e usando le proprietà della traccia parziale rispetto ai prodotti tensoriali di operatori si può scrivere

$$R = U_g^{*\otimes m} \otimes U_g^{\otimes n} \operatorname{Tr}_{\mathcal{A}}[I \otimes U_g^{*\otimes M-m} \otimes U_g^{\otimes M-n} |\psi_R\rangle\langle\psi_R| I \otimes U_g^{T\otimes M-m} \otimes U_g^{\dagger\otimes M-n}] U_g^{T\otimes m} \otimes U_g^{\dagger\otimes n}$$

che moltiplicando a destra per $U_g^{*\otimes m} \otimes U_g^{\otimes n}$ e usando la proprietà ciclica della traccia diventa

$$R\, U_g^{*\otimes m} \otimes U_g^{\otimes n} = U_g^{*\otimes m} \otimes U_g^{\otimes n} \operatorname{Tr}_{\mathcal{A}}[|\psi_R\rangle\langle\psi_R|] = U_g^{*\otimes m} \otimes U_g^{\otimes n}\, R, \qquad (2.6)$$

espressione verificata $\forall g$ e pertanto equivalente alla (2.3).

Per verificare come la condizione di covarianza semplice (2.3) non sia sufficiente a garantire la covarianza forte, basta notare che quest'ultima richiede $\operatorname{Rank} R \leq |m-n| \cdot \dim \mathcal{H}$ affinché la purificazione possa assumere la dimensione adeguata, mentre R può in generale avere anche un rango maggiore.[3]

Nicolas Cerf ha proposto su basi euristiche di cercare le soluzioni ai comuni problemi di ottimizzazione sulle Quantum Operation covarianti tra quelle che soddisfano la condizione di covarianza forte. In tutti i problemi affrontati finora con entrambi gli approcci, i risultati ottenuti sono compatibili. Sembra quindi di potenziale interesse indagare i rapporti tra le due condizioni, o

[3] La condizione

$$\operatorname{Tr}_{Out}[R] \leq \mathbb{I}_{In} \quad , \qquad (2.7)$$

per cui a un operatore positivo R corrisponde una CP-map *trace-not-increasing* e quindi dotata di senso fisico, non pone limiti sul rango di R. Infatti è semplice verificare che, per ogni operatore positivo O, $R \doteq \operatorname{Tr}[O]^{-1} O$ verifica (2.7). Siccome la moltiplicazione per uno scalare non modifica il rango, possiamo facilmente costruire CP-map per cui si ha $\operatorname{Rank} R = (m+n) \cdot \dim \mathcal{H} > |m-n| \cdot \dim \mathcal{H}$ (come esempio banale, si pensi a quella ottenuta ponendo $O = \mathbb{I}$ nel procedimento appena esposto.)

tra CP-map fortemente covarianti e classi di soluzioni ai problemi di ottimizzazione, in particolare in considerazione del significato fisico della condizione di covarianza forte in termini di realizzazioni della CP-Map.Un primo, piccolo passo in questa direzione può essere dato dai seguenti risultati:

Proposizione 2.1 *Sia R un operatore positivo da $\mathcal{H}$ in $\mathcal{H}$, covariante (nel senso di (2.2)) rispetto all'azione $\{U_g\}$ su $\mathcal{H}$ del gruppo $\mathcal{G}$. Esistono allora una purificazione $|\psi_R\rangle$ di R e una rappresentazione $\{V_g\}$ di $\mathcal{G}$ sullo spazio ancillare tali che*

$$\forall g \in \mathcal{G} \qquad U_g \otimes V_g |\psi_R\rangle = |\psi_R\rangle \tag{2.8}$$

Inoltre, si puo' sempre costruire la purificazione in modo che $V_g = U_g^*$.

Dimostrazione R è un operatore positivo, quindi si può scrivere nella forma diagonale

$$R = \sum_{i=1}^{\dim \mathcal{H}} r_i |i\rangle\langle i| \tag{2.9}$$

con tutti gli r_i reali non negativi. Allora una purificazione banale di R in $\mathcal{H} \otimes \mathcal{H}$ è

$$|\psi_R\rangle = \sum_{i=1}^{\dim l\mathcal{H}} \sqrt{r_i} |i\rangle|i\rangle \tag{2.10}$$

Vogliamo dunque trovare una rappresentazione $\{V_g\}$ tale che sia

$$\forall g \in \mathcal{G} \qquad U_g \otimes V_g \sum_{i=1}^{\dim \mathcal{H}} \sqrt{r_i} |i\rangle|i\rangle = \sum_{i=1}^{\dim \mathcal{H}} \sqrt{r_i} |i\rangle|i\rangle \tag{2.11}$$

ovvero

$$\forall g \in \mathcal{G} \qquad \sum_{i,j,k=1}^{\dim \mathcal{H}} \sqrt{r_i} u_{ij}^{(g)} v_{ik}^{(g)} |j\rangle|k\rangle = \sum_{i=1}^{\dim \mathcal{H}} \sqrt{r_i} |i\rangle|i\rangle \tag{2.12}$$

Ora basta notare che ponendo $V_g = U_g^*$, dove l'operazione di coniugazione complessa è stata effettuata rispetto alla base $\{|i\rangle\}$ si trova

$$\sum_{i=1}^{\dim \mathcal{H}} u_{ij}^{(g)} v_{ik}^{(g)} = \sum_{i=1}^{\dim \mathcal{H}} u_{ij}^{(g)} u_{ki}^{\dagger(g)} = \delta_{kj}, \tag{2.13}$$

che fatte le debite sostituzioni verifica banalmente la (2.12)□

Nota In questa costruzione, la scelta della rappresentazione sull'ancilla $\{V_g\}$ è dipendente da quella dell'operatore positivo da purificare. Infatti dipende, tramite la coniugazione complessa, dalla base su cui R è diagonale, e se $\{U_g\}$ contiene rappresentazioni irriducibili tra loro equivalenti l'algebra degli operatori postivi covarianti è non commutativa. Per cui potrebbe sembrare che analizzare lo spazio delle soluzioni della (2.8) non fornisca informazioni utili sulla varieta' degli operatori positivi covarianti in $\mathcal{H}$; dimostreremo invece nel seguito che la caratterizza completamente.

Osservazione 2.1 *Siano $\mathcal{H}$ spazio di Hilbert, $\{V_g\}$ rappresentazione unitaria su $\mathcal{H}$, $\{V_g^*\}$ e $\{V_g^{*'}\}$ rappresentazioni complesse coniugate di $\{V_g\}$ rispetto alle basi $\{|i\rangle\}$ e $\{|i'\rangle\}$ rispettivamente. Allora $\{V_g^*\}$ e $\{V_g^{*'}\}$ sono equivalenti, ossia:*

$$\exists S \in \mathbf{GL}(\mathcal{H}) : \forall g \in \mathcal{G} \qquad V_g^* = S^{-1} V_g^{*'} S \tag{2.14}$$

Dimostrazione Chiamiamo B la trasformazione che connette le due basi $\{|i\rangle\}$ e $\{|i'\rangle\}$. Si ha:

$$V_g^{*'} = B(B^{-1} V_g B)^* B^{-1}$$

che per la distributività di * diventa

$$V_g^{*'} = B B^{-1*} V_g^* B^* B^{-1} \qquad ,$$

sostituendo nella quale

$$S = B^* B^{-1} \tag{2.15}$$

si ottiene la (2.14) □

Osservazione 2.2 *Siano $\mathcal{H}$, $\{V_g\}$, $\{V_g^*\}$, $\{V_g^{*'}\}$, $\{|i\rangle\}$, $\{|i'\rangle\}$, B come sopra, S come nella* (2.15)*. Sia $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ tale che*

$$\forall g \in \mathcal{G} \qquad |\psi\rangle = V_g \otimes V_g^{*'} |\psi\rangle$$

Allora si ha:

$$\forall g \in \mathcal{G} \qquad I \otimes S|\psi\rangle = V_g \otimes V_g^{*'} \cdot I \otimes S|\psi\rangle$$

Dimostrazione Per l'equivalenza delle due rappresentazioni complesse coniugate, l'ipotesi su $|\psi\rangle$ si può scrivere

$$\forall g \in \mathcal{G} \qquad |\psi\rangle = V_g \otimes S^{-1} V_g^* S|\psi\rangle$$

ovvero

$$\forall g \in \mathcal{G} \qquad |\psi\rangle = I \otimes S^{-1} \cdot V_g \otimes V_g^* \cdot I \otimes S|\psi\rangle \quad .$$

Moltiplicando a sinistra entrambi i membri per $I \otimes S$ si ottiene la tesi $\square$

Queste osservazioni ci danno gli strumenti per enunciare il seguente

Teorema 2.3 *Siano $\mathcal{H}$ uno spazio di Hilbert e $\{V_g\}$ una rappresentazione unitaria su $\mathcal{H}$ del gruppo $\mathcal{G}$. Fissata arbitrariamente una base $\{|i\rangle\}$ ortonormale su $\mathcal{H}$, e costruita rispetto ad essa la rappresentazione complessa coniugata $\{V_g^*\}$, esiste un'applicazione ineittiva degli operatori positivi su $\mathcal{H}$ covarianti rispetto a $\{V_g\}$ nei vettori di $\mathcal{H} \otimes \mathcal{H}$ che soddisfano la condizione*

$$\forall g \in \mathcal{G} \qquad |\psi\rangle = V_g \otimes V_g^* |\psi\rangle \tag{2.16}$$

Dimostrazione Procediamo per costruzione. Per ogni R, scegliamo arbitrariamente una base di autovettori $\{|Ri\rangle\}$ e costruiamo una purificazione $|psi_R\rangle$ come nella dimostrazione della proposizione 2.1. Sia B la trasformazione che connette $\{|i\rangle\}$ a $\{|Ri\rangle\}$; posto $S = B^* B^{-1}$ si avrà per l'osservazione 2.2 che il vettore $|R\rangle = I \otimes S|\psi_R\rangle$ soddisfa

$$\forall g \in \mathcal{G} \qquad |R\rangle = V_g \otimes V_g^* |R\rangle. \tag{2.17}$$

È inoltre evidente che $|R\rangle$ è univocamente definito, e rimane una purificazione di R.

Qualunque applicazione associ ad operatori positivi loro purificazioni è iniettiva; infatti $|R\rangle = |R'\rangle$ implica per definizione di purificazione.

$$R = \mathrm{Tr}_{\mathcal{A}} \left[|R\rangle\langle R| \right] = \mathrm{Tr}_{\mathcal{A}} \left[|R'\rangle\langle R'| \right] = R'. \quad \square$$

Osservazione 2.3 *Se* $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ *soddisfa la* (2.16)*, allora* $\mathrm{Tr}_{\mathcal{A}}\left[|\psi\rangle\langle\psi|\right]$ *è un operatore positivo covariante rispetto a* $\{V_g\}$*.*

Dimostrazione Analoga alla (2.5) e seguenti.

Alla luce di questi risultati, sappiamo che tracciare sull'ancilla gli stati puri (non normalizzati) determinati dalle soluzioni della (2.16) fornisce tutti e soli gli operatori positivi covarianti rispetto a $\{V_g\}$ e che quindi studiare la (2.16) è sufficiente a determinarli tutti.

Tornando al caso fisico da cui si era partiti, si può specializzare quanto visto sopra al seguente

corollario 1 *Sia* $\mathcal{H}$ *uno spazio di Hilbert e* $\{U_g\}$ *una rappresentazione unitaria su* $\mathcal{H}$ *del gruppo* $\mathcal{G}$*. Ad ogni* $R : \mathcal{H}^{\otimes m} \otimes \mathcal{H}^{\otimes n} \to \mathcal{H}^{\otimes m} \otimes \mathcal{H}^{\otimes n}$ *positivo e covariante rispetto a* $\{U_g\}$ *nel senso della* (2.3)*, si associa iniettivamente un vettore* $|R\rangle \in \mathcal{H}^{\otimes n+m} \otimes \mathcal{H}^{\otimes n+m}$ *tale che*

$$\forall g \in \mathcal{G} \qquad U_g^{*\otimes m+n} \otimes U_g^{\otimes m+n} |R\rangle = |R\rangle. \tag{2.18}$$

Si vede allora come, scelto $\mathcal{H}$, risolvere la (2.18) a fissati $m = m'$, $n = n'$ fornisce tutte le soluzioni della (2.3) per qualsiasi coppia (m, n) tale che $m + n = m' + n'$, a patto di tracciare sugli spazi opportuni (immediatamente evidenti). Se l'applicazione che abbiamo costruito fosse in qualche modo anche suriettiva potremmo costruire un'interessante corrispondenza biunivoca tra gli operatori covarianti rispetto a $U_g^{*\otimes m} \otimes U_g^{\otimes n}$ e quelli rispetto a $U_g^{*\otimes m'} \otimes U_g^{\otimes n'}$ (con $m + n = m' + n'$, come sopra).

Inoltre si nota come la condizione di covarianza forte possa essere espressa richiedendo che la traccia di $|R\rangle\langle R|$ rispetto agli spazi opportuni abbia rango uno e sia invariante rispetto a $\left\{U_g^{\otimes M} \otimes U_g^{*\otimes M}\right\}$, con $M = \max\{m, n\}$. Questo potrebbe forse permettere di fare luce sul suo significato.

Capitolo 3

Sovrappositori covarianti ottimali

3.1 Sovrappositore universale a due canali

3.1.1 Introduzione

Un **sovrappositore universale**, cioè un'operazione quantistica che associ a un'arbitraria coppia di stati puri ortogonali $|\psi\rangle\langle\psi|$, $|\phi\rangle\langle\phi|$ lo stato puro $N(|\psi\rangle + |\phi\rangle)(\langle\psi| + \langle\phi|)$ non è fisicamente realizzabile.

Possiamo però cercare la trace-preserving quantum operation che meglio approssima un'applicazione del genere; ottenere un'approssimazione non perfetta costituirebbe di per sè una dimostrazione della sua irrealizzabilità, che pertanto non necessita di essere dimostrata a parte.

3.1.2 Impostazione generale del problema

Sia nel seguito $d = \dim \mathcal{H}$. A prima vista potrebbe sembrare che il sovrappositore ortogonale perfetto costituisca un'applicazione covariante rispetto a $\mathcal{SU}(d)$. Infatti date su $\mathcal{B}(\mathcal{H})$ due coppie di di stati puri ortogonali

$(|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|)$, $(|\phi'\rangle\langle\phi'|, |\psi'\rangle\langle\psi'|)$ esiste sempre una matrice $U \in \mathcal{SU}(d)$ tale che $\left(U|\phi\rangle\langle\phi|U^\dagger, U|\psi\rangle\langle\psi|U^\dagger\right) = (|\phi'\rangle\langle\phi'|, |\psi'\rangle\langle\psi'|)$ e inoltre si ha, per l'output, $U\left(|\psi\rangle + |\phi\rangle\right)\left(\langle\psi| + \langle\phi|\right)U^\dagger = \left(U|\psi\rangle + U|\phi\rangle\right)\left(\langle\psi|U^\dagger + \langle\phi|U^\dagger\right)$ In realtà non è così: infatti fissati $|\phi\rangle$ e $|\psi\rangle$ esiste sempre una trasformazione U appartenente a $\mathcal{SU}(d)$ tale che $U|\phi\rangle = \imath|\phi\rangle$ e $U|\psi\rangle = -\imath|\psi\rangle$. Per questa trasformazione vale:

$$\left(U|\phi\rangle\langle\phi|U^\dagger, U|\psi\rangle\langle\psi|U^\dagger\right) = (|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|)$$

$$U\left(|\psi\rangle + |\phi\rangle\right)\left(\langle\psi| + \langle\phi|\right)U^\dagger = \left(U|\psi\rangle + U|\phi\rangle\right)\left(\langle\psi|U^\dagger + \langle\phi|U^\dagger\right) = \left(|\psi\rangle - |\phi\rangle\right)\left(\langle\psi| - \langle\phi|\right)$$

Cioè l'input rimane invariante, mentre l'output viene trasformato in uno stato ortogonale.

Nonostante questo,impostare il problema in maniera covariante rispetto a $\mathcal{SU}(d)$ appare comunque una buona scelta, perchè permette di cercare approssimazioni ugualmente buone per qualunque coppia di stati ortogonali.

3.1.3 Procedimento

Il problema qui è impostato come un problema di ottimizzazione covariante; la prassi adottata consiste nel parametrizzare gli R covarianti sfruttando la loro nota decomponibilità in proiettori sugli spazi irriducibili:

$$R(r_1, ..., r_m) = \sum_{i=1}^{m} r_i P_i \tag{3.1}$$

In cui gli r_i sono reali positivi, m è il numero di rappresentazioni irriducibili in cui è decomponibile la rappresentazione considerata, e i P_i sono proiettori su sottospazi invarianti rispetto a rappresentazioni irriducibili tutte inequivalenti tra loro. Se esistono rappresentazioni irriducibili equivalenti, ai parametri va aggiunta una matrice unitaria (che in generale non spazierà su tutto $\mathcal{U}(d)$) che tenga conto delle possibili scelte[1], e in generale la parametrizzazione

[1] a tal proposito si veda [16]

diventa:

$$R(r_1, ..., r_m, U) = \sum_{i=1}^{m} r_i P_i(U) \tag{3.2}$$

ad indicare la dipendenza dei proiettori dalla matrice unitaria. Sfruttando questa parametrizzazione e la linearità della traccia si trasforma il vincolo trace-preserving in un vincolo sui parametri:

$$\mathrm{Tr}_{\mathcal{OUT}}\left[R(r_1, ..., r_m, U)\right] = \sum_{i=1}^{m} r_i \,\mathrm{Tr}_{\mathcal{OUT}}\left[P_i(U)\right] = I_{\mathcal{IN}} \tag{3.3}$$

Dopodiché si cerca di massimizzare la funzione guadagno coi metodi di analisi standard. Assumiamo come funzione guadagno la fidelity dell'output effettivo rispetto a quello atteso; nel nostro caso, posto il seed dell'orbita covariante che ci interessa $|\sigma\rangle = |IN\rangle|OUT\rangle$, si può scrivere

$$F = \langle\sigma|R|\sigma\rangle \tag{3.4}$$

Troveremo per lo più comodo prendere $|\sigma\rangle$ non normalizzato, ed esplicitare il suo fattore di normalizzazione nell'espressione della Fidelity.

3.1.4 Qubit

Si è cominciato lo studio del problema dal caso più semplice, quello del qubit. Calcoliamo la serie di Clebsch-Gordan tramite il metodo dei diagrammi di Young, ricordando che per $\mathcal{SU}(2)$ è

$$U_g \to \square \qquad , \qquad U_g^* \to \square .$$

Quindi abbiamo:

$$U_g \otimes U_g^* \otimes U_g^* = \square \otimes \square \otimes \square$$

Sviluppando:

$$(\square \otimes \square) \otimes \square = \left(\square\square \oplus \begin{array}{|c|}\hline\ \\\hline\ \\\hline\end{array}\right) \otimes \square = \square\square\square \oplus \begin{array}{|c|c|}\hline\ & \\\hline\ \\\hline\end{array} \oplus \begin{array}{|c|c|}\hline\ & \\\hline\ \\\hline\end{array} = \square\square\square \oplus \square \oplus \square$$

Quindi $U_g \otimes U_g^* \otimes U_g^*$ si decompone in tre rappresentazioni irriducibili, che resta il problema di determinare esplicitamente. Sappiamo [12] che sono legate a quelle di $U_g \otimes U_g \otimes U_g$ dalla similitudine $I_{\mathcal{OUT}} \otimes \sigma_y \otimes \sigma_y$. Conosciamo già, dalle regole per la somma dei momenti angolari, quali sono le rappresentazioni irriducibili per $I_{\mathcal{OUT}} \otimes \sigma_y \otimes \sigma_y$: una sullo spazio totalmente simmetrico, e due equivalenti (tra loro come alla rappresentazione definente) che si dividono il suo complemento ortogonale.

Dimostriamo che possiamo ricondurci a risolvere un problema equivalente covariante in $U_g \otimes U_g \otimes U_g$. Ad ogni $R \in \mathcal{B}(\mathcal{OUT} \otimes \mathcal{IN})$ covariante rispetto a $U_g \otimes U_g \otimes U_g$ si può associare in maniera biunivoca un operatore R' covariante rispetto a $U_g \otimes U_g^* \otimes U_g^*$ tramite la trasformazione unitaria $R' = (I_{\mathcal{OUT}} \otimes \sigma_y \otimes \sigma_y) R (I_{\mathcal{OUT}} \otimes \sigma_y \otimes \sigma_y)$. Per definizione questa mappa conserva la positività; inoltre manda operatori trace preserving in operatori trace preserving: infatti si trova subito

$$\mathrm{Tr}_{\mathcal{OUT}}[R'] = (\sigma_y \otimes \sigma_y)\, \mathrm{Tr}_{\mathcal{OUT}}[R]\, (\sigma_y \otimes \sigma_y)$$

che implica immediatamente $\mathrm{Tr}_{\mathcal{OUT}}[R'] = I_{\mathcal{IN}} \iff \mathrm{Tr}_{\mathcal{OUT}}[R] = I_{\mathcal{IN}}$. Prendendo come seed:

$$|\sigma'\rangle = |101\rangle + |001\rangle$$

Si trova come funzione da massimizzare

$$F' = \frac{1}{2}\langle\sigma'|R'|\sigma'\rangle = \frac{1}{2}\langle\sigma'|(I_{\mathcal{OUT}} \otimes \sigma_y \otimes \sigma_y) R (I_{\mathcal{OUT}} \otimes \sigma_y \otimes \sigma_y)|\sigma'\rangle$$

In cui il fattore $\frac{1}{2}$ è dato dalla mancata normalizzazione di $|\sigma\rangle$. Quindi una volta posto:

$$|\sigma\rangle \doteq (I_{\mathcal{OUT}} \otimes \sigma_y \otimes \sigma_y)|\sigma'\rangle = |110\rangle + |010\rangle,$$

non resta che massimizzare

$$F = \frac{1}{2}\langle\sigma|R|\sigma\rangle = F' \tag{3.5}$$

Definiamo ora alcuni gruppi di vettori utili:

$$
\begin{aligned}
|S\ 0\rangle &= |000\rangle \\
|S\ 1\rangle &= \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle) \\
|S\ 2\rangle &= \frac{1}{\sqrt{3}}(|011\rangle + |101\rangle + |110\rangle) \\
|S\ 3\rangle &= |111\rangle
\end{aligned}
$$

è una base ortonormale del simmetrico, per la quale banalmente abbiamo

$$
|\langle\sigma|S\ 0\rangle|^2 = |\langle\sigma|S\ 3\rangle|^2 = 0 \quad , \quad |\langle\sigma|S\ 1\rangle|^2 = |\langle\sigma|S\ 3\rangle|^2 = \frac{1}{3} \tag{3.6}
$$

mentre:

$$
\begin{aligned}
|A,1\rangle &= \frac{1}{\sqrt{2}}(|101\rangle - |011\rangle) \\
|A,2\rangle &= \frac{1}{\sqrt{2}}(|010\rangle - |100\rangle)
\end{aligned}
$$

e

$$
\begin{aligned}
|B\ 1\rangle &= \sqrt{\frac{2}{3}}|110\rangle - \frac{1}{\sqrt{6}}(|011\rangle + |101\rangle) \\
|B\ 2\rangle &= \sqrt{\frac{2}{3}}|001\rangle - \frac{1}{\sqrt{6}}(|100\rangle + |010\rangle)
\end{aligned}
$$

sono basi ortonormali di due sottospazi invarianti irriducibili, i quali sono ortogonali rispetto al totalmente simmetrico e tra loro. Per loro invece si ha:

$$
\begin{aligned}
\langle\sigma|A,1\rangle = 0 \quad , \quad \langle\sigma|A,2\rangle &= \frac{1}{\sqrt{2}} \\
\langle\sigma|B\ 1\rangle = \sqrt{\frac{2}{3}} \quad , \quad \langle\sigma|B\ 2\rangle &= \frac{-1}{\sqrt{6}}
\end{aligned} \tag{3.7}
$$

A partire da queste possiamo costruire basi per tutti i sottospazi invarianti irriducibili equivalenti a questi due tramite una matrice unitaria della forma:

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 \\ -\alpha_2^* & \alpha_1^* \end{pmatrix}$$

con ovviamente $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Posti quindi

$$\underline{\alpha} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \qquad \underline{\beta} = \begin{pmatrix} -\alpha_2^* \\ \alpha_1^* \end{pmatrix} \quad ,$$

$$|(\underline{\xi})1\rangle = \xi_1|A, 1\rangle + \xi_2|B\ 1\rangle$$
$$|(\underline{\xi})2\rangle = \xi_1|A, 2\rangle + \xi_2|B\ 2\rangle$$

$$P_S = |S\ 0\rangle\langle S\ 0| + |S\ 1\rangle\langle S\ 1| + |S\ 2\rangle\langle S\ 2| + |S\ 3\rangle\langle S\ 3|$$

$$P_{(\underline{\xi})} = |(\underline{\xi})1\rangle\langle(\underline{\xi})1| + |(\underline{\xi})2\rangle\langle(\underline{\xi})2|$$

Possiamo parametrizzare lo spazio degli R come segue:

$$R = a \cdot P_S + b \cdot P_{(\underline{\alpha})} + c \cdot P_{(\underline{\beta})} \tag{3.8}$$

Di conseguenza possiamo riscrivere l'espressione della fidelity:

$$F = \frac{1}{2}(a\langle\sigma|P_S|\sigma\rangle + b\langle\sigma|P_{(\underline{\alpha})}|\sigma\rangle + c\langle\sigma|P_{(\underline{\beta})}|\sigma\rangle) \tag{3.9}$$

Calcoliamo $\langle\sigma|P_S|\sigma\rangle$ e $\langle\sigma|P_{(\underline{\xi})}|\sigma\rangle$.
Per P_S:

$$\langle\sigma|P_S|\sigma\rangle = \langle\sigma|S\ 0\rangle\langle S\ 0|\sigma\rangle + \langle\sigma|S\ 1\rangle\langle S\ 1|\sigma\rangle + \langle\sigma|S\ 2\rangle\langle S\ 2|\sigma\rangle + \langle\sigma|S\ 3\rangle\langle S\ 3|\sigma\rangle$$

ovvero

$$\langle\sigma|P_S|\sigma\rangle = |\langle\sigma|S\ 0\rangle|^2 + |\langle\sigma|S\ 1\rangle|^2 + |\langle\sigma|S\ 2\rangle|^2 + |\langle\sigma|S\ 3\rangle|^2$$

Sostituendo i valori dati dalle (3.6) si ottiene

$$\langle\sigma|P_S|\sigma\rangle = \frac{2}{3} \tag{3.10}$$

Calcoliamo $P_{(\underline{\xi})}$. Per $i = 1, 2$:

$$|(\underline{\xi}), i\rangle\langle(\underline{\xi}), i| = (\xi_1|A\ i\rangle + \xi_2|B\ i\rangle)(\xi_1^*\langle A\ i| + \xi_2^*\langle B\ i|) =$$
$$= |\xi_1|^2|A\ i\rangle\langle A\ i| + \xi_1\xi_2^*|A\ i\rangle\langle B\ i| + \xi_2\xi_1^*|B\ i\rangle\langle A\ i| + |\xi_2|^2|B\ i\rangle\langle B\ i|$$

Sostituendo nell'espressione di $P_{(\underline{\xi})}$ si ha

$$P_{(\underline{\xi})} = |\xi_1|^2(|A\ 1\rangle\langle A\ 1| + |A\ 2\rangle\langle A\ 2|) + \xi_1\xi_2^*(|A\ 1\rangle\langle B\ 1| + |A\ 2\rangle\langle B\ 2|) +$$
$$+ \xi_2\xi_1^*(|B\ 1\rangle\langle A\ 1| + |B\ 2\rangle\langle A\ 2|) + |\xi_2|^2(|B\ 1\rangle\langle B\ 1| + |B\ 2\rangle\langle B\ 2|)$$

Mediando su $|\sigma\rangle$:

$$\langle\sigma|P_{(\underline{\xi})}|\sigma\rangle = |\xi_1|^2(\langle\sigma|A\ 1\rangle\langle A\ 1|\sigma\rangle + \langle\sigma|A\ 2\rangle\langle A\ 2|\sigma\rangle) + \xi_1\xi_2^*(\langle\sigma|A\ 1\rangle\langle B\ 1|\sigma\rangle + \langle\sigma|A\ 2\rangle\langle B\ 2|\sigma\rangle) +$$
$$+\xi_2\xi_1^*(\langle\sigma|B\ 1\rangle\langle A\ 1|\sigma\rangle + \langle\sigma|B\ 2\rangle\langle A\ 2|\sigma\rangle) + |\xi_2|^2(\langle\sigma|B\ 1\rangle\langle B\ 1|\sigma\rangle + \langle\sigma|B\ 2\rangle\langle B\ 2|\sigma\rangle)$$

Sostituendo i valori delle (3.7):

$$\langle\sigma|P_{(\underline{\xi})}|\sigma\rangle = |\xi_1|^2\frac{1}{2} - \xi_1\xi_2^*\frac{1}{2\sqrt{3}} - \xi_2\xi_1^*\frac{1}{2\sqrt{3}} + |\xi_2|^2(\frac{2}{3} + \frac{1}{6}) =$$
$$= |\xi_1|^2\frac{1}{2} + |\xi_2|^2\frac{5}{6} - \frac{1}{2\sqrt{3}}(\xi_1\xi_2^* + \xi_2\xi_1^*) = |\xi_1|^2\frac{1}{2} + |\xi_2|^2\frac{1}{2} + |\xi_2|^2\frac{1}{3} - \frac{1}{2\sqrt{3}}2\Re(\xi_1\xi_2^*)$$

Ricordando che $|\xi_1|^2 + |\xi_2|^2 = 1$ si riscrive:

$$\langle\sigma|P_{(\underline{\xi})}|\sigma\rangle = \frac{1}{2} + \underbrace{\frac{1}{3}|\xi_2|^2 - \frac{1}{\sqrt{3}}\Re(\xi_1\xi_2^*)}_{f(\underline{\xi})} \tag{3.11}$$

Sostituendo ora le (3.10) e (3.11) nella (3.9) otteniamo:

$$F = \frac{1}{2}\left(\frac{2}{3}a + \left(\frac{1}{2} + f(\underline{\alpha})\right)b + \left(\frac{1}{2} + f(\underline{\beta})\right)c\right) \tag{3.12}$$

Che costituisce la quantità da massimizzare.

Imponiamo i vincoli

$$|\alpha_1|^2 + |\alpha_2|^2 = 1 \quad , \quad \underline{\beta} = \begin{pmatrix} -\alpha_2^* \\ \alpha_1^* \end{pmatrix} \quad , \quad \mathrm{Tr}_{\mathcal{OUT}}[R] = I_{\mathcal{IN}} \tag{3.13}$$

$$\mathrm{Tr}_{\mathcal{OUT}}[R] = a\,\mathrm{Tr}_{\mathcal{OUT}}[P_S] + b\,\mathrm{Tr}_{\mathcal{OUT}}\left[P_{(\underline{\alpha})}\right] + c\,\mathrm{Tr}_{\mathcal{OUT}}\left[P_{(\underline{\beta})}\right] \tag{3.14}$$

$$\begin{aligned}\mathrm{Tr}_{\mathcal{OUT}}[P_S] &= |00\rangle\langle 00| + \frac{1}{3}\left(|11\rangle\langle 11| + |10\rangle\langle 10| + |01\rangle\langle 01| + |10\rangle\langle 01| + |10\rangle\langle 01|\right) + \\ &+ \frac{1}{3}\left(|00\rangle\langle 00| + |10\rangle\langle 10| + |01\rangle\langle 01| + |10\rangle\langle 01| + |10\rangle\langle 01|\right) + |11\rangle\langle 11| = \\ &= \frac{4}{3}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right) + \frac{2}{3}\left(|10\rangle\langle 10| + |01\rangle\langle 01| + |10\rangle\langle 01| + |01\rangle\langle 10|\right)\end{aligned} \tag{3.15}$$

$$\begin{aligned}\mathrm{Tr}_{\mathcal{OUT}}\left[P_{(\underline{\xi})}\right] = {} & \frac{|\xi_1|^2}{2}\left(|01\rangle\langle 01| + |11\rangle\langle 11|\right) + \\ & + \xi_1\xi_2^*\left(\frac{1}{\sqrt{2}}\cdot\frac{\sqrt{2}}{\sqrt{3}}|01\rangle\langle 10| - \frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{6}}\left(|01\rangle\langle 01| - |11\rangle\langle 11|\right)\right) + \\ & + \xi_1^*\xi_2\left(\frac{1}{\sqrt{3}}|10\rangle\langle 01| - \frac{1}{2\sqrt{3}}\left(|01\rangle\langle 01| - |11\rangle\langle 11|\right)\right) + \\ & + |\xi_2|^2\left(\frac{2}{3}|10\rangle\langle 10| - \frac{1}{3}\left(|10\rangle\langle 01| + |01\rangle\langle 10|\right) + \frac{1}{6}\left(|11\rangle\langle 11| + |01\rangle\langle 01|\right)\right) + \\ & + \frac{|\xi_1|^2}{2}\left(|10\rangle\langle 10| + |00\rangle\langle 00|\right) + \\ & + \xi_1\xi_2^*\left(\frac{-1}{\sqrt{3}}|10\rangle\langle 01| + \frac{1}{2\sqrt{3}}\left(|10\rangle\langle 10| - |00\rangle\langle 00|\right)\right) + \\ & + \xi_1^*\xi_2\left(\frac{-1}{\sqrt{3}}|01\rangle\langle 10| + \frac{1}{2\sqrt{3}}\left(|10\rangle\langle 10| - |00\rangle\langle 00|\right)\right) + \\ & + |\xi_2|^2\left(\frac{2}{3}|01\rangle\langle 01| - \frac{1}{3}\left(|10\rangle\langle 01| + |01\rangle\langle 10|\right) + \frac{1}{6}\left(|00\rangle\langle 00| + |10\rangle\langle 10|\right)\right)\end{aligned}$$

Raccogliendo:

$$\begin{aligned}&\mathrm{Tr}_{\mathcal{OUT}}\left[P_{(\underline{\xi})}\right] = \\ &\left(\frac{|\xi_1|^2}{2} - \frac{\xi_1\xi_2^* + \xi_2\xi_1^*}{2\sqrt{3}} + \frac{|\xi_2|^2}{6} + \frac{2|\xi_2|^2}{3}\right)|01\rangle\langle 01| + \left(\frac{|\xi_1|^2}{2} + \frac{\xi_1\xi_2^* + \xi_2\xi_1^*}{2\sqrt{3}} + \frac{|\xi_2|^2}{6}\right)|11\rangle\langle 11| + \\ &+ \left(-\frac{|\xi_2|^2}{3} + \frac{\xi_1\xi_2^* - \xi_2\xi_1^*}{\sqrt{3}} - \frac{|\xi_2|^2}{3} +\right)|01\rangle\langle 10| + \left(-\frac{|\xi_2|^2}{3} - \frac{\xi_1\xi_2^* + \xi_2\xi_1^*}{\sqrt{3}} - \frac{|\xi_2|^2}{3}\right)|10\rangle\langle 01| + \\ &+ \left(\frac{1}{2} + \frac{\Re\xi_1\xi_2^*}{\sqrt{3}} + \frac{|\xi_2|^2}{3}\right)|10\rangle\langle 10| + \left(\frac{|\xi_1|^2}{2} - \frac{\Re\xi_1\xi_2^*}{\sqrt{3}} - \frac{|\xi_2|^2}{3}\right)|00\rangle\langle 00|\end{aligned}$$

Sommando e ricordando che $|\xi_1|^2 + |\xi_2|^2 = 1$:

$$\begin{aligned}\mathrm{Tr}_{\mathcal{OUT}}\left[P_{(\underline{\xi})}\right] = &\left(\frac{1}{2} - \frac{\Re(\xi_1\xi_2^*)}{\sqrt{3}} + \frac{|\xi_2|^2}{3}\right)|01\rangle\langle 01| + \left(\frac{1}{2} + \frac{\Re(\xi_1\xi_2^*)}{\sqrt{3}} - \frac{|\xi_2|^2}{3}\right)|11\rangle\langle 11| + \\ &+ \left(\frac{2\Im(\xi_1\xi_2^*)}{\sqrt{3}} - \frac{2|\xi_2|^2}{3}\right)|01\rangle\langle 10| + \left(-\frac{2\Im(\xi_1\xi_2^*)}{\sqrt{3}} - \frac{2|\xi_2|^2}{3}\right)|10\rangle\langle 01| + \\ &+ \left(\frac{1}{2} + \frac{\Re(\xi_1\xi_2^*)}{\sqrt{3}} + \frac{|\xi_2|^2}{3}\right)|10\rangle\langle 10| + \left(\frac{1}{2} - \frac{\Re(\xi_1\xi_2^*)}{\sqrt{3}} - \frac{|\xi_2|^2}{3}\right)|00\rangle\langle 00|\end{aligned}$$

Che ponendo $f(\underline{\xi})$ come nella (3.11) e $g(\underline{\xi}) = \frac{\Re(\xi_1\xi_2^*)}{\sqrt{3}} + \frac{|\xi_2|^2}{3}$ diventa:

$$\begin{aligned}\mathrm{Tr}_{\mathcal{OUT}}\left[P_{(\underline{\xi})}\right] = &\left(\frac{1}{2} + f(\underline{\xi})\right)|01\rangle\langle 01| + \left(\frac{1}{2} - f(\underline{\xi})\right)|11\rangle\langle 11| + \\ &+ \left(\frac{2\Im(\xi_1\xi_2^*)}{\sqrt{3}} - \frac{2|\xi_2|^2}{3}\right)|01\rangle\langle 10| + \left(-\frac{2\Im(\xi_1\xi_2^*)}{\sqrt{3}} - \frac{2|\xi_2|^2}{3}\right)|10\rangle\langle 01| + \\ &+ \left(\frac{1}{2} + g(\underline{\xi})\right)|10\rangle\langle 10| + \left(\frac{1}{2} - g(\underline{\xi})\right)|00\rangle\langle 00|\end{aligned} \tag{3.16}$$

Tenendo presenti la (3.14), la (3.1.4) e la (3.16) possiamo tradurre il vincolo trace-preserving in un vincolo sui parametri, imponendo che i coefficienti dei proiettori siano uguali a uno e che i termini fuori diagonale siano uguali a zero, come nella seguente tabella

Operatore	Coefficiente
$\|11\rangle\langle 11\|$	$\frac{4}{3}a + \left(\frac{1}{2} - f(\underline{\alpha})\right)b + \left(\frac{1}{2} - f(\underline{\beta})\right)c = 1$
$\|10\rangle\langle 10\|$	$\frac{2}{3}a + \left(\frac{1}{2} + g(\underline{\alpha})\right)b + \left(\frac{1}{2} + g(\underline{\beta})\right)c = 1$
$\|01\rangle\langle 01\|$	$\frac{2}{3}a + \left(\frac{1}{2} + f(\underline{\alpha})\right)b + \left(\frac{1}{2} + f(\underline{\beta})\right)c = 1$
$\|00\rangle\langle 00\|$	$\frac{4}{3}a + \left(\frac{1}{2} - g(\underline{\alpha})\right)b + \left(\frac{1}{2} - g(\underline{\beta})\right)c = 1$
$\|10\rangle\langle 01\|$	$\frac{2}{3}a - \left(\frac{2}{\sqrt{3}}\Im(\alpha_1\alpha_2^*) + \frac{2}{3}\|\alpha_2\|^2\right)b - \left(\frac{2}{\sqrt{3}}\Im(\beta_1\beta_2^*) + \frac{2}{3}\|\beta_2\|^2\right)c = 0$
$\|01\rangle\langle 10\|$	$\frac{2}{3}a + \left(\frac{2}{\sqrt{3}}\Im(\alpha_1\alpha_2^*) - \frac{2}{3}\|\alpha_2\|^2\right)b + \left(\frac{2}{\sqrt{3}}\Im(\beta_1\beta_2^*) - \frac{2}{3}\|\beta_2\|^2\right)c = 0$

Risolvendo la $|01\rangle\langle 01|$ della prima tabella rispetto a $\frac{2}{3}a$ si ottiene:

$$\frac{2}{3}a = 1 - \left(\frac{1}{2} + f(\underline{\alpha})\right)b - \left(\frac{1}{2} + f(\underline{\beta})\right)c \tag{3.17}$$

che sostituita nella (3.12), dà

$$F = \frac{1}{2}\left(1 - \left(\frac{1}{2} + f(\underline{\alpha})\right) b - \left(\frac{1}{2} + f(\underline{\beta})\right) c + \left(\frac{1}{2} + f(\underline{\alpha})\right) b + \left(\frac{1}{2} + f(\underline{\beta})\right) c\right) = \frac{1}{2} \tag{3.18}$$

3.1.5 Dimensione generica

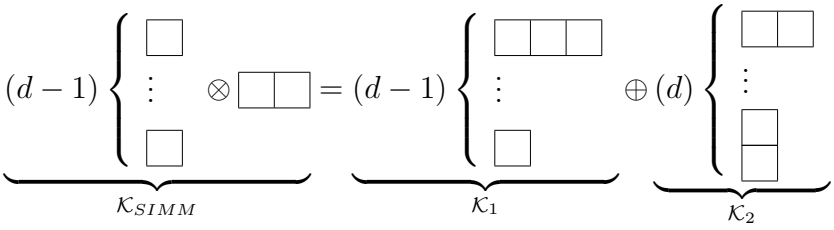
Generalizziamo al caso in cui $\dim \mathcal{H} = d \in \mathbb{N}$. Poniamo allora, in termini di diagrammi di Young:

$$U_g \longrightarrow (d-1)\left\{\begin{array}{c}\square\\ \vdots\\ \square\end{array}\right. \quad , \qquad U_g^* \longrightarrow \square \tag{3.19}$$

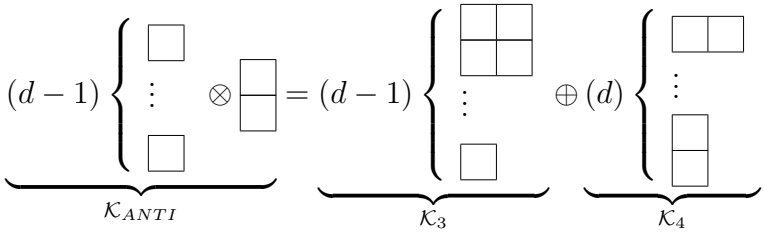
Dove il parametro prima della graffa verticale indica la lunghezza della colonna, in questo caso $d-1$ caselle. Procedendo coi calcoli secondo il metodo noto si trova:

$$\underbrace{(d-1)\left\{\begin{array}{c}\square\\ \vdots\\ \square\end{array}\right.}_{\mathcal{OUT}} \otimes \underbrace{\left(\square \otimes \square\right)}_{\mathcal{IN}} = (d-1)\left\{\begin{array}{c}\square\\ \vdots\\ \square\end{array}\right. \otimes \left(\square\square \oplus \begin{array}{c}\square\\ \square\end{array}\right) \tag{3.20}$$

$$\underbrace{(d-1)\left\{\begin{array}{c}\square\\ \vdots\\ \square\end{array}\right.}_{\mathcal{OUT}} \otimes \underbrace{\left(\square\square \oplus \begin{array}{c}\square\\ \square\end{array}\right)}_{\mathcal{IN}} = \underbrace{(d-1)\left\{\begin{array}{c}\square\\ \vdots\\ \square\end{array}\right. \otimes \square\square}_{\mathcal{K}_{SIMM}} \oplus \underbrace{(d-1)\left\{\begin{array}{c}\square\\ \vdots\\ \square\end{array}\right. \otimes \begin{array}{c}\square\\ \square\end{array}}_{\mathcal{K}_{ANTI}} \tag{3.21}$$



(3.22)



(3.23)

Dove con le graffe orizzontali si sono etichettati i sottospazi invarianti rispetto alla rappresentazione irriducibile relativa. Possiamo riassumere questa etichettatura scrivendo

$$\mathcal{OUT} \otimes \mathcal{IN} = \mathcal{K}_{SIMM} \oplus \mathcal{K}_{ANTI} \tag{3.24}$$

$$\mathcal{K}_{SIMM} = \mathcal{K}_1 \oplus \mathcal{K}_2 \qquad , \qquad \mathcal{K}_{ANTI} = \mathcal{K}_3 \oplus \mathcal{K}_4 \tag{3.25}$$

e ricordando che $\mathcal{K}_{SIMM}$ e $\mathcal{K}_{ANTI}$ sono rispettivamente il prodotto tensore dello spazio di input con le parti simmetrica e antisimmetrica dello spazio di output, e che entrambi ammettono un'unica decomposizione non banale in sottospazi invarianti, data dalla coppia $\mathcal{K}_1$, $\mathcal{K}_2$ per $\mathcal{K}_{SIMM}$ e dalla coppia $\mathcal{K}_3$, $\mathcal{K}_4$ per$\mathcal{K}_{ANTI}$. Inoltre possiamo notare che $\mathcal{K}_2$ e $\mathcal{K}_4$ sono isomorfi a $\mathcal{H}$, e le rispettive rappresentazioni irriducibili sono equivalenti a $\left\{U_g^*\right\}$. Posti inoltre

$$|\mathcal{K}_2 \ m\rangle \doteq \frac{1}{\sqrt{2(d+1)}} \sum_{i=1}^{d} |i\rangle \left(|i\rangle|m\rangle + |m\rangle|i\rangle\right) \tag{3.26}$$

e

$$|\mathcal{K}_4 \ m\rangle \doteq \frac{1}{\sqrt{2(d-1)}} \sum_{i=1}^{d} |i\rangle \left(|i\rangle|m\rangle - |m\rangle|i\rangle\right) \tag{3.27}$$

Si verifica facilmente che

$$\mathcal{B}_2 \doteq \{|\mathcal{K}_2 \ m\rangle \quad , \quad m = 1, \ldots, d\} \tag{3.28}$$

e

$$\mathcal{B}_4 \doteq \{|\mathcal{K}_4\ m\rangle \quad , \quad m = 1, \ldots, d\} \tag{3.29}$$

costituiscono basi ortonormali per $\mathcal{K}_2$ e $\mathcal{K}_4$.

Detti rispettivamente P_{SIMM}, P_{ANTI}, P_1, P_2, P_3, P_4 i proiettori su $\mathcal{K}_{SIMM}$, $\mathcal{K}_{ANTI}$, $\mathcal{K}_1$, $\mathcal{K}_2$, $\mathcal{K}_3$ e $\mathcal{K}_4$, le equazioni (3.24) e (3.25) diventano:

$$I = P_{SIMM} + P_{ANTI} \tag{3.30}$$

$$P_{SIMM} = P_1 + P_2 \qquad , \qquad P_{ANTI} = P_3 + P_4 \tag{3.31}$$

Come nel caso del qubit, essendo $\mathcal{K}_2$ e $\mathcal{K}_4$ invarianti rispetto a rappresentazioni equivalenti, esistono infiniti modi di decomporre $\mathcal{K}_2 \oplus \mathcal{K}_4$ in una coppia di sottospazi invarianti rispetto a rappresentazioni irriducibili equivalenti. Infatti, per ogni $\underline{\alpha} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \in \mathbb{C}^2$ unimodulare lo spazio

$$\mathcal{K}_{\underline{\alpha}} \doteq \text{span}\,\{|\mathcal{K}_{\underline{\alpha}}\ m\rangle \doteq \alpha_1|\mathcal{K}_1\ m\rangle + \alpha_2|\mathcal{K}_2\ m\rangle, \quad m = 1, \ldots, d\} \tag{3.32}$$

ed il suo complemento ortogonale $\mathcal{K}_{\underline{\beta}}$, con $\underline{\beta} = \begin{pmatrix} -\alpha_2^* \\ \alpha_1^* \end{pmatrix}$ costituiscono una decomposizione di $\mathcal{K}_2 \oplus \mathcal{K}_4$ che risponde ai criteri dati. Detti $P_{\underline{\alpha}}$ e $P_{\underline{\beta}}$ i proiettori su $\mathcal{K}_{\underline{\alpha}}$ e $\mathcal{K}_{\underline{\beta}}$, possiamo parametrizzare R rispetto ad x, y, z, t, $\underline{\alpha}$ e $\underline{\beta}$ (dipendente da $\underline{\alpha}$); gli ultimi due sono vettori complessi definiti come sopra, i primi quattro parametri reali. Otteniamo:

$$R = xP_1 + yP_3 + zP_{\underline{\alpha}} + tP_{\underline{\beta}} \tag{3.33}$$

Da cui, fissato $|\sigma\rangle = |1\rangle|1\rangle|2\rangle + |2\rangle|1\rangle|2\rangle$ e ricordando che $F = \frac{1}{2}\langle\sigma|R|\sigma\rangle$, possiamo ricavare la parametrizzazione della fidelity:

$$F(x, y, z, t, \underline{\alpha}) = \frac{1}{2}\left[\langle\sigma|P_1|\sigma\rangle x + \langle\sigma|P_3|\sigma\rangle y + \langle\sigma|P_{\underline{\alpha}}|\sigma\rangle z + \langle\sigma|P_{\underline{\beta}}|\sigma\rangle t\right] \tag{3.34}$$

Partendo dalla forma di $\mathcal{K}_{\underline{\alpha}}$ (3.32) si ricava facilmente:

$$\langle\sigma|P_{\underline{\alpha}}|\sigma\rangle = |\alpha_1|^2\langle\sigma|P_2|\sigma\rangle + |\alpha_2|^2\langle\sigma|P_4|\sigma\rangle \tag{3.35}$$

E dalle (3.31)

$$\langle\sigma|P_1|\sigma\rangle = \langle\sigma|P_{SIMM}|\sigma\rangle - \langle\sigma|P_2|\sigma\rangle \tag{3.36}$$

$$\langle\sigma|P_3|\sigma\rangle = \langle\sigma|P_{ANTI}|\sigma\rangle - \langle\sigma|P_4|\sigma\rangle \tag{3.37}$$

A questo punto, con calcoli semplici, si ottiene la forma esplicita in d e $\underline{\alpha}$ dei termini

$$\langle\sigma|P_{SIMM}|\sigma\rangle = 1 \qquad , \qquad \langle\sigma|P_{ANTI}|\sigma\rangle = 1 \tag{3.38}$$

$$\langle\sigma|P_2|\sigma\rangle = \frac{1}{d+1} \qquad , \qquad \langle\sigma|P_4|\sigma\rangle = \frac{1}{d-1} \tag{3.39}$$

$$\langle\sigma|P_1|\sigma\rangle = 1 - \frac{1}{d+1} = \frac{d}{d+1} \tag{3.40}$$

$$\langle\sigma|P_3|\sigma\rangle = 1 - \frac{1}{d-1} = \frac{d-2}{d-1} \tag{3.41}$$

$$\begin{aligned}\langle\sigma|P_{\underline{\alpha}}|\sigma\rangle &= \frac{|\alpha_1|^2}{d+1} + \frac{|\alpha_2|^2}{d-1} = \frac{(d-1)|\alpha_1|^2 + (d+1)|\alpha_2|^2}{d^2-1} = \\ &= \frac{(d-1)(|\alpha_1|^2 + |\alpha_2|^2) + 2|\alpha_2|^2}{d^2-1} = \frac{1}{d+1} + \frac{2|\alpha_2|^2}{d^2-1}\end{aligned} \tag{3.42}$$

che debitamente sostituita, porta alla seguente scrittura della fidelity:

$$F = \frac{1}{2}\left[\frac{d}{d+1}x + \frac{d-2}{d-1}y + \left(\frac{1}{d+1} + \frac{2|\alpha_2|^2}{d^2-1}\right)z + \left(\frac{1}{d+1} + \frac{2|\alpha_1|^2}{d^2-1}\right)t\right] \tag{3.43}$$

Ora procediamo a scrivere in termini dei parametri il vincolo trace-preserving $\mathrm{Tr}_{\mathcal{OUT}}[R] = I_{\mathcal{IN}}$. Detti $P^S_{\mathcal{IN}}, P^A_{\mathcal{IN}} \in \mathcal{B}(\mathcal{IN})$ i proiettori rispettivamente sui sottospazi totalmente simmetrico e totalmente antisimmetrico dell'input,

troviamo:

$$\mathrm{Tr}_{\mathcal{OUT}}\left[P_{SIMM}\right] = \mathrm{Tr}_{\mathcal{OUT}}\left[I_{\mathcal{IN}} \otimes P^{S}_{\mathcal{IN}}\right] = dP^{S}_{\mathcal{IN}} \tag{3.44}$$

$$\mathrm{Tr}_{\mathcal{OUT}}\left[P_{ANTI}\right] = \mathrm{Tr}_{\mathcal{OUT}}\left[I_{\mathcal{IN}} \otimes P^{A}_{\mathcal{IN}}\right] = dP^{A}_{\mathcal{IN}} \tag{3.45}$$

$$\begin{aligned}\mathrm{Tr}_{\mathcal{OUT}}\left[P_2\right] &= \frac{1}{2(d+1)} \sum_{i,k,l,m=1}^{d} \langle i|k\rangle(|k\rangle|m\rangle + |m\rangle|k\rangle)(\langle l|\langle m| + \langle m|\langle l|)\langle l|i\rangle \\ &= \frac{1}{2(d+1)} \sum_{k,m=1}^{d} (|k\rangle|m\rangle + |m\rangle|k\rangle)(\langle k|\langle m| + \langle m|\langle k|) = \\ &\frac{1}{2(d+1)} 4P^{S}_{\mathcal{IN}} = \frac{2}{d+1} P^{S}_{\mathcal{IN}}\end{aligned} \tag{3.46}$$

$$\begin{aligned}\mathrm{Tr}_{\mathcal{OUT}}\left[P_4\right] &= \frac{1}{2(d-1)} \sum_{i,k,l,m=1}^{d} \langle i|k\rangle(|k\rangle|m\rangle - |m\rangle|k\rangle)(\langle l|\langle m| - \langle m|\langle l|)\langle l|i\rangle \\ &= \frac{1}{2(d-1)} \sum_{k,m=1}^{d} (|k\rangle|m\rangle - |m\rangle|k\rangle)(\langle k|\langle m| - \langle m|\langle k|) = \frac{1}{2(d-1)} 4P^{A}_{\mathcal{IN}} \\ &= \frac{2}{d-1} P^{A}_{\mathcal{IN}}\end{aligned} \tag{3.47}$$

$$\mathrm{Tr}_{\mathcal{OUT}}\left[P_1\right] = \mathrm{Tr}_{\mathcal{OUT}}\left[P_{SIMM}\right] - \mathrm{Tr}_{\mathcal{OUT}}\left[P_2\right] = \frac{d^2+d-2}{d+1} P^{S}_{\mathcal{IN}} \tag{3.48}$$

$$\mathrm{Tr}_{\mathcal{OUT}}\left[P_3\right] = \mathrm{Tr}_{\mathcal{OUT}}\left[P_{ANTI}\right] - \mathrm{Tr}_{\mathcal{OUT}}\left[P_4\right] = \frac{d^2-d-2}{d-1} P^{A}_{\mathcal{IN}} \tag{3.49}$$

$$\mathrm{Tr}_{\mathcal{OUT}}\left[P_{\underline{\alpha}}\right] = \frac{2|\alpha_1|^2}{d+1} P^{S}_{\mathcal{IN}} + \frac{2|\alpha_2|^2}{d-1} P^{A}_{\mathcal{IN}} \tag{3.50}$$

$$\left(\mathrm{Tr}_{\mathcal{OUT}}\left[P_{\underline{\beta}}\right] = \frac{2|\alpha_2|^2}{d+1} P^{S}_{\mathcal{IN}} + \frac{2|\alpha_1|^2}{d-1} P^{A}_{\mathcal{IN}}\right) \tag{3.51}$$

Tenendo presente le ultime quattro delle precedenti e la (3.33), si puo' scrivere il vincolo trace preserving come il sistema:

$$\begin{array}{ll} P^{S}_{\mathcal{IN}} & \left\{ \begin{array}{l} \dfrac{d^2+d-2}{d+1}x + \dfrac{2|\alpha_1|^2}{d+1}z + \dfrac{2|\alpha_2|^2}{d+1}t = 1 \\ \dfrac{d^2-d-2}{d-1}y + \dfrac{2|\alpha_2|^2}{d-1}z + \dfrac{2|\alpha_1|^2}{d-1}t = 1 \end{array} \right. \\ P^{A}_{\mathcal{IN}} & \end{array} \tag{3.52}$$

Nota Tanto qui che nell'espressione della fidelity, possiamo osservare come il coefficiente di y, che rappresenta l'autovalore di R relativo allo spazio invariante $\mathcal{K}_3$, si annulli per $d = 2$. Ciò riflette semplicemente il fatto che la decomposizione in rappresentazioni irriducibili di $\mathcal{SU}(d) \otimes \mathcal{SU}(d)^* \otimes \mathcal{SU}(d)^*$ ha quattro elementi non nulli solo per $d > 2$, e per $d = 2$ perde proprio la rappresentazione su $\mathcal{K}_3$.

Osservazione Nei problemi di ottimizzazione convessa, quale questo, i punti estremi si trovano in corrispondenza di quelli detti *estremali* del convesso che costituisce il dominio. Considerando l'insieme convesso delle CP-Map covarianti rispetto a una rappresentazione data, si ha che una mappa completamente positiva e' estremale se e solo se, considerati solo gli spazi irriducibili che sono autospazi di un autovalore non nullo rispetto all'operatore positivo associato alla mappa, le tracce sull'output dei proiettori su questi spazi e degli isomorfismi che connettono quelli tra loro su cui agiscono rappresentazioni equivalenti costituiscono un insieme di operatori sull'input linearmente indipendenti. Osservando le equazioni dalla (3.48) alla (3.51) è evidente che condizione necessaria e sufficiente per l'estremalità di R è che esso abbia almeno due autovalori nulli (le tracce sull'output dei proiettori sono linearmente indipendenti a due a due). Inoltre, svolgendo il calcolo, possiamo vedere come anche la traccia sull'output dell'isomorfismo che connette $\mathcal{K}_{\underline{\alpha}}$ a $\mathcal{K}_{\underline{\beta}}$ sia una combinazione lineare di $P^S_{\mathcal{IN}}$ e $P^A_{\mathcal{IN}}$; questo impone come condizione necessaria per l'estremalità di R

$$z = 0 \vee t = 0.$$

Il grado di libertà in $\underline{\alpha}$ assicura che non ci siano differenze tra la scelta di annullare l'uno o l'altro dei due autovalori; quindi possiamo riscrivere

arbitrariamente

$$\begin{array}{ll} P^S_{\mathcal{IN}} & \\ & \left\{ \begin{array}{l} \dfrac{d^2+d-2}{d+1}x + \dfrac{2|\alpha_1|^2}{d+1}z = 1 \\ \dfrac{d^2-d-2}{d-1}y + \dfrac{2|\alpha_2|^2}{d-1}z = 1 \end{array} \right. \\ P^A_{\mathcal{IN}} & \end{array} \tag{3.53}$$

come vincolo trace-preserving per gli operatori covarianti estremali.

A questo punto, sappiamo che affinchè R sia estremale non deve avere più di due autovalori non nulli, e ne abbiamo già eliminato uno. Possiamo dunque limitarci ad esaminare i casi per cui è, rispettivamente $z = 0, x = 0, y = 0$.

Caso z = 0

$$\begin{array}{ll} P^S_{\mathcal{IN}} & \\ & \left\{ \begin{array}{l} \dfrac{d^2+d-2}{d+1}x = 1 \\ \dfrac{d^2-d-2}{d-1}y = 1 \end{array} \right. \\ P^A_{\mathcal{IN}} & \end{array} \tag{3.54}$$

Il sistema è determinato, e ha banalmente come soluzioni:

$$\left\{ \begin{array}{l} x = \dfrac{d+1}{d^2+d-2} = \dfrac{d+1}{(d-1)(d+2)} \\ y = \dfrac{d-1}{d^2-d-2} = \dfrac{d-1}{(d+1)(d-2)} \end{array} \right. , \tag{3.55}$$

che sostituite nell'espressione della fidelity (3.43) danno

$$\begin{aligned} F &= \frac{1}{2}\left[\frac{d}{(d+1)}\frac{d+1}{(d-1)(d+2)} + \frac{d-2}{(d-1)}\frac{d-1}{(d+1)(d-2)}\right] \\ &= \frac{1}{2}\frac{d(d+1)+(d-1)(d+2)}{(d-1)(d+1)(d+2)} = \frac{1}{2}\frac{d^2+2d-2}{(d-1)(d+1)(d+2)} \end{aligned} \tag{3.56}$$

risultato che per $d > 2$ è minore di $\frac{1}{2}$.

Caso x=0

$$\begin{array}{ll} P^S_{\mathcal{IN}} & \\ & \left\{ \begin{array}{l} \dfrac{2|\alpha_1|^2}{d+1}z = 1 \\ \dfrac{d^2-d-2}{d-1}y + \dfrac{2|\alpha_2|^2}{d-1}z = 1 \end{array} \right. \\ P^A_{\mathcal{IN}} & \end{array} \tag{3.57}$$

Per la fidelity, invece:

$$F = \frac{1}{2}\left[\frac{d-2}{d-1}y + \left(\frac{1}{d+1} + \frac{2|\alpha_2|^2}{(d+1)(d-1)}\right)z\right] \tag{3.58}$$

Riscriviamo il sistema come:

$$\begin{array}{ll} P^S_{\mathcal{IN}} & \left\{ \begin{array}{l} \dfrac{z}{d+1} = \dfrac{1}{2|\alpha_1|^2} \\ \dfrac{d-2}{d-1}y = \dfrac{1}{d+1} - \dfrac{2|\alpha_2|^2}{(d-1)(d+1)}z \end{array} \right. \\ P^A_{\mathcal{IN}} & \end{array} \tag{3.59}$$

e sostituiamo nell'espressione della fidelity, ottenendo:

$$\begin{aligned} F &= \frac{1}{2}\left[\frac{1}{d+1} - \frac{2|\alpha_2|^2}{(d-1)(d+1)}z + \frac{1}{2|\alpha_1|^2} + \frac{2|\alpha_2|^2}{(d+1)(d-1)}z\right] \\ &= \frac{1}{2}\left[\frac{1}{d+1} + \frac{1}{2|\alpha_1|^2}\right] \end{aligned} \tag{3.60}$$

che a prima vista potrebbe sembrare non limitata superiormente. Ma possiamo considerare l'equazione relativa a $P^A_{\mathcal{IN}}$ nel sistema (3.59) e riscriverla come

$$(d-2)y = \frac{d-1}{d+1} - \frac{|\alpha_2|^2}{|\alpha_1|^2} \tag{3.61}$$

Ricordando che vale

$$d \geq 2 \qquad , \qquad y \geq 0 \qquad , \qquad z \geq 0 \tag{3.62}$$

Possiamo dedurre:

$$\frac{d-1}{d+1} - \frac{|\alpha_2|^2}{|\alpha_1|^2} \geq 0 \tag{3.63}$$

che dato $|\alpha_2|^2 = 1 - |\alpha_1|^2$ si riscrive

$$\frac{d-1}{d+1} + 1 \geq \frac{1}{|\alpha_1|^2} \tag{3.64}$$

ossia

$$\frac{1}{|\alpha_1|^2} \leq \frac{2d}{d+1} \tag{3.65}$$

Per la fidelity si ha quindi:

$$F = \frac{1}{2}\left[\frac{1}{d+1} + \frac{1}{2|\alpha_1|^2}\right] \leq \frac{1}{2}\left[\frac{1}{d+1} + \frac{d}{d+1}\right] = \frac{1}{2} \tag{3.66}$$

caso y=0

$$\begin{array}{ll} P^S_{\mathcal{IN}} & \left\{ \begin{array}{l} \dfrac{d^2+d-2}{d+1}x + \dfrac{2|\alpha_1|^2}{d+1}z = 1 \\ \\ \dfrac{2|\alpha_2|^2}{d-1}z = 1 \end{array} \right. \\ P^A_{\mathcal{IN}} & \end{array} \tag{3.67}$$

Procedendo analogamente al caso precedente:

$$\begin{array}{ll} P^S_{\mathcal{IN}} & \left\{ \begin{array}{l} \dfrac{x}{d+1} = \dfrac{1}{(d-1)(d+2)} - \dfrac{2|\alpha_1|^2}{(d+1)(d-1)(d+2)}z \\ \\ \dfrac{2|\alpha_2|^2}{d-1}z = 1 \end{array} \right. \\ P^A_{\mathcal{IN}} & \end{array} \tag{3.68}$$

Sostituendo

$$\begin{aligned} F &= \frac{1}{2}\left[\frac{d}{(d-1)(d+2)} - \frac{2|\alpha_1|^2 z}{(d+1)(d-1)(d+2)} + \frac{z}{d+1} + \frac{1}{d+1}\right] = \\ &= \frac{1}{2}\left[\frac{2d^2+2d-2}{(d-1)(d+1)(d+2)} - \frac{d^2+d-4}{(d-1)(d+1)(d+2)}z + \frac{1}{(d+1)(d+2)}\right] \end{aligned} \tag{3.69}$$

Il massimo si ha per $z = 0$, ossia:

$$\begin{aligned} F &= \frac{1}{2}\left[\frac{2d^2+2d-2}{(d-1)(d+1)(d+2)} + \frac{1}{(d+1)(d+2)}\right] \\ &= \frac{1}{2}\left[\frac{d^2+3d-3}{(d-1)(d+1)(d+2)}\right] \end{aligned} \tag{3.70}$$

Avendo che:

$$d \geq 1 \Rightarrow \frac{d^2+3d-3}{(d-1)(d+1)(d+2)} \leq 1 \tag{3.71}$$

si ha che anche in questo caso

$$F \leq \frac{1}{2} \tag{3.72}$$

Possiamo quindi concludere dopo il calcolo esplicito che, in dimensione finita, nessuna macchina quantistica universalmente covariante approssima sovrappositore ortogonale a due ingressi di pari ampiezza. meglio della banale operazione di traccia parziale rispetto a uno qualsiasi dei due canali di ingresso.

3.2 Sovrappositore generalizzato

Fissato $\mathcal{H} \in \mathbf{Hilb}(\mathbb{C})$ tale che $d \doteq \dim \mathcal{H} \in \mathbb{N}$, poniamo

$$\mathcal{S} \doteq \{|i\rangle \in \mathcal{H} : \langle i|i\rangle = 1, \quad i = 1, \cdots, m \leq d\}$$

ed associamo ad ogni $|i\rangle \in \mathcal{S}$ un numero reale positivo p_i in modo tale che

$$\sum_{i,j=1}^{m} p_i p_j \langle i|j\rangle^N = 1. \tag{3.73}$$

Andiamo a studiare le operazioni quantistiche corrispondenti all'applicazione da $\mathcal{H}^{\otimes mM}$ a $\mathcal{H}^{\otimes N}$ (con $N, M \in \mathbb{N}$):

$$\bigotimes_{i=1}^{m} |i\rangle^{\otimes M} \longmapsto \sum_{i=1}^{m} p_i |i\rangle^{\otimes N} \tag{3.74}$$

Possiamo fare immediatamente le seguenti osservazioni:

- Il vincolo imposto sulle p_i garantisce la normalizzazione dello stato di output; infatti il primo membro della (3.73) è proprio l'espressione della sua norma quadra.

- Aver posto reali i p_i non costituisce un limite alla scelta delle fasi relative dell'output; infatti rifasando opportunamente a uno a uno i $|i\rangle \in \mathcal{S}$ si possono imporre fasi relative abritrarie per output corrispondenti ad uno stesso input fisico (una trasformazione di fase su un vettore in $\mathcal{H}$ lascia invariante il proiettore corrispondente)

- Per $m = 1$ l'applicazione mappa M copie di uno stato in N copie dello stesso stato; quindi per $M < N, m = 1$ la (3.74), meglio se opportunamente estesa tramite un vincolo di covarianza, rappresenta una particolare clonazione quantistica.

- In particolare per $M = N = 1$ e più in generale per $M = N$, l'applicazione in studio mappa m stati di $\mathcal{H}$ nella loro sovrapposizione, con

fasi relative date dalle fasi relative $\langle i|j\rangle$ dei vettori in $\mathcal{S}$, e "pesi" dati dall'insieme dei p_i. Qualsiasi sovrappositore si costruisce imponendo vincoli della forma della (3.74), con $M = N = 1$. Per questo sembra opportuno chiamare una macchina quantistica costruita a partire dal vincolo in studio **sovrappositore generalizzato**.

- Una macchina quantistica soddisfacente il vincolo può essere usata per creare entanglement: per esempio, se $\mathcal{S}$ è contenuto in una base ortonormale e $M < N$, l'output è uno stato entangled con numero di Schmidt pari alla cardinalità di $\mathcal{S}$.

- Non stiamo prendendo in considerazione un'applicazione definita ma una classe di applicazioni; a meno di isomorfismi naturali, i parametri che determinano univocamente un'applicazione all'interno della classe sono $d, M, N \in \mathbb{N}$, l'insieme $\mathcal{S} \subset \mathcal{H}$ e la mappa $p_i : \mathcal{S} \to \mathbb{R}^+$

È chiaro che applicare, così com'è scritto, un unico vincolo della forma (3.74) significa imporre all'output della macchina una sovrapposizione generalizzata solo per lo stato di input specificato. Una condizione di questo tipo può sempre essere soddisfatta tramite una macchina quantistica deterministica: un esempio banale è la preparazione dello stato di output selezionato dal vincolo. Di conseguenza per imporre una condizione che abbia un qualche contenuto fisico (definire "sovrappositore" una preparazione suona poco sensato; inoltre, si vede subito come per *qualsiasi* preparazione (pura) sia possibile trovare un insieme ordinato $\mathcal{S}$ e una distribuzione di pesi p_i tali che la preparazione soddisfi un vincolo della forma (3.74) è necessario imporre vincoli di tipo (3.74) a più insiemi $\mathcal{S}$ oppure, forse più significativamente, aggiungere a uno di questi una condizione di covarianza (2.3), estendendo il vincolo di partenza all'orbita di $\mathcal{S}$ rispetto alla rappresentazione scelta. Questo secondo approccio è quello che abbiamo seguito.

Abbiamo preso in esame il caso covariante in fase, ossia – fissata in $\mathcal{H}$ una base $\mathcal{B}_{\text{Num}} \doteq \{|n\rangle \in \mathcal{H}, \quad n = 0, \ldots, d-1\}$, detta **base numero** – rispetto alla rappresentazione di $\mathcal{U}(1)$ su $\mathcal{H}$ data da:

$$U_{\Phi}|n\rangle = e^{\mathrm{i}n\Phi}|n\rangle \tag{3.75}$$

Si dimostra inoltre facilmente che vale:

$$U_{\Phi}^{\otimes M} = \sum_{N=0}^{M(d-1)} e^{\mathrm{i}N\Phi} P_N \tag{3.76}$$

dove

$$P_N \doteq \sum_{(n_1,\ldots,n_M)\in\mathcal{I}_N} |n_1\rangle \cdots |n_M\rangle\langle n_1| \cdots \langle n_M| \tag{3.77}$$

con

$$\mathbb{N}^M \supset \mathcal{I}_N \doteq \left\{ (n_1, \ldots, n_M) \quad : \quad \sum_{i=1}^{M} n_i = N \right\} \qquad , \qquad |n_i\rangle \in \mathcal{B}_{\text{Num}}.$$

Gli stati corrispondenti ai vettori $|n\rangle \in \mathcal{B}_{\text{Num}}$ sono detti **stati numero**.

Le rappresentazioni irriducibili della fase sono sempre monodimensionali; esse sono tutte reciprocamente inequivalenti nel caso della rappresentazione definente, mentre il prodotto tensoriale introduce $M(d-1)$ classi di equivalenza, ognuna con degenerazione pari alla cardinalità del relativo $\mathcal{I}_N$. Questo porta a trovare un elevato numero di parametri nella descrizione dello spazio degli R covarianti, complicando anche notevolmente la ricerca coi metodi standard di un estremo superiore per la fidelity: pertanto ci siamo limitati allo studio di alcuni sottocasi particolari.

3.2.1 Sovrappositore di stati numero

Consideriamo il caso $\mathcal{S} \subset \mathcal{B}_{\text{Num}}$.
In particolare avremo

$$\mathcal{S} \doteq \{|n_i\rangle \in \mathcal{B}_{\text{Num}}, \quad i = 1, \ldots, m \leq d\} \tag{3.78}$$

con

$$n_i \in \{0, \ldots, d-1\} \subset \mathbb{N} \quad \forall i \qquad , \qquad i \neq j \Rightarrow n_i \neq n_j \tag{3.79}$$

Sia $\mathcal{E}$ una CP-Map da $\mathcal{B}(\mathcal{H}^{\otimes mM})$ in $\mathcal{B}(\mathcal{H}^{\otimes N})$ covariante in fase, e definiamo

$$|IN\rangle \doteq \bigotimes_{i=1}^{m} |n_i\rangle^{\otimes M} \qquad , \qquad |XOUT\rangle \doteq \sum_{i=1}^{m} p_i |n_i\rangle^{\otimes N}$$

in cui simboli non altrimenti definiti hanno lo stesso significato che nella (3.74). Possiamo allora dimostrare che, posti $\rho_{IN} = |IN\rangle\langle IN|$ e $\rho_{OUT} = |XOUT\rangle\langle XOUT|$ vale la disuguaglianza:

$$F(\mathcal{E}(\rho_{IN}), \rho_{OUT}) \leq \max p_i^2 \tag{3.80}$$

Dimostrazione del limite superiore

Ricordiamo a questo proposito due risultati che ci saranno utili nel seguito:

Proposizione 3.1 *Sia $\mathcal{E}$ una Quantum Operation genericamente covariante rispetto alle rappresentazioni del gruppo $\mathcal{G}$ $\{V_g\}$ e $\{U_g\}$, rispettivamente sull'output e sull'input. Se per uno stato ρ dello spazio di input si ha $U_g \rho U_g^\dagger = \rho$ per qualche $g \in \mathcal{G}$, allora sarà anche $V_g \mathcal{E}(\rho) V_g^\dagger = \mathcal{E}(\rho)$.*

Dimostrazione. Banalmente, per il g dell'ipotesi:

$$V_g \mathcal{E}(\rho) V_g^\dagger = \mathcal{E}(U_g \rho U_g^\dagger) = \mathcal{E}(\rho)$$

Dove si è usata la covarianza nel passaggio dal primo al secondo membro, e l'invarianza di ρ rispetto a U_g dal secondo al terzo.□

Proposizione 3.2 *Siano $\{a_i\}, \{b_i\}$ due n-uple di numeri reali, con $a_i \geq 0$. Allora*

$$\sum_{i=1}^{n} a_i b_i \leq \sum_{i=1}^{n} a_i \max\{b_j\}.$$

Dimostrazione (schema). Per la positività di a_i, si ha che $a_i b_i \leq a_i \max\{b_i\}\, \forall i$, e in particolare $a_1 b_1 \leq a_1 \max\{b_j\}$. Da qui, ricordando che $a \leq c, b \leq d \Rightarrow a + b \leq c + d$, si può procedere per induzione a dimostrare la tesi.□

Passiamo ora a dimostrare la (3.80):

Dimostrazione. Essendo ρ_{OUT} uno stato puro si può scrivere:

$$F(\mathcal{E}(\rho_{IN}), \rho_{OUT}) = \langle XOUT|\mathcal{E}(\rho_{IN})|XOUT\rangle \tag{3.81}$$

che esplicitando $|XOUT\rangle$ diventa

$$F(\mathcal{E}(\rho_{IN}), \rho_{OUT}) = \sum_{i,j=1}^{m} p_i p_j \langle n_i|^{\otimes N} \mathcal{E}(\rho_{IN}) |n_j\rangle^{\otimes N}. \tag{3.82}$$

Lo stato di input ρ_{IN}, essendo il prodotto tensore di stati numero, è invariante rispetto a trasformazioni di fase. Questo permette di dedurre, tramite la proposizione 3.1, che:

$$\forall \Phi \in [0, 2\pi[\quad V_\Phi \mathcal{E}(\rho_{IN}) V_\Phi^\dagger = \mathcal{E}(\rho_{IN}) \tag{3.83}$$

Con $V_\Phi \doteq U_\Phi^{\otimes N}$. Prendiamo ora in considerazione gli elementi di matrice di $\mathcal{E}(\rho_{IN})$ rispetto al set ortonormale $\left\{|n\rangle\!\rangle \doteq |n\rangle^{\otimes N}, \quad |n\rangle \in \mathcal{B}_{\text{Num}}\right\}$. Per la (3.83) troviamo che

$$\forall \Phi \in [0, 2\pi[\quad \langle\!\langle m|\mathcal{E}(\rho_{IN})|n\rangle\!\rangle = \langle\!\langle m|V_\Phi \mathcal{E}(\rho_{IN}) V_\Phi^\dagger|n\rangle\!\rangle \tag{3.84}$$

Ricordando che $V_\Phi^\dagger |n\rangle\!\rangle = e^{-\mathrm{i}Nn\Phi}$, possiamo riscrivere

$$\forall \Phi \in [0, 2\pi[\quad \langle\!\langle m|\mathcal{E}(\rho_{IN})|n\rangle\!\rangle = e^{\mathrm{i}N(m-n)\Phi} \langle\!\langle m|\mathcal{E}(\rho_{IN})|n\rangle\!\rangle \tag{3.85}$$

Da cui possiamo dedurre

$$m \neq n \Rightarrow \langle\!\langle m|\mathcal{E}(\rho_{IN})|n\rangle\!\rangle = 0 \tag{3.86}$$

notando che per $m \neq n$ esiste sempre un $\Phi \in [0, 2\pi[$ tale che $e^{\mathrm{i}N(m-n)\Phi} \neq 1$.[2]

[2] È possibile dedurre la (3.86) anche integrando membro a membro in Φ la (3.85), o equivalentemente mediando la (3.84) sul gruppo. Ho preferito però non ricorrere all'integrale per analogia al procedimento adottato nelle sezioni successive

Per la (3.86) e l'iniettività di $\{n_i\}$, la (3.82) si riscrive immediatamente:

$$F(\mathcal{E}(\rho_{IN}), \rho_{OUT}) = \sum_{i=1}^{m} p_i^2 \langle\langle n_i|\mathcal{E}(\rho_{IN})|n_i\rangle\rangle. \tag{3.87}$$

Applicando al secondo membro la proposizione 3.2 otteniamo

$$F(\mathcal{E}(\rho_{IN}), \rho_{OUT}) \leq \sum_{i=1}^{m} \langle\langle n_i|\mathcal{E}(\rho_{IN})|n_i\rangle\rangle \max\left\{p_j^2\right\}. \tag{3.88}$$

Inoltre $\mathrm{Tr}_{\mathcal{E}(\rho_{IN})}\,[\leq]\,1$ implica con la positività di $\mathcal{E}(\rho_{IN})$ che

$$\sum_{i=1}^{m} \langle\langle n_i|\mathcal{E}(\rho_{IN})|n_i\rangle\rangle \leq 1$$

per cui possiamo scrivere

$$F(\mathcal{E}(\rho_{IN}), \rho_{OUT}) \leq \max\left\{p_j^2\right\} \tag{3.89}$$

che è equivalente alla (3.80).□

Osservazioni

- Il risultato si estende banalmente a qualsiasi sovrappositore (generalizzato) ortogonale covariante rispetto a $\mathcal{SU}(d \doteq \dim \mathcal{H})$. Basta notare che dato un qualunque set ortonormale $\mathcal{S} \subset \mathcal{H}$, $\mathcal{SU}(d)$ ammette semprecome sottogruppo una rappresentazione della fase $\left\{e^{-\mathrm{i}\frac{d-1}{2}\Phi} U_\Phi\right\}$, in cui le U_Φ sono definite come nella (3.75), tale per cui $\mathcal{S} \subset \mathcal{B}_{\mathrm{Num}}$.

- Sia per la fase che per $\mathcal{SU}(d)$ (e di conseguenza per qualunque altro gruppo) esiste una macchina quantistica covariante che raggiunge il limite fissato dalla (3.80). Si realizza semplicemente scartando tutti i sistemi di input tranne quello corrispondente al canale di massima ampiezza nell'output (matematicamente è una traccia parziale, fisicamente è sufficiente appunto ignorare gli altri sistemi e considerare quello privilegiato come l'output della macchina), ed è universalmente covariante in maniera manifesta.

- Questa macchina non è in generale l'unica. Per esempio, se $m = d$ e $p_i = \frac{1}{\sqrt{d}} \forall i$, anche le preparazioni dello stato massimamente caotico massimizzano la fidelity.

- La natura delle operazioni ottimali viste finora (scartare dei sistemi dall'input, prendere uno stato a caso) chiarisce il significato fisico del limite qui ricavato: quando è verificato, non si puo' approssimare meglio la sovrapposizione in maniera covariante che restituendo come output uno degli stati da sovrapporre, cioè non sovrapponendo affatto.

Una negazione tanto decisa della possibilità di sovrapporre stati ortogonali in maniera covariante rispetto a certi gruppi – giungente addirittura a proibire di fatto anche una sovrapposizione approssimata – porta naturalmente a sospettare l'intervento di qualche principio fisico che sarebbe altrimenti violato. Le ipotesi sotto cui è stata ricavata la (3.80), cioè che si stia cercando di mappare un insieme di stati invarianti rispetto a $\mathcal{G}$ in una loro sovrapposizione che in generale non lo è, unite al fatto che la fidelity massima aumenti col diminuire della "sensibilità" alle trasformazioni di fase dell'output atteso e diventi uno proprio quando questo è invariante, suggerirebbero la violazione di qualche principio di natura informatica tramite la creazione di informazione sulla fase.

3.2.2 Qubit

Il successivo caso da noi preso in considerazione è quello del sovrapposito re ortogonale equipesato covariante in fase per il qubit, sufficientemente semplice da permettere di ricavare un risultato anche col metodo di calcolo diretto già usato nella sezione 2.

Posti $a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1$, possiamo ai nostri scopi scrivere il generico qubit e il suo complemento ortogonale rispettivamente come

$$a|0\rangle + b|1\rangle \tag{3.90}$$

e

$$b^*|0\rangle - a^*|1\rangle \tag{3.91}$$

con $\mathcal{B}_{\text{Num}} = \{|0\rangle, |1\rangle\}$.
Il generico stato di input sarà quindi il loro prodotto tensore:

$$|IN\rangle \doteq ab^*|00\rangle - |a|^2|01\rangle + |b|^2|10\rangle - ba^*|11\rangle \tag{3.92}$$

La forma del problema fa pensare che possa essere conveniente adottare come base per lo spazio di input $\mathcal{B} \doteq \left\{|00\rangle, |A\rangle \doteq \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), |B\rangle \doteq \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right), |11\rangle\right\}$[3].
In questa base lo stato di input si riscrive:

$$|IN\rangle = ab^*|00\rangle + \frac{|b|^2 - |a|^2}{\sqrt{2}}|A\rangle + \frac{1}{\sqrt{2}}|B\rangle - ba^*|11\rangle \tag{3.93}$$

Lo stato di output che vogliamo approssimare sarà invece dato dalla sovrapposizione di (3.90) e (3.91), ossia

$$|XOUT\rangle = \frac{1}{\sqrt{2}}\left(\left(a + b^*\right)|0\rangle + \left(b - a^*\right)|1\rangle\right) \tag{3.94}$$

$\mathcal{B} \otimes \mathcal{B}_{\text{Num}}$ è una base di $\mathcal{IN} \otimes \mathcal{OUT}$; inoltre i suoi elementi giacciono ciascuno su un diverso sottospazio invariante sotto l'azione di $\{U_\Phi^* \otimes U_\Phi^* \otimes U_\Phi\}$, permettendoci di classificarli immediatamente.

La CP-Map covariante in studio è associata ad un operatore positivo su $\mathcal{IN} \otimes \mathcal{OUT}$ diagonalizzabile simultaneamente a $\hat{N}$. Se restringiamo la nostra ricerca agli operatori covarianti estremali, un risultato dovuto a Giulio Chiribella garantisce per il nostro caso che R ammetterà al più due autovalori

[3]Si noti che span $\{|A\rangle\}$ e span $\{|B\rangle\}$ sono invarianti rispetto a U_Φ, e che le rappresentazioni irriducibili definite su di essi sono equivalenti tra loro e a quelle su span $\{|01\rangle\}$ e span $\{|10\rangle\}$.

non nulli per ogni autospazio dell'operatore numero.[4] Pertanto possiamo scrivere

$$R = r^{(1)}P^{(1)} + r^{(-2)}P^{(-2)} + \sum_{\mu=-1}^{0}\sum_{i=1}^{2} r_i^{(\mu)}P_i^{(\mu)} \tag{3.95}$$

La traccia sull'output si scrive:

$$\begin{pmatrix} r^{(1)} + |u_{i1}|^2 r_i^{(0)} & 0 & 0 & 0 \\ 0 & |u_{i2}|^2 r_i^{(0)} + |v_{i2}|^2 r_i^{(-1)} & u_{i2}u_{i3}^* r_i^{(0)} + v_{i2}v_{i3}^* r_i^{(-1)} & 0 \\ 0 & u_{i3}u_{i2}^* r_i^{(0)} + v_{i3}v_{i2}^* r_i^{(-1)} & |u_{i3}|^2 r_i^{(0)} + |v_{i3}|^2 r_i^{(-1)} & 0 \\ 0 & 0 & 0 & r^{(-2)} + |v_{i1}|^2 r_i^{(-1)} \end{pmatrix}$$

in cui è sottointesa e lo sarà d'ora in poi la somma sugli indici ripetuti, e i $u_{1i}, u_{2i}, v_{1i}, v_{2i} \in \mathbb{C}^3$, con

$$u_{ij}u_{jk}^* = \delta_{ik} \qquad , \qquad v_{ij}v_{jk}^* = \delta_{ik} \tag{3.96}$$

rappresentano i gradi di libertà nella scelta dei proiettori $P_i^{(\mu)}$. Il vincolo

[4] Si confronti l'osservazione a pagina 57. Nel caso in studio, basta osservare che, per ciascuna classe di equivalenza tre volte degenere, i nove operatori sullo spazio di input che si vorrebbero linearmente indipendenti affinchè nessun autovalore di R si annulli appartengono a span $\{|0\rangle\langle 0|, |A\rangle\langle A|, |B\rangle\langle B|, |A\rangle\langle B|, |B\rangle\langle A|\}$, che è uno spazio vettoriale a cinque dimensioni.

Autovalore	1	0	-1	-2
Base	$\|00\rangle\|1\rangle$	$\|00\rangle\|0\rangle$	$\|11\rangle\|1\rangle$	$\|11\rangle\|0\rangle$
		$\|A\rangle\|1\rangle$	$\|A\rangle\|0\rangle$	
		$\|B\rangle\|1\rangle$	$\|B\rangle\|0\rangle$	

Tabella 3.1: Classificazione degli autospazi dell'operatore numero totale $\hat{N}$

trace preserving si riduce quindi a cinque equazioni:

$$r^{(1)} + |u_{i1}|^2 r_i^{(0)} = 1 \tag{3.97a}$$

$$|u_{i2}|^2 r_i^{(0)} + |v_{i2}|^2 r_i^{(-1)} = 1 \tag{3.97b}$$

$$|u_{i3}|^2 r_i^{(0)} + |v_{i3}|^2 r_i^{(-1)} = 1 \tag{3.97c}$$

$$r^{(-2)} + |v_{i1}|^2 r_i^{(-1)} = 1 \tag{3.97d}$$

$$u_{i2} u_{i3}^* r_i^{(0)} + v_{i2} v_{i3}^* r_i^{(-1)} = 0 \tag{3.97e}$$

Poniamo $|\sigma\rangle \doteq \sqrt{2}|IN\rangle^*|XOUT\rangle$, dove l'operazione di coniugazione complessa è riferita, come quella già effettuata sulla rappresentazione della fase sullo spazio di input, alla base numero, cioè:

$$|IN\rangle^* = ba^*|00\rangle + \frac{|b|^2 - |a|^2}{\sqrt{2}}|A\rangle + \frac{1}{\sqrt{2}}|B\rangle - ab^*|11\rangle \tag{3.98}$$

Tenendo presenti la (3.98), la (3.94), e i gradi di libertà nella scelta dei proiettori abbiamo

$$\langle\sigma|P^{(1)}|\sigma\rangle = |ab^*(b - a^*)|^2 \tag{3.99}$$

$$\begin{aligned}\langle\sigma|P_i^{(0)}|\sigma\rangle = |u_{i1}|^2|ba^*(a + b^*)|^2 + \frac{|b - a^*|^2}{2}[|u_{i2}|^2(|b|^2 - |a|^2)^2 + \\ + 2\Re u_{i2}u_{i3}^*(|b|^2 - |a|^2) + |u_{i3}|^2] + \\ + 2\Re[(a + b^*)ba^*(b^* - a)\frac{|b|^2 - |a|^2}{\sqrt{2}}(u_{i1}u_{i2}^* + u_{i1}u_{i3}^*)]\end{aligned} \tag{3.100}$$

$$\begin{aligned}\langle\sigma|P_i^{(-1)}|\sigma\rangle = |v_{i1}|^2|ba^*(b - a^*)|^2 + \frac{|a + b^*|^2}{2}[|v_{i2}|^2(|b|^2 - |a|^2)^2 + \\ + 2\Re v_{i2}v_{i3}^*(|b|^2 - |a|^2) + |v_{i3}|^2] \\ - 2\Re[(b - a^*)ab^*(a^* + b)\frac{|b|^2 - |a|^2}{\sqrt{2}}(v_{i1}v_{i2}^* + v_{i1}v_{i3}^*)]\end{aligned} \tag{3.101}$$

$$\langle\sigma|P^{(-2)}|\sigma\rangle = |ba^*(a + b^*)|^2 \tag{3.102}$$

Sostituendo nell'espressione della fidelity

$$F = \frac{1}{2}[\langle\sigma|r^{(1)}P^{(1)}|\sigma\rangle + \langle\sigma|r^{(-2)}P^{(-2)}|\sigma\rangle + \sum_{\mu=-1}^{0}\sum_{i=1}^{2}\langle\sigma|r_i^{(\mu)}P_i^{(\mu)}|\sigma\rangle], \quad (3.103)$$

raccogliendo opportunamente e sfruttando solo proprietà banali della coniugazione complessa ($|z| = |z^*| \quad , \quad \Re z = \Re z^*$) si ottiene:

$$\begin{aligned}
F = \frac{1}{2}\Big\{ & |ab^*|^2 \Big[|b-a^*|^2 r^{(1)} + |a+b^*|^2|u_{i1}|^2 r_i^{(0)} + |a+b^*|^2 r^{(-2)} \; + \\
& + |b-a^*|^2|v_{i1}|^2 r_i^{(-1)}\Big] + \\
& + \frac{\left(|b|^2-|a|^2\right)^2}{2}\left(|b-a^*|^2|u_{i2}|^2 r_i^{(0)} + \; |a+b^*|^2|v_{i2}|^2 r_i^{(-1)}\right) + \\
& + \frac{1}{2}\left(|b-a^*|^2|u_{i3}|^2 r_i^{(0)} + |a+b^*|^2|v_{i3}|^2 r_i^{(-1)}\right) + \\
& + \left(|b|^2-|a|^2\right)\left(|b-a^*|^2 \Re u_{i2}u_{i3}^* r_i^{(0)} + |a+b^*|^2 \Re v_{i2}v_{i3}^* r_i^{(-1)}\right) + \\
& + \sqrt{2}\Re(a+b^*)ba^*(b^*-a)\Big[\left(|b|^2-|a|^2\right)\left(u_{i1}u_{i2}^* r_i^{(0)} - v_{i1}v_{i2}^* r_i^{(-1)}\right) + \\
& + u_{i3}u_{i3}^* r_i^{(0)} - v_{i3}v_{i3}^* r_i^{(-1)}\Big]\Big\}
\end{aligned} \quad (3.104)$$

L'espressione si può ulteriormente semplificare, ma rimane di massimizzazione non immediata

3.3 Generalizzazione ad altre macchine

Il risultato trovato nella sezione 3.2.1 si può generalizzare ad altri gruppi e ad approssimazioni di macchine di altro tipo con quanto segue:

Teorema 3.1 *Sia $\mathcal{E} \in \mathcal{QO}(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ una quantum operation covariante rispetto a $\{U_g\} \subset \mathcal{B}(\mathcal{H})$ e $\{V_g\} \subset \mathcal{B}(\mathcal{K})$, rappresentazioni unitarie del gruppo di Lie ad un parametro $\mathcal{G}$. Siano $\rho_{\mathcal{H}} \in \mathcal{B}(\mathcal{H})$ uno stato invariante rispetto a $\{U_g\}$, e $|\psi\rangle\langle\psi|$ uno stato puro in $\mathcal{B}(\mathcal{K})$. Sia $A \in \mathcal{B}(\mathcal{K})$ il generatore infinitesimo di $\{V_g\}$, e $\sum_i a_i P_i$ la sua risoluzione spettrale. Se la restrizione di A a*

$\mathcal{J} \doteq \text{span}\{P_i|\psi\rangle\}$ *ha spettro privo di degenerazione, vale*

$$F(\mathcal{E}(\rho_{\mathcal{H}}), |\psi\rangle\langle\psi|) \leq \max_i \langle\psi|P_i|\psi\rangle \tag{3.105}$$

Se inoltre si hanno $\mathcal{J} = \mathcal{K}$ *e* $\langle\psi|P_i|\psi\rangle = p$ *costante, la* (3.105) *diventa*

$$F(\mathcal{E}(\rho_{\mathcal{H}}), |\psi\rangle\langle\psi|) = \frac{1}{\dim \mathcal{K}} \tag{3.106}$$

Dimostrazione. Per la proposizione 3.1, l'invarianza di $\rho_{\mathcal{H}}$ implica

$$\forall g \in \mathcal{G} \qquad V_g \mathcal{E}(\rho_{\mathcal{H}}) V_g^\dagger = \mathcal{E}(\rho_{\mathcal{H}}), \tag{3.107}$$

mentre la Fidelity si scrive

$$F(\mathcal{E}(\rho_{\mathcal{H}}), |\psi\rangle\langle\psi|) = \text{Tr}\left[\mathcal{E}(\rho_{\mathcal{H}})|\psi\rangle\langle\psi|\right] = \langle\psi|\mathcal{E}(\rho_{\mathcal{H}})|\psi\rangle.$$

Dato che $\{P_i\}$ è una risoluzione dell'identità:

$$F(\mathcal{E}(\rho_{\mathcal{H}}), \rho_{\mathcal{K}}) = \langle\psi| \left(\sum_i P_i\right) \mathcal{E}(\rho_{\mathcal{H}}) \left(\sum_j P_j\right) |\psi\rangle. = \sum_{i,j,} \langle\psi|P_i \mathcal{E}(\rho_{\mathcal{H}}) P_j|\psi\rangle$$

Consideriamo ora una trasformazione V_g in un intorno dell'identità. V_g potrà essere scritta tramite la mappa esponenziale come segue:

$$V_g = e^{\mathrm{i}A\phi(g)},$$

in cui $\phi : \mathcal{G} \to \mathbb{R}$ è la parametrizzazione di $\mathcal{G}$ da cui si è ricavato A. In particolare si avrà che $V_g P_i|\psi\rangle = e^{\mathrm{i}a_i\phi(g)} P_i|\psi\rangle$.

Quindi dalla (3.107) discende

$$\exists \epsilon > 0 : \forall \phi \in]-\epsilon, \epsilon[\qquad \langle\psi|P_i\mathcal{E}(\rho_{\mathcal{H}})P_j|\psi\rangle = e^{\mathrm{i}(a_i - a_j)\phi} \langle\psi|P_i\mathcal{E}(\rho_{\mathcal{H}})P_j|\psi\rangle,$$

da cui si deduce che $\langle\psi|P_i\mathcal{E}(\rho_{\mathcal{H}})P_j|\psi\rangle \neq 0 \Rightarrow i = j$. Infatti per $\langle\psi|P_i\mathcal{E}(\rho_{\mathcal{H}})P_j|\psi\rangle \neq 0$ l'equazione precedente equivale a

$$\exists \epsilon > 0 : \forall \phi \in]-\epsilon, \epsilon[\quad 1 = e^{\mathrm{i}(a_i - a_j)\phi},$$

che è verificata solo per $a_i = a_j$. Ma $a_i = a_j \iff i = j$ per costruzione. Quindi l'espressione della fidelity diventa

$$F(\mathcal{E}(\rho_{\mathcal{H}}), |\psi\rangle\langle\psi|) = \sum_i \langle\psi|P_i\mathcal{E}(\rho_{\mathcal{H}})P_i|\psi\rangle$$

Posto $|\psi_i\rangle \doteq \frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$ per tutti i $P_i|\psi\rangle \neq 0$, risulta evidente che $\mathcal{B}_{\mathcal{J}} \doteq \{|\psi_i\rangle\}$ costituisce una base ortonormale di $\mathcal{J}$. La fidelity si riscrive:

$$F(\mathcal{E}(\rho_{\mathcal{H}}), |\psi\rangle\langle\psi|) = \sum_i \langle\psi|P_i|\psi\rangle\langle\psi_i|\mathcal{E}(\rho_{\mathcal{H}})|\psi_i\rangle \tag{3.108}$$

Per la proposizione 3.2 allora si ha:

$$F(\mathcal{E}(\rho_{\mathcal{H}}), |\psi\rangle\langle\psi|) \leq \max_i \langle\psi|P_i|\psi\rangle \left(\sum_j \langle\psi_j|\mathcal{E}(\rho_{\mathcal{H}})|\psi_j\rangle\right) =$$
$$= \max_i \langle\psi|P_i|\psi\rangle \operatorname{Tr}_{\mathcal{J}}[\mathcal{E}(\rho_{\mathcal{H}})] \leq \max_i \langle\psi|P_i|\psi\rangle,$$

che equivale alla (3.105). Se inoltre $\mathcal{J} = \mathcal{K}$ e $\langle\psi|P_i|\psi\rangle = k$ per ogni i, partendo dalla (3.108) si calcola:

$$F(\mathcal{E}(\rho_{\mathcal{H}}), |\psi\rangle\langle\psi|) = \sum_i k\langle\psi_i|\mathcal{E}(\rho_{\mathcal{H}})|\psi_i\rangle = k \operatorname{Tr}_{\mathcal{K}}[\mathcal{E}(\rho_{\mathcal{H}})] = k.$$

Imponendo la normalizzazione di $|\psi\rangle$ scritto sulla base degli $|\psi_i\rangle$ si trova immediatamente $k = \frac{1}{\dim \mathcal{K}}$.□

Conclusioni

Bibliografia

[1] M. A. Nielsen e I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000)

[2] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, NJ (1955)

[3] A. S. Holevo, *Probabilistic and statistical aspects of quantum theory*, Nort-Holland, Amsterdam (1982)

[4] P. Bush, P.J. Lahti, P. Mittelstaedt. *The Quantum Theory of Measurement*, Springer-Verlag (1991)

[5] K. Kraus, *States, effects and operations: fundamental notions of quantum theory*, Lecture notes in Physics **190**, Springer-Verlag (1983)

[6] G. M. D'Ariano e P. Lo Presti, *Optimal Non-Universally Covariant Cloning*, Phys. Rev. A **64** 042308 (2001) - /quant-ph/0101100 (2001)

[7] M. D. Choi, *Completely positive linear maps on complex matrices*, Linear algebra and its applications **10**, 285-290 (1975)

[8] P. Stelmachovic, V. Buzek, *Dynamics of open quantum systems initially entangled with environment: Beyond the Kraus representation*, Phys. Rev. A **64** 062106 - /quant-ph/0108136 (2001)

[9] C. H. Bennet, G. Brassard, C. Crépeau, R. Jozsa, A. Peres e W. Wootters, *Teleporting an unknown quantum state via dual classical and EPR channels*, Phys. Rev. Lett. **70** 1895-1899 (1993)

[10] D. Boschi, S. Branca, F. De Martini, L. Hardy e S. Popescu, *Experimental realization of teleporting an unknown quantum state via dual classical and Einstein-Podolski-Rosen channels*, Phys. Rev. Lett. **80** 1121-1125 - /quant-ph/9710013 (1998)

[11] D. Bouwmeester, J. W. pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, *Experimental quantum teleportation*, Nature **390**(6660) 575-579 (1997)

[12] H. F. Jones, *Groups, representations and physics*, IOP, Bristol (1990)

[13] M. Hammermesh, *Group theory and its application to physical problems*, Dover, New York (1989)

[14] R. T. Rockafellar, *Convex Analysis*, Princeton University Press, Princeton (1970)

[15] F. Valentine, *Convex Sets*, McGraw-Hill, New York (1964)

[16] G. Chiribella, G. M. D'Ariano, P. Perinotti, e M. F. Sacchi, *Covariant quantum measurements which maximize the likelihood*, approvato per la pubblicazione su Phys. Rev A - /quant-ph/0403083 (2004)