Indice

Introduzione

Il processo di misurazione in Fisica Classica veniva dato per "scontato": un dinamometro, un amperometro o un microscopio erano visti semplicemente come ausilio e amplificazione dei sensi umani. Il loro utilizzo si riteneva del tutto ininfluente sull'evoluzione deterministica del sistema fisico che veniva misurato. E in effetti, su scale macroscopiche, questo è vero.

Con l'avvento della Meccanica Quantistica, al contrario, si è capito che il processo di misurazione, in generale, è tutt'altro che innocuo: i Postulati della Misura predicono un comportamento non più deterministico dei risultati, bensì probabilistico secondo una distribuzione di probabilità dipendente dal sistema oggetto della misura. Quest'ultimo, inoltre, è influenzato dalla misurazione stessa, e il suo stato dopo la misurazione è diverso da quello precedente la misurazione.

Oltre alle ben note conseguenze filosofiche, i Postulati della Misura, sempre più perfezionati e generalizzati grazie ai concetti di *POVM* e di *strumento*, hanno portato anche a conseguenze teoriche e tecnologiche di grande impatto: insieme con l'utilizzo dell'*entanglement* (la "macchina delle meraviglie" della Meccanica Quantistica), si è giunti a realizzare il modello teorico (e, in alcuni casi, anche l'apparato strumentale) del teletrasporto, del computer quantistico e della comunicazione e crittografia quantistiche. Alla base di tutto ciò stanno semplicemente i Principi della Misurazione e il Principio

dei Sistemi Composti postulati dalla Meccanica Quantistica.

È chiaro, quindi, come lo studio delle trasformazioni di un sistema quantistico sia fondamentale in quest'ottica di approfondimento. Il lavoro presente sarà incentrato sul concetto di *quantum operation* il quale racchiude in sé la massima generalità. Infatti qualunque evoluzione, unitaria o stocastica, di un sistema quantistico, chiuso o aperto, può essere ottenuta tramite l'applicazione di una *quantum operation*.

Nel **primo capitolo** viene introdotta, con tre diversi approcci (assiomatico, fisico e matematico), la definizione di operazione quantistica. Si presentano, in seguito, i principali risultati teorici noti tra cui le decomposizioni di Kraus e le purificazioni di Neumark. Viene dato spazio anche all'interpretazione fisica della teoria esposta con un'analogia tra *quantum operations* e canali rumorosi classici e con un'applicazione nell'ambito della misurazione quantistica. In coda vengono presentati alcuni esempi di semplici operazioni quantistiche.

Il **secondo capitolo** contiene il principale risultato originale: partendo dalle dilatazioni di Stinespring, di cui si danno le coordinate essenziali, viene presentato un metodo *costruttivo* per ottenere realizzazioni unitarie di *quantum operations* qualsiasi. È noto che mappe *trace-preserving* possono essere ottenute dall'interazione unitaria del sistema con un'*ancilla* la quale, al termine dell'interazione, viene "tracciata via". Tuttavia questo metodo funziona solo per mappe *trace-preserving* con spazi di partenza e di arrivo uguali. Si è allora considerato il caso più generale di mappe *trace-not-increasing* con spazi di partenza e di arrivo generici e si è arrivati alla costruzione esplicita di loro estensioni unitarie. In letteratura non ci risultano trattazioni di queste problematiche.

Nel **terzo capitolo** viene presentata la teoria della maggiorizzazione la

quale consente di ottenere relazioni di "quasi"-ordinamento (l'ordinamento che si ottiene non è, infatti, parziale) tra vettori, anche (sotto opportune ipotesi) appartenenti a spazi di Hilbert di diversa dimensione. Come applicazioni fisiche si citano le funzioni Schur-convesse e un risultato dovuto a Nielsen che permette di classificare tutti gli *ensembles* compatibili con una data matrice-densità. Generalizzando e adattando tale risultato, viene dimostrato un teorema originale di classificazione per tutte le estensioni unitarie di cui al secondo capitolo.

Il **quarto capitolo** introduce brevemente la teoria dei *frames*, sorta di basi over-complete strettamente legate alle trasformazioni isometriche di spazi vettoriali. Al termine, viene presentata un'originale interpretazione fisica della libertà isometrica che esiste nel definire le possibili decomposizioni di Kraus per una mappa come la possibilità di descrivere lo spazio di ancilla tramite basi ortonormali, basi generiche o *frames*.

Nel **quinto capitolo** viene affrontato il problema delle mappe estremali: le *quantum operations*, infatti, formano un insieme convesso e la classificazione dei vertici di quest'ultimo corrisponde a classificare le mappe "non rumorose". Il Teorema di Choi, che fornisce una condizione necessaria e sufficiente per l'estremalità, viene riscritto in termini di mappe ausiliarie, introdotte per la prima volta qui e denominate *mappe ancillari*, le quali possono essere viste come le *quantum operations* indotte sull'ancilla dalla *quantum operation* agente sul sistema principale. Effettivamente risulterà che le mappe estremali sono tutte e sole quelle che possiedono, come corrispettivo ancillare, mappe invertibili.

In chiusura di tesi, nel **sesto capitolo**, viene presentato il problema della distinguibilità tra mappe. L'argomento viene attaccato utilizzando i concetti di distanza tra mappe (ottenuta estendendo la definizione nota di norme di

operatori) e di *fidelity* tra mappe (idea, quest'ultima, valida solo per spazi di Hilbert finiti e proposta da Raginsky).

Convenzioni matematiche

Notazione

- $\langle \cdot | \cdot \rangle$ prodotto scalare euclideo;
- $\| \cdot \|$ norma: per vettori indica quella euclidea; per operatori indica la norma di Schatten $\| \cdot \|_\infty$;
- $\| \cdot \|_{HS}$ norma di Hilbert-Schmidt per operatori corrispondente alla norma di Schatten $\| \cdot \|_2$;
- $\cong$ isomorfismo;
- ^{T} trasposto;
- * complesso coniugato;
- † dagato;
- $^\tau$ duale;
- $\cdot + \cdot$, $\dot{+}$, $\oplus$ somme dirette rispettivamente orizzontale, verticale e diagonale (in genere quest'ultima dicitura si omette e si intende la somma diretta diagonale come somma diretta standard); come esempio $A \cdot + \cdot B = \begin{pmatrix} A & B \end{pmatrix}$, $A \dot{+} B = \begin{pmatrix} A \\ B \end{pmatrix}$, mentre $A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$;

- $\otimes$ prodotto tensore; si segue la convenzione di Kronecker per cui
$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & ... & a_{1n}B \\ a_{21}B & a_{22}B & ... & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & ... & a_{mn}B \end{pmatrix};$$
- a parità di lettera, A indica un operatore, A una mappa da operatori in operatori e A uno spazio di Hilbert o, più genericamente, un insieme;
- $\mathsf{M}_{n,m}$ spazio vettoriale delle matrici $n \times m$;
- $\mathsf{L}(\mathsf{H}, \mathsf{K})$ spazio di Hilbert degli operatori lineari da H in K; per dimensioni finite, esiste un isomorfismo tra $\mathsf{L}(\mathbb{C}^m, \mathbb{C}^n)$ e $\mathsf{M}_{n,m}$ (nota lo scambio di posizione tra gli indici di dimensione);
- $\mathsf{T}(\mathsf{H}, \mathsf{K})$ insieme degli operatori di classe traccia da H in K, cioè tali che $\|T\|_1 < +\infty$;
- $\mathsf{B}(\mathsf{H}, \mathsf{K})$ insieme degli operatori limitati da H in K, cioè tali che $\|B\|_\infty < +\infty$;
- $\mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ insieme delle mappe completamente positive da $\mathsf{B}(\mathsf{K})$ in $\mathsf{B}(\mathsf{H})$ con $I_\mathsf{K} \longmapsto K$; c'è relazione di dualità tra $\mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}))$ e $\mathsf{CP}(\mathsf{T}(\mathsf{H}), \mathsf{T}(\mathsf{K}))$.

Isomorfismo tra operatori e vettori

Sia $A : \mathsf{H} \longrightarrow \mathsf{K}$ un operatore. Si fissino basi ortonormali $\{|h_j\rangle\}$ per H e $\{|k_i\rangle\}$ per K. Si può allora costruire una corrispondenza:

$$A = \sum_{i,j} A_{ij} |k_i\rangle\langle h_j| \longmapsto |A\rangle\!\rangle = \sum_{i,j} A_{ij} |k_i\rangle \otimes |h_j\rangle \tag{1}$$

dove il "doppio ket" $|A\rangle\!\rangle$ indica un vettore in $\mathsf{K} \otimes \mathsf{H}$.

Siano $A : \mathsf{K} \longrightarrow \mathsf{K}$, $B : \mathsf{H} \longrightarrow \mathsf{H}$ e $C : \mathsf{H} \longrightarrow \mathsf{K}$; allora valgono le seguenti:

1. $(A \otimes B)|C\rangle\!\rangle = |ACB^T\rangle\!\rangle$;

2. $\mathrm{Tr}_1 |A\rangle\!\rangle\langle\!\langle B| = A^T B^*$;

3. $\mathrm{Tr}_2 |A\rangle\!\rangle\langle\!\langle B| = AB^\dagger$.

Se $|A\rangle\!\rangle = \sum_{i,j} A_{ij}|k_i\rangle \otimes |h_j\rangle$ allora $\langle\!\langle A| = \sum_{i,j} A^*_{ij}\langle k_i| \otimes \langle h_j|$ e quindi, nelle ipotesi precedenti:

$$(A \otimes B)\langle\!\langle C| = \langle\!\langle A^\dagger C B^*|. \tag{2}$$

È notevole che, se $A, B : \mathsf{H} \longrightarrow \mathsf{K}$, allora $\langle\!\langle A|B\rangle\!\rangle = \mathrm{Tr}[A^\dagger B]$, cioè il prodotto scalare euclideo $\langle\!\langle \cdot|\cdot\rangle\!\rangle$ induce, tramite l'isomorfismo definito in eq.(1), il prodotto scalare di Hilbert-Schmidt tra operatori.

Prodotti tensoriali misti

Si farà uso di prodotti tensoriali anche tra oggetti intrinsecamente diversi, come vettori e matrici. Il procedimento richiama il formalismo tensoriale per il quale sono definiti prodotti tensoriali tra tensori di ordini diversi. Così, ad esempio, per $A \in \mathsf{M}_{n,m}$ e $|v\rangle \in \mathbb{C}^k$, si ha, seguendo la convenzione di

Kronecker:

$$A \otimes |v\rangle = \begin{pmatrix} a_{11}v_1 & a_{12}v_1 & ... & a_{1m}v_1 \\ a_{11}v_2 & a_{12}v_2 & ... & a_{1m}v_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{11}v_k & a_{12}v_k & ... & a_{1m}v_k \\ a_{21}v_1 & a_{22}v_1 & ... & a_{2m}v_1 \\ a_{21}v_2 & a_{22}v_2 & ... & a_{2m}v_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}v_k & a_{n2}v_k & ... & a_{nm}v_k \end{pmatrix} \tag{3}$$

e

$$|v\rangle \otimes A = \begin{pmatrix} v_1 A \\ v_2 A \\ \vdots \\ v_k A \end{pmatrix}. \tag{4}$$

Analogamente si scrive il prodotto tensore tra una matrice e un bra e viceversa.

Capitolo 1

Quantum operations

1.1 Introduzione e nozioni generali

Con il termine *quantum operations* (*QO*'s) si intendono gli strumenti matematici utilizzati per descrivere una qualsiasi evoluzione di un sistema quantistico, sia essa unitaria (un'evoluzione libera di un sistema chiuso) o stocastica (come avviene, ad esempio, in un processo di misura).

Vi sono diversi modi per caratterizzare una QO: assiomatizzando le sue proprietà; introducendo la generalizzazione di un'interazione unitaria tra il sistema e un *environment* (ambiente); utilizzando rappresentazioni che automaticamente identificano la QO in maniera univoca (come la rappresentazione di Kraus).

1.1.1 Definizione assiomatica

Definizione 1 *Una mappa $\mathcal{E}$ da stati $\rho \in \mathsf{T}(\mathsf{H})$ in stati $\mathcal{E}(\rho) \in \mathsf{T}(\mathsf{K})$ è una* quantum operation *se soddisfa i seguenti assiomi:*

- ***A1****:* $\mathrm{Tr}[\mathcal{E}(\rho)]$ *rappresenta la probabilità che avvenga il processo descrit-*

to da $\mathcal{E}$ quando ρ è lo stato iniziale. Quindi deve essere $0 \leq \mathrm{Tr}[\mathcal{E}(\rho)] \leq 1$ *per ogni* ρ.

- ***A2****: la mappa deve essere lineare nelle combinazioni lineari convesse di stati, cioè* $\mathcal{E}(\sum_i p_i\rho_i) = \sum_i p_i\mathcal{E}(\rho_i)$ [1].

- ***A3****: la mappa deve essere* completamente positiva *(abbreviato* CP*); cioè la mappa $\mathcal{E}$ deve essere positiva come pure la mappa estesa $\mathcal{E} \otimes \mathcal{I}$, dove $\mathcal{I}$ è la mappa identica su un qualunque altro spazio di Hilbert.*

Per completare la definizione sono necessari alcuni commenti.

Assioma1. La prima proprietà richiesta è necessaria per raccordarsi al caso generale di *state reduction* originata da una misurazione. La situzione in cui si ha un processo deterministico (che avviene cioè con probabilità unitaria) è rappresentata dalle cosiddette QO's *trace-preserving*: una QO è trace-preserving nel caso in cui $\mathrm{Tr}[\mathcal{E}(\rho)] = 1$. Bisogna sottolineare che una QO trace-preserving non è necessariamente un'evoluzione unitaria. Basti pensare al caso di una misurazione alla von Neumann di cui si ignora (o non si legge) il risultato: questa è sicuramente una QO trace-preserving ma la coerenza è distrutta in quanto sopravvivono soltanto gli elementi diagonali della matrice densità.

Assioma2. Anche la seconda proprietà nasce dalla richiesta di descrivere misurazioni nella situazione in cui queste siano effettuate su stati miscela del tipo $\{p_i, \rho_i\}$ con $\rho = \sum_i p_i\rho_i$. In questo caso si ha

$$\mathcal{E}(\rho) = p(\mathcal{E}) \sum_i p(i|\mathcal{E}) \frac{\mathcal{E}(\rho_i)}{\mathrm{Tr}[\mathcal{E}(\rho_i)]} \tag{1.1}$$

dove $p(\mathcal{E})$ è la probabilità che avvenga il processo $\mathcal{E}$, mentre $p(i|\mathcal{E})$ è la probabilità condizionata che lo stato preparato sia ρ_i dato per avvenuto il

[1] Questa condizione, insieme con $\mathcal{E}(0) = 0$, assicura la linearità della mappa.

processo $\mathcal{E}$. Utilizzando la regola di Bayes per le probabilità condizionate per cui

$$p(i|\mathcal{E}) = \frac{\mathrm{Tr}[\mathcal{E}(\rho_i)]p_i}{p(\mathcal{E})}, \tag{1.2}$$

si ottiene la condizione postulata.

Assioma3. L'ultima proprietà discende dalla richiesta che la mappa $\mathcal{E}$ porti stati fisici in stati fisici: in altre parole, deve mantenere la positività degli stati anche in presenza di spazi di Hilbert estesi (eventualmente con *entanglement*). La completa positività è più forte della semplice positività: un esempio di mappa positiva ma non completamente positiva è dato dall'operatore di trasposizione [1]. Sia $\mathsf{H} = \mathbb{C}^2$ e, fissata una base, sia $\mathcal{T} : \rho \longrightarrow \rho^T$ la mappa trasposizione. Chiaramente questa è una mappa positiva. Tuttavia non è completamente positiva. Si consideri infatti lo stato di singoletto $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$ e gli si applichi la mappa estesa; si ha:

$$\begin{aligned} &\mathcal{T} \otimes \mathcal{I}(|\psi\rangle\langle\psi|) = \\ &= \frac{1}{2}(|0\rangle\langle 0| \otimes |1\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0| - |1\rangle\langle 0| \otimes |1\rangle\langle 0| - |0\rangle\langle 1| \otimes |0\rangle\langle 1|). \end{aligned} \tag{1.3}$$

Lo stato ottenuto non è positivo in quanto, posto $|v\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$, si ha

$$\langle v|\ \mathcal{T} \otimes \mathcal{I}(|\psi\rangle\langle\psi|)\ |v\rangle = -\frac{1}{4}. \tag{1.4}$$

1.1.2 *Quantum operations* e interazione con un *environment*

Si era detto che è possibile introdurre il concetto di QO anche partendo da un'interazione tra il sistema e l'ambiente. È noto come l'evoluzione di un sistema *chiuso* avvenga tramite un operatore unitario. Partendo da questo

fatto, un modo naturale per descrivere la dinamica di un sistema *aperto* è quello di vedere l'evoluzione del sistema come originata da un'interazione tra il sistema principale e l'ambiente. L'insieme *sistema-environment* subisce poi un'evoluzione unitaria al termine della quale viene "tracciato via" l'ambiente. In generale, lo stato finale del sistema ottenuto in questo modo non sarà legato allo stato iniziale da una trasformazione unitaria ma da una QO.

Per cominciare, assumiamo che lo stato di input sistema-environment sia una stato fattorizzato del tipo $\rho \otimes \rho_{env}$ e quindi:

$$\mathcal{E}(\rho) = \mathrm{Tr}_{env}\left[U(\rho \otimes \rho_{env})U^{\dagger}\right]. \tag{1.5}$$

Naturalmente, se l'operatore unitario U non prevede interazione tra il sistema e l'ambiente, si può scrivere $U = W \otimes W_{env}$ con W e W_{env} entrambi unitari e quindi

$$\mathcal{E}(\rho) = W\rho W^{\dagger} \tag{1.6}$$

cioè il sistema è in realtà un sistema chiuso. Nel caso generale invece, posto $\rho_{env} = \sum_i |\psi_i\rangle\langle\psi_i|$ (i vettori $\{|\psi_i\rangle\}$ non sono normalizzati), è possibile scrivere

$$\mathcal{E}(\rho) = \sum_{ik} E_{ik}\rho E_{ik}^{\dagger} \tag{1.7}$$

dove $E_{ik} = \langle e_k|U|\psi_i\rangle$, essendo $\{|e_k\rangle\}$ una base per lo spazio di environment. Il modo di scrivere una QO usato in eq.(1.7), detto *operator-sum representation* o anche *Kraus representation* [2], coinvolge operatori $\{E_{ik}\}$ che non godono di particolari proprietà: sono semplicemente elementi parziali di matrice dell'operatore di interazione unitaria U.

Una QO definita a partire da un'interazione unitaria tra il sistema principale e l'ambiente sarà sicuramente trace-preserving [2] , ma in generale

[2]In quanto originata, appunto, da un'interazione unitaria ed è noto come la traccia

non riconducibile a una semplice trasformazione unitaria sul solo sistema principale.

Per semplicità abbiamo assunto che lo stato sistema-ambiente sia fattorizzato. Questa però non è un'assunzione così limitativa come può sembrare: infatti, nonostante l'interazione sistema-ambiente esista e continui a creare correlazioni (o entanglements), il fatto di *preparare* il sistema prima di una misura annulla tutte queste correlazioni e per tempi sufficientemente brevi è realmente possibile considerare lo stato totale come fattorizzato.

1.2 Caratterizzazioni matematiche per le QO's

1.2.1 Operatori

Cominciamo con un teorema fondamentale [3]:

Teorema 1 *Una mappa $\mathcal{E}$ da stati $\rho \in \mathsf{T}(\mathsf{H})$ in stati $\mathcal{E}(\rho) \in \mathsf{T}(\mathsf{K})$ è una quantum oparation se e solo se l'operatore*

$$R_{\mathcal{E}} = \mathcal{E} \otimes \mathcal{I}(|I\rangle\rangle\langle\langle I|) \tag{1.8}$$

è un operatore positivo su $\mathsf{K} \otimes \mathsf{H}$,
dove $\mathcal{I}$ è la mappa identica da stati $\rho \in \mathsf{T}(\mathsf{H})$ in stati $\mathcal{I}(\rho) \in \mathsf{T}(\mathsf{H})$, e $|I\rangle\rangle = \sum_r |r\rangle|r\rangle$ è lo stato maximally entangled *in $\mathsf{H} \otimes \mathsf{H}$.*

In aggiunta si ha che

$$0 \leq \mathrm{Tr}_1 [R_{\mathcal{E}}] \leq I_{\mathsf{H}} \tag{1.9}$$

con $\mathrm{Tr}_1 [R_{\mathcal{E}}] = I_{\mathsf{H}}$ se e solo se la mappa $\mathcal{E}$ è trace-preserving.

sia invariante sotto trasformazioni unitarie. Mappe trace-decreasing possono essere anch'esse associate, come vedremo, a interazioni unitarie seguite, però, da una compressione (isometria) a uno spazio di Hilbert di dimensione minore rispetto a quello di partenza.

La mappa $\mathcal{E}$ può essere ricostruita da $R_{\mathcal{E}}$ come

$$\mathcal{E}(\rho) = \mathrm{Tr}_2\left[(I_{\mathsf{K}} \otimes \rho^T) R_{\mathcal{E}}\right]. \tag{1.10}$$

Dim. Per prima cosa verifichiamo l'eq.(1.10):

$$\mathrm{Tr}_2\left[(I_{\mathsf{K}} \otimes \rho^T) R_{\mathcal{E}}\right] = \mathrm{Tr}_2\left[(I_{\mathsf{K}} \otimes \rho^T)\ \mathcal{E} \otimes \mathcal{I}(|I\rangle\!\rangle\langle\!\langle I|)\right]; \tag{1.11}$$

espandendo lo stato $|I\rangle\!\rangle\langle\!\langle I|$ si ha:

$$\mathrm{Tr}_2\left[(I_{\mathsf{K}} \otimes \rho^T) R_{\mathcal{E}}\right] = \mathrm{Tr}_2\left[\sum_{rs} (I_{\mathsf{K}} \otimes \rho^T)\ \mathcal{E}(|r\rangle\langle s|) \otimes |r\rangle\langle s|\right]; \tag{1.12}$$

scrivendo $\rho^T = \sum_{ij} \rho^T_{ij} |i\rangle\langle j|$:

$$\mathrm{Tr}_2\left[(I_{\mathsf{K}} \otimes \rho^T) R_{\mathcal{E}}\right] = \mathrm{Tr}_2\left[\sum_{rs} \left(\mathcal{E}(|r\rangle\langle s|) \otimes \sum_{ij} \rho^T_{ij} |i\rangle\langle j|r\rangle\langle s|\right)\right]; \tag{1.13}$$

eseguendo la traccia parziale e riarrangiando i termini si ottiene

$$\mathrm{Tr}_2\left[(I_{\mathsf{K}} \otimes \rho^T) R_{\mathcal{E}}\right] = \sum_{rs} \mathcal{E}(|r\rangle\langle s|)\rho^T_{sr} = \mathcal{E}(\rho). \tag{1.14}$$

Supponiamo ora di avere una QO $\mathcal{E}$. Poiché la mappa $\mathcal{E}$ è CP per ipotesi, ed essendo l'operatore $|I\rangle\!\rangle\langle\!\langle I|$ chiaramente positivo sullo spazio di Hilbert esteso, si ha automaticamente che $R_{\mathcal{E}} \geq 0$. Inoltre, da eq.(1.10) e dall'assioma(1) per le QO's, si ha:

$$0 \leq \mathrm{Tr}\left[\mathcal{E}(\rho)\right] = \mathrm{Tr}\left[\rho^T\, \mathrm{Tr}_1\left[R_{\mathcal{E}}\right]\right] \leq 1 \tag{1.15}$$

da cui la condizione $0 \leq \mathrm{Tr}_1\left[R_{\mathcal{E}}\right] \leq I_{\mathsf{H}}$. A mappe trace-preserving corrispondono operatori per cui $\mathrm{Tr}_1\left[R_{\mathcal{E}}\right] = I_{\mathsf{H}}$.

Per verificare l'implicazione opposta, supponiamo di avere un operatore $R_{\mathcal{E}} \in \mathsf{L}(\mathsf{K} \otimes \mathsf{H})$ positivo e quindi diagonalizzabile. Sia

$$R_{\mathcal{E}} = \sum_i |E_i\rangle\!\rangle\langle\!\langle E_i| \tag{1.16}$$

la sua risoluzione spettrale dove $\|E_i\|_2^2 \doteq \mathrm{Tr}[E_i^\dagger E_i]$ sono gli autovalori. Da eq.(1.10), ricordando che si può sempre scrivere $|E_i\rangle\rangle\langle\langle E_i| = E_i \otimes I_{\mathsf{H}} |I\rangle\rangle\langle\langle I| E_i^\dagger \otimes I_{\mathsf{H}}$ con $E_i \in \mathsf{L}(\mathsf{H},\mathsf{K})$ [3], si ottiene la forma per la QO detta *di Kraus*:

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger. \tag{1.17}$$

Da quest'ultima equazione è evidente la linearità della mappa e quindi la validità dell'assioma(2). L'assioma(1) si ottiene trasferendo la proprietà $0 \leq \mathrm{Tr}_1[R_{\mathcal{E}}] \leq I_{\mathsf{H}}$ sugli operatori di Kraus per cui $\sum_i E_i^\dagger E_i \leq I_{\mathsf{H}}$. Per quanto riguarda la completa positività della mappa, si può notare che per ogni estensione J dello spazio di Hilbert, per ogni $|\Psi\rangle\rangle \in \mathsf{H} \otimes \mathsf{J}$ e per ogni operatore positivo $P \in \mathsf{L}(\mathsf{H} \otimes \mathsf{J})$ si ha

$$\sum_i \langle\langle\Psi|(E_i \otimes I_{\mathsf{J}})\ P\ (E_i^\dagger \otimes I_{\mathsf{J}})|\Psi\rangle\rangle = \sum_i \left(\langle\langle\Psi|E_i \otimes I_{\mathsf{J}}\right) P \left(\langle\langle\Psi|E_i \otimes I_{\mathsf{J}}\right)^\dagger \geq 0. \tag{1.18}$$

È così dimostrata anche la completa positività della mappa che quindi è a tutti gli effetti una QO. ■

Da questo teorema e dalla sua dimostrazione discendono naturalmente alcuni corollari:

Corollario 1 *La corrispondenza $\mathcal{E} \longleftrightarrow R_{\mathcal{E}}$ è biunivoca.*

Dim. L'enunciato è equivalente a dire che $R_{\mathcal{E}} = R_{\mathcal{F}}$ se e solo se $\mathcal{E} = \mathcal{F}$.

[Se] È evidente dalla costruzione definita in eq.(1.8).

[Solo se] Basta dimostrare l'iniettività dell'applicazione $R \longmapsto \mathcal{E}_R$. Supponiamo che esista un operatore positivo R per cui valga

$$\mathrm{Tr}_2\left[(I_{\mathsf{K}} \otimes \rho^T)\ R\right] = 0_{\mathsf{K}} \tag{1.19}$$

[3] Visto che hanno norma finita, si può specificare meglio dicendo che $E_i \in \mathsf{B}(\mathsf{H},\mathsf{K})$.

per ogni $\rho \in \mathsf{L}(\mathsf{H})$ positivo. Ciò significa che deve essere

$$\mathrm{Tr}_2 \left[(I_\mathsf{K} \otimes |v\rangle\langle v|) \; R \right] = 0_\mathsf{K} \tag{1.20}$$

per ogni $|v\rangle \in \mathsf{H}$. Scritto $R = \sum_i a_i \otimes b_i$, dove $\{a_i\} \subset \mathsf{L}(\mathsf{K})$ è una base per $\mathsf{L}(\mathsf{K})$ e $\{b_i\} \subset \mathsf{L}(\mathsf{H})$, eq.(1.20) implica che $b_i = 0$ per ogni i e quindi che $R = 0$. ■

Corollario 2 *Una mappa $\mathcal{E}$ da stati $\rho \in \mathsf{T}(\mathsf{H})$ in stati $\mathcal{E}(\rho) \in \mathsf{T}(\mathsf{K})$ è* completamente positiva *se e solo se è* positiva *la sua estensione $\mathcal{E} \otimes \mathcal{I}$ a uno spazio di Hilbert isomorfo a quello originale.*

Quest'ultimo corollario è molto utile in quanto limita i controlli da effettuare sulle infinite estensioni possibili di una mappa per verificarne la completa positività. A questo riguardo esiste un altro risultato:

Teorema 2 *Una mappa lineare $\mathcal{E} : \mathsf{L}(\mathsf{H}) \longrightarrow \mathsf{L}(\mathsf{K})$ è CP se e solo se per tutte le sequenze di vettori $\{|h_i\rangle\} \in \mathsf{H}$ e $\{|k_i\rangle\} \in \mathsf{K}$, con $i = 1, ..., n$ per ogni n, si ha*

$$\sum_{ij=1}^{n} \langle k_i| \; \mathcal{E}(|h_i\rangle\langle h_j|) \; |k_j\rangle \geq 0. \tag{1.21}$$

Dim. Abbiamo già visto che $\mathcal{E}$ è CP se e solo se $R_\mathcal{E}$ è positivo, cioè se e solo se

$$\langle\langle \Psi | R_\mathcal{E} | \Psi \rangle\rangle \geq 0 \tag{1.22}$$

per ogni $|\Psi\rangle\rangle \in \mathsf{K} \otimes \mathsf{H}$.

Scrivendo $|\Psi\rangle\rangle = \sum_{i=1}^{n} |e_i\rangle|f_i\rangle$, dove n può essere un numero naturale qualunque non dipendente in alcun modo dalla dimensione di K o di H, ma variabile unicamente con $|\Psi\rangle\rangle$, si ha:

$$\langle\langle \Psi | R_\mathcal{E} | \Psi \rangle\rangle = \sum_{rs} \sum_{ij=1}^{n} \langle e_i| \; \mathcal{E}(|r\rangle\langle s|) \; |e_j\rangle \; \langle f_i|r\rangle \; \langle s|f_j\rangle \geq 0. \tag{1.23}$$

Ponendo $|k_i\rangle = |e_i\rangle$ e $|h_i\rangle = \sum_r \langle f_i|r\rangle|r\rangle$ si ottiene il risultato. ■

1.2.2 Decomposizioni di Kraus

Dal Teorema(1) discende il seguente [2]:

Corollario 3 (decomposizione di Kraus) *Una mappa $\mathcal{E}$ da stati $\rho \in \mathsf{T}(\mathsf{H})$ in stati $\mathcal{E}(\rho) \in \mathsf{T}(\mathsf{K})$ è una QO se e solo se ammette una decomposizione nella forma detta* di Kraus

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{1.24}$$

con $E_i \in \mathsf{B}(\mathsf{H},\mathsf{K})$ e $\sum_i E_i^\dagger E_i \leq I_{\mathsf{H}}$.

Come non è biunivoca la corrispondenza ensemble-stati, così non è biunivoca la corrispondenza QO's-decomposizioni di Kraus. Più precisamente:

Teorema 3 *Due decomposizioni di Kraus $\{E_1, ..., E_m\}$ e $\{F_1, ..., F_n\}$ con $m \leq n$ sono equivalenti (cioè descrivono la stessa CP-map) se e solo se esiste un'isometria $T \in \mathsf{M}_{n,m}$ tale per cui*

$$F_i = \sum_j T_{ij} E_j \tag{1.25}$$

Dim. [Se] Questa direzione è banale:

$$\sum_{i=1}^{n} F_i \cdot F_i^\dagger = \sum_{i=1}^{n} \sum_{j,k=1}^{m} T_{ij} T_{ik}^* E_j \cdot E_k = \sum_{j=1}^{m} E_j \cdot E_j^\dagger \tag{1.26}$$

dove si è fatto uso della proprietà dell'isometria T per cui $T^\dagger T = I_m$.

[Solo se] Data la CP-map $\mathcal{E}$, sia $R_{\mathcal{E}}$ l'operatore positivo a essa associato. Per ipotesi deve essere

$$R_{\mathcal{E}} = \sum_{i=1}^{m} |E_i\rangle\rangle\langle\langle E_i| = \sum_{j=1}^{n} |F_j\rangle\rangle\langle\langle F_j| \tag{1.27}$$

e supponiamo, senza perdere in generalità, che $\{|E_i\rangle\rangle\}$ sia un insieme di elementi linearmente indipendenti. Deve quindi essere $\mathsf{Supp}(R_{\mathcal{E}}) = \mathsf{Span}\{|E_i\rangle\rangle\} = \mathsf{Span}\{|F_j\rangle\rangle\}$ ed esistono coefficienti $\{t_{ij}\}$ per cui

$$|F_k\rangle\rangle = \sum_l t_{kl}|E_l\rangle\rangle. \tag{1.28}$$

Poiché l'indipendenza lineare degli $\{|E_i\rangle\rangle\}$ implica automaticamente l'indipendenza lineare degli operatori $\{|E_i\rangle\rangle\langle\langle E_j|\}$ (in effetti questi ultimi sono una base per $\mathsf{L}(\mathsf{Supp}(R_{\mathcal{E}}))$), imponendo eq.(1.27) si ottiene la condizione [4] $\sum_k t^*_{ki}t_{kj} = \delta_{ij}$.■

Tra tutte le possibili (infinite) decomposizioni di Kraus associate a una data CP-map, ne esistono alcune particolari:

Definizione 2 *Data una CP-map $\mathcal{E} = \sum_i K_i \cdot K_i^\dagger$, sono dette decomposizioni di Kraus* minimali *quelle per cui gli operatori $\{K_i\}$ formano un insieme linearmente indipendente.*

Tra le decomposizioni minimali vi sono anche quelle dette canoniche *per le quali vale anche*

$$\mathrm{Tr}[K_i^\dagger K_j] = \|K_i\|_2^2\ \delta_{ij}. \tag{1.29}$$

La definizione è ben posta, nel senso che, data una CP-map, è sempre possibile costruire una decomposizione di Kraus che sia canonica. Infatti basta diagonalizzare l'operatore $R_{\mathcal{E}}$ in modo tale che i suoi autovettori siano tutti ortogonali tra di loro (e questa opportunità ci è assicurata dal teorema spettrale per operatori positivi).

[4] In effetti, l'indipendenza lineare degli operatori $\{|E_i\rangle\rangle\langle\langle E_j|\}$ è necessaria per affermare che la matrice $T = (t_{ij})$ ha rango massimo. Se così non fosse, T non potrebbe in alcun modo essere isometrica.

Da una decomposizione di Kraus canonica [5] si possono poi ottenere *tutte* le altre decomposizioni minimali applicando il Teorema(3) nel caso di una matrice T unitaria.

Si dimostra che

Proposizione 1 *Una decomposizione di Kraus è minimale se e solo se la sua cardinalità è pari a* $\text{rank}(R_{\mathcal{E}})$.

Dim. [Se] Supponiamo di avere una decomposizione di Kraus $R_{\mathcal{E}} = \sum_{i=1}^{r} |E_i\rangle\rangle\langle\langle E_i|$ con cardinalità $r = \text{rank}(R_{\mathcal{E}})$. Ciò significa che, poiché deve essere sempre $\mathsf{Span}\{|E_i\rangle\rangle\} = \mathsf{Supp}(R_{\mathcal{E}})$, l'insieme $\{|E_i\rangle\rangle\}$ è una base per $\mathsf{Supp}(R_{\mathcal{E}})$. Da questo discende l'indipendenza lineare della decomposizione che quindi è minimale.

[Solo se] Sia $R_{\mathcal{E}} = \sum_{i=1}^{k} |K_i\rangle\rangle\langle\langle K_i|$ una decomposizione minimale. Poiché deve essere $\mathsf{Span}\{|K_i\rangle\rangle\} = \mathsf{Supp}(R_{\mathcal{E}})$ e deve valere l'indipendenza lineare dei $\{K_i\}$, si ha che l'insieme $\{K_i\}$ forma una base per $\mathsf{Supp}(R_{\mathcal{E}})$, i.e. $k = \text{rank}(R_{\mathcal{E}})$.■

1.2.3 Contrazioni

Nella medesima ottica di quello che si era fatto nella sezione 1.1.2 "QO's e interazione con un environment" e cioè estendere lo spazio di Hilbert del sistema principale e studiarne l'evoluzione come interazione unitaria con uno spazio di *ancilla*, esiste un teorema di realizzazione di CP-map's in termini di contrazioni su spazi di Hilbert allargati:

[5] La decomposizione di Kraus canonica è unica nel caso in cui l'operatore $R_{\mathcal{E}}$ non abbia autovalori degeneri; se autovalori degeneri sono presenti, vi sono infinite decomposizioni canoniche, corrispondenti alla libertà unitaria che esiste nel definire la base ortonormale degli autospazi degeneri di $R_{\mathcal{E}}$.

Teorema 4 *Per ogni quantum operation* $\mathcal{E} : \mathsf{T}(\mathsf{H}) \longrightarrow \mathsf{T}(\mathsf{H})$ [6] *esiste sempre un'estensione* J *dello spazio di Hilbert e una preparazione di* J *in uno stato puro* $|\phi\rangle \in \mathsf{J}$ *tali per cui la QO può essere ottenuta da una contrazione pura* $M \in \mathsf{B}(\mathsf{H} \otimes \mathsf{J})$.

Nel caso che $\mathcal{E}$ *sia trace-preserving, si può scegliere* M *unitaria.*

Dim. Sia $\mathcal{E} = \sum_i E_i \cdot E_i^\dagger$ una decomposizione di Kraus per la QO. Scelto e fissato lo stato $|\phi\rangle \in \mathsf{J}$, definiamo l'operatore M in questo modo:

$$M = \sum_i E_i \otimes |i\rangle\langle\phi| \tag{1.30}$$

dove $\{|i\rangle\}$ è un insieme di vettori ortonormali in J.

Notando che, per ogni $|\psi\rangle \in \mathsf{H}$, si ha

$$(\langle\psi| \otimes \langle\phi|)\ M^\dagger M\ (|\psi\rangle \otimes |\phi\rangle) = \langle\psi| \sum_i E_i^\dagger E_i |\psi\rangle, \tag{1.31}$$

è chiaro che

- per $\sum_i E_i^\dagger E_i < I_{\mathsf{H}}$, l'operatore M è una contrazione, in quanto $\|M\| < 1$;
- per $\sum_i E_i^\dagger E_i = I_{\mathsf{H}}$, l'operatore M è un'isometria su $\mathsf{H}_{|\phi\rangle} = \mathsf{Span}\{|\psi\rangle \otimes |\phi\rangle : |\psi\rangle \in \mathsf{H}\} \cong \mathsf{H} \subseteq \mathsf{H} \otimes \mathsf{J}$ la quale a sua volta può essere estesa con Gram-Schmidt a un operatore unitario su tutto $\mathsf{H} \otimes \mathsf{J}$.

Resta da vedere come ottenere la QO dalla contrazione M. Sia $\rho = \sum_i |\psi_i\rangle\langle\psi_i|$ lo stato di input del sistema principale. Poiché

$$M(\rho \otimes |\phi\rangle\langle\phi|)M^\dagger = \sum_{ijk} (E_j|\psi_i\rangle \otimes |j\rangle)\ (\langle\psi_i|E_k^\dagger \otimes \langle k|), \tag{1.32}$$

[6] Qui per semplicità si è scelta una mappa con spazi di partenza e di arrivo uguali. In seguito si farà l'analogo per il caso generale di spazi di partenza e di arrivo diversi; saranno necessari però metodi più potenti per la purificazione della mappa. Per la generalizzazione si veda il Teorema(9).

si ha

$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathsf{J}}[M(\rho \otimes |\phi\rangle\langle\phi|)M^{\dagger}].\blacksquare \tag{1.33}$$

La dimostrazione appena conclusa sottolinea il fatto che, in generale, un operatore unitario appaia localmente solo come CP-map trace-preserving [7].

1.2.4 Proiezioni

Anche questo risultato può essere visto come un corollario del Teorema(1). Estendendo ulteriormente lo spazio di Hilbert si ottiene una semplificazione drastica del concetto di QO [4]:

Corollario 4 *Qualunque CP-map* $\mathcal{E} : \mathsf{T}(\mathsf{H}_2) \longrightarrow \mathsf{T}(\mathsf{H}_1)$ *può essere ottenuta da una* fissata *proiezione nel modo seguente:*

$$\mathcal{E}(\rho) = \mathrm{Tr}_{2,3}\left[(I \otimes |I\rangle\!\rangle\langle\!\langle I|)\ (R_{\mathcal{E}} \otimes \rho)\right], \tag{1.34}$$

dove si è introdotto lo spazio $\mathsf{H}_3 \cong \mathsf{H}_2$.

Dim. Infatti si può scrivere

$$\mathcal{E}(\rho) = \mathrm{Tr}_{2,3}\left[(I \otimes I \otimes \rho)\ (I \otimes |I\rangle\!\rangle\langle\!\langle I|)\ (R_{\mathcal{E}} \otimes I)\right] \tag{1.35}$$

avendo fatto uso anche della proprietà di invarianza sotto permutazione ciclica di operatori negli spazi H_2 e H_3. Tracciando prima sul terzo spazio si ha:

$$\mathcal{E}(\rho) = \mathrm{Tr}_2\left[I \otimes \mathrm{Tr}_3\left[\ (I \otimes \rho)|I\rangle\!\rangle\langle\!\langle I|\ \right]\ R_{\mathcal{E}}\right] = \mathrm{Tr}_2\left[\left(I \otimes \rho^T\right) R_{\mathcal{E}}\right] \tag{1.36}$$

risultato che coincide con eq.(1.10). ■

[7] Vedi anche, per l'appunto, sezione 1.1.2.

1.3 Interpretazione fisica

1.3.1 QO's e canali rumorosi

Da [1]: sia $\rho \in \mathsf{T}(\mathsf{H})$ lo stato in cui si trova il sistema e sia $|e_0\rangle\langle e_0|$ lo stato dell'ancilla. Applichiamo un'interazione unitaria sistema-ancilla per poi effettuare una misura proiettiva sull'ancilla. Alla fine, lo stato del sistema sarà:

$$\rho_k = \frac{\mathrm{Tr}_2[\ (I_{\mathsf{H}} \otimes |e_k\rangle\langle e_k|)\ U\ (\rho \otimes |e_0\rangle\langle e_0|)\ U^\dagger\ ]}{\mathrm{Tr}[\ (I_{\mathsf{H}} \otimes |e_k\rangle\langle e_k|)\ U\ (\rho \otimes |e_0\rangle\langle e_0|)\ U^\dagger\ ]} = \frac{E_k \rho E_k^\dagger}{\mathrm{Tr}[E_k \rho E_k^\dagger]} \tag{1.37}$$

dove il fattore $\frac{1}{\mathrm{Tr}[E_k \rho E_k^\dagger]}$ compare come normalizzazione dello stato. La probabilità di misurare l'evento k è data da

$$p_k = \mathrm{Tr}[\ (I_{\mathsf{H}} \otimes |e_k\rangle\langle e_k|)\ U\ (\rho \otimes |e_0\rangle\langle e_0|)\ U^\dagger\ ] = \mathrm{Tr}[E_k \rho E_k^\dagger]. \tag{1.38}$$

Unendo le equazioni (1.37) e (1.38) si ottiene:

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger = \sum_k p_k \rho_k. \tag{1.39}$$

Dall'ultima uguaglianza si può evincere che l'azione di una QO è equivalente a trasformare casualmente lo stato ρ di partenza in stati finali $\{\rho_k\}$ secondo una distribuzione di probabilità data dai $\{p_k\}$. In questo senso, una QO è molto vicina all'idea di canale rumoroso classico presente in teoria classica dell'informazione.

1.3.2 QO's e misure

Le QO's sono utili anche per modellizzare un qualsiasi processo di misura. Questo in genere consiste in un'evoluzione stocastica del sistema da uno stato di input ρ a uno stato di output ρ_k con probabilità p_k dipendente dall'*outcome* k.

Per generalizzare i postulati di misura dati per gli stati puri in termini di contrazioni (eventualmente di proiezioni) pure [8], si introduce il concetto di *strumento*:

Definizione 3 *Sia* Ω *uno spazio di probabilità che sia chiuso sotto unioni, intersezioni e complementi e sul quale sia definita una misura positiva (la probabilità)* $p(\Delta)$ *per ogni* $\Delta \subseteq \Omega$ *tale che* $p(\Omega) = 1$. *Allora si dice* strumento *una mappa* $\mathrm{S} : \Omega \longrightarrow \mathsf{CP}(\mathsf{T}(\mathsf{H}))$ [9]*, con* $\mathrm{S}(\Delta) = \mathcal{S}_\Delta$*, tale per cui:*

1. $\mathcal{S}_\Delta(\rho) \geq 0$ *per ogni* $\rho \geq 0$ *e per ogni* $\Delta \subseteq \Omega$*;*
2. $\mathrm{Tr}[\mathcal{S}_\Delta(\rho)] \leq 1$ *con l'uguale se e solo se* $\Delta \equiv \Omega$*;*
3. $\mathcal{S}_{\bigcup_n \Delta_n}(\rho) = \sum_n \mathcal{S}_{\Delta_n}(\rho)$ *dove* $\{\Delta_n\}$ *è un insieme numerabile di sottoinsiemi disgiunti di* Ω*;*
4. $\mathcal{S}_\emptyset = 0$.

Si dimostra che è possibile associare una CP-map trace preserving $\mathcal{E}_\mathrm{S}$ a ogni strumento S, in modo tale da rispecchiare la struttura dello spazio Ω (su cui S è definito) nella struttura della CP-map. Consideriamo infatti uno spazio delle probabilità che abbia struttura *discreta* [10] del tipo

$$\Omega = \bigcup_{n=1}^{N} \Delta_n \tag{1.40}$$

dove $N < \infty$ e i sottoinsiemi $\{\Delta_n\}$ sono tutti disgiunti. Per ogni $n \in \{1, ..., N\}$ si costruisce la CP-map $\mathcal{E}_n = \sum_{i_n} E_{i_n}^{(n)} \cdot E_{i_n}^{(n)\dagger}$ [11] in modo tale che

$$\mathcal{E}_n(\rho) = \mathcal{S}_{\Delta_n}(\rho) \tag{1.41}$$

[8] Vedi a questo proposito il Corollario(5), più avanti.

[9] Del fatto che la completa positività sia una proprietà più forte della semplice positività si è già parlato.

[10] È questo il caso di misura di un'osservabile con spettro discreto.

[11] Per il punto(2) della definizione, se $N \geq 2$, le singole $\mathcal{E}_n$ *devono* essere trace-decreasing.

e

$$\sum_{n=1}^{N} \mathcal{E}_n = \sum_{n=1}^{N} \sum_{i_n} E_{i_n}^{(n)} \cdot E_{i_n}^{(n)\dagger} = \mathcal{S}_\Omega \tag{1.42}$$

sia trace-preserving.

Il discorso è estendibile anche al caso di struttura *continua* [12] per lo spazio Ω. Anche lo strumento avrà struttura continua e, definendo

$$\mathrm{d}\,\mathrm{S}(x) \doteq \mathrm{S}([x, x + \mathrm{d}\,x]) \tag{1.43}$$

dove $x \in \Omega$, si avrà anche un insieme non numerabile di QO's $\{\mathcal{E}_x\,\mathrm{d}\,x\}_{x\in\Omega}$ tali che

$$\int_\Omega \mathrm{d}\,x\ \mathcal{E}_x \tag{1.44}$$

sia una CP-map trace-preserving.

Espandendo in forma di Kraus le CP-map infinitesime $\mathcal{E}_x\,\mathrm{d}\,x$, si definiscono due categorie disgiunte di misura:

Definizione 4 *Sia*

$$\mathrm{d}\,\mathrm{S}(x) = \mathcal{E}_x\,\mathrm{d}\,x = \sum_{l_x} E_{l_x}^{(x)} \cdot E_{l_x}^{(x)\dagger}\,\mathrm{d}\,x \tag{1.45}$$

una decomposizione di Kraus per la CP-map infinitesima $\mathcal{E}_x\,\mathrm{d}\,x$*. Se per ogni* $x \in \Omega$ *e per ogni* l_x *si ha che* $\mathrm{rank}(E_{l_x}^{(x)}) = 1$ *la misura è detta* di Gordon-Louiselle-Yuen *(o* GLY-measurement*); altrimenti si parla più in generale di misura* di von Neumann-Davies *(o* VND-measurement*).*

Approfondendo questo aspetto delle QO's, esiste un risultato dovuto a Ozawa [5]:

Teorema 5 *Tutti i processi quantistici di misurazione* pura *possono essere decomposti in componenti GLY e VND.*

[12] È questo il caso di misura di un'osservabile con spettro continuo.

Dim. Come fatto precedentemente, diciamo che per ogni $x \in \Omega$ si ha una decomposizione di Kraus differente

$$\mathcal{S}_x(\rho)\,\mathrm{d}\,x = \sum_{l_x} E_{l_x}^{(x)} \rho E_{l_x}^{(x)\dagger}\,\mathrm{d}\,x. \tag{1.46}$$

Ma lo strumento è puro; quindi, per stati di input puri, del tipo $\rho = |\phi\rangle\langle\phi|$, la somma $\sum_{l_x} E_{l_x}^{(x)} \rho E_{l_x}^{(x)\dagger}$ deve essere anch'essa pura. Questo implica che i vettori $\{E_{l_x}^{(x)}|\phi\rangle\}$, per fissato x, siano tutti linearmente dipendenti al variare di l_x. Ma allora solo un unico operatore $E^{(x)}$ è necessario per descrivere la CP-map infinitesima:

$$\mathcal{S}_x(\rho)\,\mathrm{d}\,x = E^{(x)} \rho E^{(x)\dagger}\,\mathrm{d}\,x. \tag{1.47}$$

Ora, decomponendo lo spazio Ω come $\Omega = \Lambda \bigcup \Delta$, in modo tale che per $x \in \Lambda$ sia $\mathrm{rank}(E^{(x)}) = 1$ mentre per $x \in \Delta$ sia $\mathrm{rank}(E^{(x)}) > 1$, si ha la decomposizione cercata. ■

Nella dimostrazione del precedente teorema si è implicitamente chiarito anche un aspetto che avevamo lasciato scoperto introducendo il concetto di strumento:

Corollario 5 *Una misurazione è* pura *(cioè manda stati puri in stati puri) se e solo se può essere scritta nella forma*

$$\mathcal{S}_x(\rho)\,\mathrm{d}\,x = E^{(x)} \rho E^{(x)\dagger}\,\mathrm{d}\,x; \tag{1.48}$$

se e solo se, cioè, è associata a un'espansione di contrazioni pure con

$$\int \mathrm{d}\,x E^{(x)\dagger} E^{(x)} = I. \tag{1.49}$$

1.4 Esempi di *quantum operations*

1.4.1 Traccia e traccia parziale

Consideriamo la mappa che ha, come decomposizione di Kraus, la seguente:

$$\mathcal{E}(\rho) = \sum_i |0\rangle\langle i|\rho|i\rangle\langle 0|; \tag{1.50}$$

chiaramente questa è una QO trace-preserving (infatti $\sum_i E_i^\dagger E_i = \sum_i |i\rangle\langle i| = I$) che mappa stati $\rho \in \mathsf{T}(\mathsf{H})$ in $\mathcal{E}(\rho) = \mathrm{Tr}[\rho]|0\rangle\langle 0|$. A meno quindi del fattore fisso $|0\rangle\langle 0|$, questa è proprio la mappa corrispondente alla traccia.

Per quanto riguarda la traccia parziale, procedendo per analogia, definiamo gli operatori di Kraus come $E_i = |0\rangle\langle i| \otimes I_{\mathsf{K}}$ e costruiamo la mappa $\mathsf{T}(\mathsf{H} \otimes K) \longrightarrow \mathsf{T}(\mathsf{H} \otimes K)$ come

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger = |0\rangle\langle 0| \otimes \mathrm{Tr}_{\mathsf{H}}[\rho]; \tag{1.51}$$

anche questa è trace-preserving e corrisponde alla traccia parziale.

1.4.2 Canale *depolarizing*

L'azione di questa mappa [13] consiste nel sostituire, con probabilità p, a uno stato di input $\rho \in \mathsf{T}(\mathbb{C}^2)$, lo stato completamente caotico $\frac{I}{2}$; l'altra possibilità è lasciare lo stato immutato. Lo stato del sistema all'uscita sarà quindi

$$\mathcal{E}(\rho) = p\,\frac{I}{2} + (1-p)\rho. \tag{1.52}$$

[13] Questo esempio e quello successivo saranno specifici per il caso di un qubit (stato quantistico in uno spazio di Hilbert bidimensionale); la generalizzazione al caso di dimensione finita è possibile, come anche al caso di dimensione numerabile (come per l'oscillatore armonico).

Questa scrittura non evidenzia una decomposizione di Kraus; tuttavia notando che

$$I = \frac{1}{2}(\rho + X\rho X + Y\rho Y + Z\rho Z) \tag{1.53}$$

dove X, Y, Z sono le tre matrici di Pauli, si può riscrivere la mappa depolarizzante come

$$\mathcal{E}(\rho) = \left(1 - \frac{3}{4}p\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z). \tag{1.54}$$

1.4.3 Canale di *phase damping*

Questa mappa è tipicamente quantistica: lo stato di input viene sottoposto a una rotazione di fase (*phase-kick*) ϕ casuale in accordo con una distribuzione di probabilità $\mathrm{d}\,\mu(\phi)$; si ha [14]

$$\mathcal{E}(\rho) = \int \mathrm{d}\,\mu(\phi)\ e^{-\frac{i}{2}\phi Z}\rho e^{\frac{i}{2}\phi Z} \tag{1.55}$$

dove $Z = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$.

Il canale di phase damping causa un decadimento esponenziale dei termini fuori diagonale della matrice densità: lo stato di input è reso completamente decoerente. Per vedere come funziona la mappa, supponiamo che la distribuzione di probabilità usata sia in accordo con una gaussiana con valore medio 0 e varianza 2λ:

$$\mathcal{E}(\rho) = \int \mathrm{d}\,\phi\ e^{-\frac{i}{2}\phi Z}\rho e^{\frac{i}{2}\phi Z} e^{-\frac{1}{4\lambda}\phi^2}; \tag{1.56}$$

svolgendo i calcoli si ottiene

$$\mathcal{E}(\rho) = \begin{bmatrix} \rho_{11} & \rho_{12}e^{-\lambda} \\ \rho_{21}e^{-\lambda} & \rho_{22} \end{bmatrix}. \tag{1.57}$$

[14] Questo è un esempio di decomposizione di Kraus continua. Restano validi i principali risultati sulle decomposizioni di Kraus discrete.

In questo senso, si è riconosciuto per il canale di phase-damping un ruolo chiave nel passaggio da stato quantistico a stato classico.

Capitolo 2

Dilatazioni unitarie

Si era visto, nella sezione 1.1.2 "*Quantum operations* e interazione con un *environment*", che una qualunque CP-map trace-preserving può essere descritta da un'interazione unitaria tra il sistema principale e un'ancilla la quale, dopo che l'interazione è avvenuta, viene "tracciata via". Questo approccio è in realtà possibile anche nel caso di una mappa trace-decreasing: c'è bisogno però di uno spazio di ancilla con dimensione maggiore e di una *compressione* che riduca la dimensione dello spazio di arrivo.

Nel capitolo precedente si è sempre fatto uso della convenzione per cui ci si riferisce alla mappa $\mathcal{E} : \mathsf{T}(\mathsf{H}) \longrightarrow \mathsf{T}(\mathsf{K})$ quale mappa *diretta*, mentre la mappa *duale* $\mathcal{E}^\tau : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ è definita dalla relazione [1]

$$\mathrm{Tr}[X\mathcal{E}(\rho)] = \mathrm{Tr}[\mathcal{E}^\tau(X)\rho]. \tag{2.1}$$

Data quindi una quantum operation in forma di Kraus $\mathcal{E} = \sum_i E_i \cdot E_i^\dagger$ la sua duale è $\mathcal{E}^\tau = \sum_i E_i^\dagger \cdot E_i$. Le condizioni per cui una mappa è trace-preserving o trace-decreasing si riscrivono in termini della duale come $\mathcal{E}^\tau(I_\mathsf{K}) = K \leq$

[1] Le due tracce sono su spazi diversi.

I_{H}: la mappa $\mathcal{E}$ è trace-preserving se e solo se la sua duale è tale per cui $\mathcal{E}^{\tau}(I_{\mathsf{K}}) = I_{\mathsf{H}}$, i.e. è unit-preserving.

Nel seguito faremo invece uso della convenzione opposta per cui la mappa *diretta* è $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ mentre quella *duale* è $\mathrm{M}^{\tau} : \mathsf{T}(\mathsf{H}) \longrightarrow \mathsf{T}(\mathsf{K})$ [2]. La relazione che lega le due mappe è sempre quella per cui

$$\mathrm{Tr}[\mathrm{M}(X)\rho] = \mathrm{Tr}[X\mathrm{M}^{\tau}(\rho)]. \tag{2.2}$$

Per quanto riguarda la notazione, l'insieme delle quantum operations che mappano operatori $\mathsf{B}(\mathsf{K})$ in operatori $\mathsf{B}(\mathsf{H})$ con $\mathrm{M}(I_{\mathsf{K}}) = K \leq I_{\mathsf{H}}$ sarà indicato con $\mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$.

2.1 Dilatazioni ed estensioni

Prima di proseguire, è necessario chiarire le differenze tra i concetti di *dilatazione-compressione* e quelli di *estensione-restrizione*.

Da [6]: supponiamo che H sia un sottospazio di uno spazio di Hilbert K e che P sia il proiettore ortogonale da K su H. Qualunque operatore B su K induce in maniera naturale un operatore A su H definito da

$$A|v\rangle = PB|v\rangle \tag{2.3}$$

per ogni $|v\rangle \in \mathsf{H}$. In questo caso, l'operatore A è *la compressione* di B, mentre B è *una dilatazione* di A. È evidente come la compressione sia unica mentre le dilatazioni possibili siano infinite. La relazione tra A e B può anche essere espressa come

$$A = PBP. \tag{2.4}$$

[2] Dire quindi che M è *unit-preserving* è identico ad affermare che M^{τ} è *trace-preserving*. Completamente diverso è invece dire che M^{τ} è unit-preserving: questa proprietà caratterizza le quantum operations *bistocastiche*. Tuttavia, dove non c'è pericolo di confusione, si manterrà il termine *trace-preserving* anche in riferimento alla mappa diretta M.

Per avere, invece, una restrizione, è necessario che il sottospazio H sia invariante sotto l'azione di B: in questo caso, in eq.(2.3), non serve più il proiettore P. Allora A è *la restrizione* di B, mentre B è *un'estensione* di A.

L'operazione di estensione-restrizione è un caso particolare dell'operazione di dilatazione-compressione in cui l'operatore sullo spazio più grande lascia invariante lo spazio più piccolo.

2.2 Dilatazioni di Stinespring

Il processo di dilatazione di Stinespring ([7], [8]) dà la possibilità di purificare quantum operations con spazi di partenza e di arrivo generici tramite un procedimento per certi versi simile a quello adottato nella sezione 1.2.3 "Contrazioni".

Teorema 6 (dilatazioni di Stinespring) *Per ogni quantum operation* $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ *esiste sempre uno spazio di Hilbert* L *tale per cui la QO può essere ottenuta da una contrazione pura* $M \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{L})$.

Dim. Sia $\mathrm{M} = \sum_{i=1}^{n} M_i^\dagger \cdot M_i$ una qualunque decomposizione di Kraus per la mappa M. Sia L uno spazio di Hilbert con $\dim \mathsf{L} = n$ e sia $\{|e_i\rangle\} \subset \mathsf{L}$ una base ortonormale per L. L'operatore cercato è

$$M = \sum_{i=1}^{n} M_i \otimes |e_i\rangle \tag{2.5}$$

ed è una contrazione in quanto $M^\dagger M = K \leq I$.

La mappa diretta si ottiene con

$$\mathrm{M}(X) = M^\dagger (X \otimes I_{\mathsf{L}}) M; \tag{2.6}$$

la mappa duale con

$$\mathrm{M}^\tau(\rho) = \mathrm{Tr}_{\mathsf{L}}[M \rho M^\dagger]. \blacksquare \tag{2.7}$$

2.3 Dilatazioni di Stinespring unitarie

Per una mappa trace-preserving il Teorema(6) costruisce una contrazione M che in realtà è un'isometria in quanto $M^\dagger M = I$. È possibile estendere il risultato in modo tale da avere un'isometria anche nel caso di mappe trace-decreasing. Cominciamo dimostrando il seguente:

Lemma 1 *Dato un operatore positivo $P \in \mathsf{B}(\mathsf{H})$, per ogni K spazio di Hilbert, esiste un insieme di operatori $\{A_i\} \subset \mathsf{B}(\mathsf{H}, \mathsf{K})$ per cui*

$$P = \sum_{i=1}^{n} A_i^\dagger A_i \tag{2.8}$$

per un opportuno $n \in \mathbb{N}$.

Dim. Sia $\mathsf{K} \cong \mathsf{H}$. Allora il risultato vale con $n = 1$ e $A = P^{1/2}$.
Sia $\dim \mathsf{K} > \dim \mathsf{H}$. Allora il risultato vale con $n = 1$ e $A = TP^{1/2}$ dove $T \in \mathsf{B}(\mathsf{H}, \mathsf{K})$ è tale che $T^\dagger T = I_{\mathsf{H}}$, i.e. T è un'isometria.
Sia $\dim \mathsf{K} < \dim \mathsf{H}$. Diagonalizzando P si ottiene $P = \sum_{j=1}^{\mathrm{rank}(P)} |v_j\rangle\langle v_j|$. A questo punto vi sono due possibilità:

1. $\dim \mathsf{K} \geq \mathrm{rank}(P)$: allora il risultato vale con $n = 1$ e $A = (\langle v_1| \dot{+} \langle v_2| \dot{+} \ ... \ \dot{+} \langle v_{\mathrm{rank}(P)}|)$ eventualmente completato da zeri nel caso in cui $\dim \mathsf{K} > \mathrm{rank}(P)$;

2. $\dim \mathsf{K} < \mathrm{rank}(P)$: allora il risultato vale con $n = \mathrm{rank}(P)$ [3] e $A_i = (\langle v_i| \dot{+} 0_{\mathsf{H},\mathsf{K}'})$ dove K' è uno spazio di Hilbert con $\dim \mathsf{K}' = \dim \mathsf{K} - 1$.■

Teorema 7 (dilatazioni di Stinespring isometriche) *Una mappa* $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ *è una quantum operation se e solo se può essere scritta nella forma*

$$\mathrm{M}(X) = T^\dagger X \otimes \Sigma T \tag{2.10}$$

[3] In realtà, con una scelta appropriata degli $\{A_i\}$, basta $n = \min\{n \in \mathbb{N} : \ n \times \dim \mathsf{K} >$

dove $T \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{L})$ *è un'isometria e* $\Sigma \in \mathsf{B}(\mathsf{L})$ *è un proiettore non nullo.*

Dim. [Se] Siano $\{|\sigma_j\rangle\}_{j=1,...,\mathrm{rank}(\Sigma)} \subset \mathsf{L}$ gli autovettori di Σ corrispondenti all'autovalore $\{1\}$. Allora gli operatori $\{M_j\}_{j=1,...,\mathrm{rank}(\Sigma)}$ ottenuti come $M_j = (I_\mathsf{K} \otimes \langle\sigma_j|)T$ sono precisamente gli operatori di una decomposizione di Kraus della mappa M la quale, per il Corollario(3), è una quantum operation.

[Solo se] Sia M una quantum operation e siano $\{A_i\} \subset \mathsf{B}(\mathsf{H}, \mathsf{K})$ gli elementi di una sua decomposizione di Kraus qualsiasi. Per il Lemma(1) esiste un insieme di operatori $\{\tilde{A}_j\} \subset \mathsf{B}(\mathsf{H}, \mathsf{K})$ tali che $\sum_j \tilde{A}_j{}^\dagger \tilde{A}_j = I_\mathsf{H} - \sum_i A_i^\dagger A_i \geq 0$. Sia $\{|e_i\rangle, |\tilde{e_j}\rangle\} \subset \mathsf{L}$ un insieme di vettori ortonormali. Posto $\Sigma = \sum_i |e_i\rangle\langle e_i|$ e $T = \sum_i A_i \otimes |e_i\rangle + \sum_j \tilde{A}_j \otimes |\tilde{e_j}\rangle$ si ottiene il risultato [4]. Per mappe trace-preserving si ha $\tilde{A}_j = 0$ per ogni j.■

In maniera del tutto analoga all'estensione di Gram-Schmidt di un insieme di vettori ortonormali a una base ortonormale, un'isometria può essere

---

$\mathrm{rank}(P)\}$. Sia, infatti, $k = \dim \mathsf{K}$; costruiamo allora gli operatori

$$\begin{aligned}
A_1 &= (\langle v_1| \dot{+} \langle v_2| \dot{+} \ ... \ \dot{+} \langle v_k|) \\
A_2 &= (\langle v_{k+1}| \dot{+} \langle v_{k+2}| \dot{+} \ ... \ \dot{+} \langle v_{2k}|) \\
A_3 &= ... \\
&... \\
A_n &= (\langle v_{(n-1)k+1}| \dot{+} \langle v_{(n-1)k+2}| \dot{+} \ ... \ \dot{+} \langle v_{\mathrm{rank}(P)}| \dot{+} 0_{\mathsf{H},\mathsf{K}''})
\end{aligned} \tag{2.9}$$

dove K'' è uno spazio di Hilbert per cui $\dim \mathsf{K}'' = k - \mathrm{rank}(P) + (n-1)k = nk - \mathrm{rank}(P)$.

[4] $T \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{L})$ è un'isometria. Deve quindi essere $\dim \mathsf{H} \leq \dim \mathsf{K} \times \dim \mathsf{L}$. Consideriamo il caso più stringente per questa disuguaglianza, cioè quello in cui si è partiti dalla decomposizione di Kraus canonica (sia c la sua cardinalità), da un insieme di operatori $\{\tilde{A}_j\}$ con cardinalità pari a $\mathrm{rank}(I_\mathsf{H} - K)$ e da uno spazio L con dimensione pari a $c + \mathrm{rank}(I_\mathsf{H} - K)$. Allora deve valere:

$$(c + \mathrm{rank}(I_\mathsf{H} - K)) \times \dim \mathsf{K} \geq \dim \mathsf{H} \tag{2.11}$$

per *qualunque* mappa $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$.

dilatata a un operatore unitario [9]:

Lemma 2 (dilatazioni di Gram-Schmidt) *Un'isometria* $T \in \mathsf{B}(\mathsf{R},\mathsf{S})$ *ammette sempre una dilatazione unitaria* $U \in \mathsf{B}(\mathsf{S})$.

Dim. Sia J lo spazio di Hilbert definito dalla relazione $\mathsf{S} = \mathsf{R} \oplus \mathsf{J}$. Deve essere $\dim \mathsf{J} \geq 1$ poiché T è un'isometria, i.e. $\dim \mathsf{S} > \dim \mathsf{R}$ (se $\dim \mathsf{S} = \dim \mathsf{R}$, T è già unitario). Costruiamo $U = T \cdot + \cdot W$ dove anche $W \in \mathsf{B}(\mathsf{J},\mathsf{S})$ è un'isometria. Se è soddisfatta la seguente condizione:

$$T^\dagger W = 0 \tag{2.12}$$

l'operatore U definito sopra è chiaramente unitario. Resta da dimostrare l'esistenza di un W con le caratteristiche richieste: questa è però assicurata dal fatto che i W adatti sono tutti e soli quegli operatori che hanno per colonne $\{W(k)\}_{k=1,\ldots,\dim \mathsf{J}}$ i vettori di una base ortonormale per $\mathsf{J} = \mathsf{Rng}(I_\mathsf{S} - TT^\dagger) \subset \mathsf{S}$ [5]; poiché $\dim \mathsf{J} > 0$, è sempre possibile costruirne.■

Siamo ora in grado di dimostrare il seguente:

Teorema 8 (dilatazioni di Stinespring unitarie) *Una mappa* $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ *è una quantum operation se e solo se può essere scritta nella forma*

$$\mathrm{M}(X) = (I_\mathsf{H} \dot{+} 0_{\mathsf{H},\mathsf{D}})^\dagger \; U^\dagger \; (X \otimes \Sigma) \; U \; (I_\mathsf{H} \dot{+} 0_{\mathsf{H},\mathsf{D}}) \tag{2.13}$$

dove, posto $\mathsf{D} \doteq (\mathsf{K} \otimes \mathsf{L}) \ominus \mathsf{H}$, *l'operatore* $U \in \mathsf{B}(\mathsf{K} \otimes \mathsf{L})$ *è unitario,* $\Sigma \in \mathsf{B}(\mathsf{L})$ *è un proiettore non nullo e* $0_{\mathsf{H},\mathsf{D}} \in \mathsf{B}(\mathsf{H},\mathsf{D})$ *è l'operatore nullo.*

Dim. [Se] L'operatore $U(I_\mathsf{H} \dot{+} 0_{\mathsf{H},\mathsf{D}})$ è un'isometria in $\mathsf{B}(\mathsf{H},\mathsf{K} \otimes \mathsf{L})$. Allora, per il Teorema(7), la mappa M è una quantum operation.

[5] I vettori $\{W(k)\}_{k=1,\ldots,\dim \mathsf{J}}$ sono pure ortogonali a *tutti* i vettori di R, dal momento che J e R sono in somma diretta per costruzione.

[Solo se] Sia M una quantum operation. Per il Teorema(7) possiamo scrivere $\mathrm{M}(X) = T^\dagger(X \otimes \Sigma)T$ con $T \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{L})$ isometria e $\Sigma \in \mathsf{B}(\mathsf{L})$ proiettore non nullo. Ora, grazie al Lemma(2), dilatiamo l'isometria T all'operatore unitario $U = (T \cdot + \cdot W)$ con $W \in \mathsf{B}(\mathsf{D}, \mathsf{K} \otimes \mathsf{L})$ isometria. Poiché $U(I_{\mathsf{H}} \dot{+} 0_{\mathsf{H},\mathsf{D}}) = T$, si ottiene il risultato voluto.■

Si vede quindi che anche una quantum operation trace-decreasing può essere interpretata come interazione unitaria tra il sistema e un'ancilla. La presenza dell'operatore di compressione $(I_{\mathsf{H}} \dot{+} 0_{\mathsf{H},\mathsf{D}})$, il quale non è nient'altro che un'isometria da H in $\mathsf{K} \otimes \mathsf{L}$, serve solamente a ridurre lo spazio di arrivo dell'operatore unitario allo spazio di arrivo originale della mappa. La "fisica", tuttavia, rimane per intero contenuta nell'operatore unitario U.

Per ricavare la forma duale di eq.(2.13), c'è prima bisogno del seguente risultato:

Lemma 3 *Siano* H, D *spazi di Hilbert. Vale la seguente identità* [6]*:*

$$\mathrm{Tr}[(\Gamma_{\mathsf{H}} \cdot + \cdot 0_{\mathsf{D},\mathsf{H}})\Lambda(\Delta_{\mathsf{H}} \dot{+} 0_{\mathsf{H},\mathsf{D}})] = \mathrm{Tr}[(\Gamma_{\mathsf{H}} \oplus 0_{\mathsf{D}})\Lambda(\Delta_{\mathsf{H}} \oplus 0_{\mathsf{D}})] \tag{2.14}$$

dove $\Gamma_{\mathsf{H}}, \Delta_{\mathsf{H}} \in \mathsf{B}(\mathsf{H})$, $0_{\mathsf{D},\mathsf{H}} \in \mathsf{B}(\mathsf{D}, \mathsf{H})$, $\Lambda \in \mathsf{B}(\mathsf{H} \oplus \mathsf{D})$, $0_{\mathsf{H},\mathsf{D}} \in \mathsf{B}(\mathsf{H}, \mathsf{D})$ *e* $0_{\mathsf{D}} \in \mathsf{B}(\mathsf{D})$.

Dim. Si ha che

$$(\Gamma_{\mathsf{H}} \cdot + \cdot 0_{\mathsf{D},\mathsf{H}})\Lambda(\Delta_{\mathsf{H}} \dot{+} 0_{\mathsf{H},\mathsf{D}}) = \begin{pmatrix} \Gamma_{\mathsf{H}} & 0_{\mathsf{D},\mathsf{H}} \end{pmatrix} \begin{pmatrix} \Lambda^1_{\mathsf{H}\oplus\mathsf{D},\mathsf{H}} \\ \Lambda^2_{\mathsf{H}\oplus\mathsf{D},\mathsf{D}} \end{pmatrix} \begin{pmatrix} \Delta_{\mathsf{H}} \\ 0_{\mathsf{H},\mathsf{D}} \end{pmatrix} \tag{2.15}$$

e quindi

$$\mathrm{Tr}[(\Gamma_{\mathsf{H}} \cdot + \cdot 0_{\mathsf{D},\mathsf{H}})\Lambda(\Delta_{\mathsf{H}} \dot{+} 0_{\mathsf{H},\mathsf{D}})] = \mathrm{Tr}\left[(\Gamma\Lambda^1)_{\mathsf{H}\oplus\mathsf{D},\mathsf{H}} \begin{pmatrix} \Delta_{\mathsf{H}} \\ 0_{\mathsf{H},\mathsf{D}} \end{pmatrix} \right]. \tag{2.16}$$

[6] Le due tracce sono entrambe totali ma su spazi diversi: in particolare la taccia al primo membro è su H mentre la seconda è su $\mathsf{H} \oplus \mathsf{D}$.

D'altra parte

$$(\Gamma_{\mathsf{H}} \oplus 0_{\mathsf{D}})\Lambda(\Delta_{\mathsf{H}} \oplus 0_{\mathsf{D}}) = \begin{pmatrix} \Gamma_{\mathsf{H}} & 0 \\ 0 & 0_{\mathsf{D}} \end{pmatrix} \begin{pmatrix} \Lambda^1_{\mathsf{H}\oplus\mathsf{D},\mathsf{H}} \\ \Lambda^2_{\mathsf{H}\oplus\mathsf{D},\mathsf{D}} \end{pmatrix} \begin{pmatrix} \Delta_{\mathsf{H}} & 0 \\ 0 & 0_{\mathsf{D}} \end{pmatrix} \tag{2.17}$$

e quindi

$$\mathrm{Tr}[(\Gamma_{\mathsf{H}} \oplus 0_{\mathsf{D}})\Lambda(\Delta_{\mathsf{H}} \oplus 0_{\mathsf{D}})] = \mathrm{Tr}\left[\begin{pmatrix} (\Gamma\Lambda^1)_{\mathsf{H}\oplus\mathsf{D},\mathsf{H}} \begin{pmatrix} \Delta_{\mathsf{H}} \\ 0 \end{pmatrix} & 0 \\ 0 & 0_{\mathsf{D}} \end{pmatrix}\right] . \blacksquare \tag{2.18}$$

È possibile ora enunciare il seguente:

Corollario 6 (forma duale per le dilatazioni unitarie) *La forma duale della quantum operation data in eq.(2.13) è* [7]*:*

$$\mathrm{M}^{\tau}(\rho) = \mathrm{Tr}_{\mathsf{L}}[(I_{\mathsf{K}} \otimes \Sigma)\ U\ (\rho \oplus 0_{\mathsf{D}})\ U^{\dagger}] \tag{2.19}$$

dove $\rho \in \mathsf{T}(\mathsf{H})$ *è lo stato di input e* $0_{\mathsf{D}} \in \mathsf{B}(\mathsf{D})$ *è l'operatore nullo su* $\mathsf{D} = (\mathsf{K} \otimes \mathsf{L}) \ominus \mathsf{H}$.

Dim. La relazione di dualità è data da

$$\mathrm{Tr}[\mathrm{M}(X)\rho] = \mathrm{Tr}[X\mathrm{M}^{\tau}(\rho)]. \tag{2.20}$$

Espandendo il primo membro si ha:

$$\begin{aligned} \mathrm{Tr}[\mathrm{M}(X)\rho] &= \mathrm{Tr}[(I_{\mathsf{H}} \dot{+} 0_{\mathsf{H},\mathsf{D}})^{\dagger} U^{\dagger}(X \otimes \Sigma)U(I_{\mathsf{H}} \dot{+} 0_{\mathsf{H},\mathsf{D}})\rho] = \\ &= \mathrm{Tr}[(I_{\mathsf{H}} \cdot + \cdot\, 0_{\mathsf{D},\mathsf{H}})U^{\dagger}(X \otimes \Sigma)U(\rho \dot{+} 0_{\mathsf{H},\mathsf{D}})]; \end{aligned} \tag{2.21}$$

facendo uso del Lemma(20) e permutando ciclicamente gli operatori tracciati, possiamo scrivere:

$$\mathrm{Tr}[\mathrm{M}(X)\rho] = \mathrm{Tr}[U^{\dagger}(X \otimes \Sigma)U(\rho \oplus 0_{\mathsf{D}})(I_{\mathsf{H}} \oplus 0_{\mathsf{D}})]. \tag{2.22}$$

[7] Se $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ allora $\mathrm{M}^{\tau} : \mathsf{T}(\mathsf{H}) \longrightarrow \mathsf{T}(\mathsf{K})$.

Siamo arrivati ad avere

$$\mathrm{Tr}[X\mathrm{M}^{\tau}(\rho)] = \mathrm{Tr}[U^{\dagger}(X \otimes \Sigma)U(\rho \oplus 0_{\mathsf{D}})] \tag{2.23}$$

e quindi, ricordando l'isomorfismo $\mathsf{H} \oplus \mathsf{D} \cong \mathsf{K} \otimes \mathsf{L}$,

$$\mathrm{Tr}[X\mathrm{M}^{\tau}(\rho)] = \mathrm{Tr}_{\mathsf{K}}[X \ \ \mathrm{Tr}_{\mathsf{L}}[(I_{\mathsf{K}} \otimes \Sigma)U(\rho \oplus 0_{\mathsf{D}})U^{\dagger}] \ ]. \ \blacksquare \tag{2.24}$$

Fin qui abbiamo sviluppato il procedimento più generale per ottenere le dilatazioni di Stinespring unitarie. Piuttosto che con compressioni, però, è più semplice lavorare con elementi parziali di matrice, come si era fatto, ad esempio, nel Teorema(4). È possibile ottenere una riscrittura in questo senso dei risultati ottenuti scegliendo, nel processo di dilatazione, uno spazio di Hilbert L tale per cui $\dim \mathsf{L} \times \dim \mathsf{K} = r \dim \mathsf{H}$ con $r \in \mathbb{N}$. Allora, introducendo un secondo spazio di ancilla R con $\dim \mathsf{R} = r$, si ha che $\mathsf{K} \otimes \mathsf{L} \cong \mathsf{H} \otimes \mathsf{R}$ e si ottiene il seguente:

Teorema 9 *Una mappa* $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ *è una quantum operation se e solo se può essere scritta come* [8]

$$\mathrm{M}(X) = \langle \phi_{\mathsf{R}} | U^{\dagger}(X \otimes \Sigma)U | \phi_{\mathsf{R}} \rangle \tag{2.25}$$

dove $X \in \mathsf{B}(\mathsf{K})$ *è l'input,* $\Sigma \in \mathsf{B}(\mathsf{L})$ *è un proiettore non nullo sullo spazio di ancilla* L*,* $U \in \mathsf{B}(\mathsf{K} \otimes \mathsf{L})$ *è un operatore unitario e* $|\phi_{\mathsf{R}}\rangle \in \mathsf{R}$ *è un fissato vettore normalizzato. La forma duale è*

$$\mathrm{M}^{\tau}(\rho) = \mathrm{Tr}_{\mathsf{L}}[(I_{\mathsf{K}} \otimes \Sigma)U(|\phi_{\mathsf{R}}\rangle\langle\phi_{\mathsf{R}}| \otimes \rho)U^{\dagger}] \tag{2.26}$$

dove ora l'input è lo stato $\rho \in \mathsf{T}(\mathsf{H})$*.*

[8] $\langle \phi_{\mathsf{R}} | U^{\dagger}(X \otimes \Sigma)U | \phi_{\mathsf{R}} \rangle$ è solo un elemento parziale di matrice. Per rendere la scrittura più chiara si può scrivere come $(\langle \phi_{\mathsf{R}}| \otimes I_{\mathsf{H}})U^{\dagger}(X \otimes \Sigma)U(|\phi_{\mathsf{R}}\rangle \otimes I_{\mathsf{H}})$.

Dim. Partiamo dalla forma data in eq.(2.13):

$$\mathrm{M}(X) = (I_{\mathsf{H}} \dot{+} 0_{\mathsf{H,D}})^{\dagger} U^{\dagger} \ (X \otimes \Sigma) U (I_{\mathsf{H}} \dot{+} 0_{\mathsf{H,D}}) \tag{2.27}$$

dove ora lo spazio L è stato dilatato fino ad essere tale che

$$\dim \mathsf{K} \otimes \mathsf{L} = \dim \mathsf{K} \times \dim \mathsf{L} = r \dim \mathsf{H} \tag{2.28}$$

con $r \in \mathbb{N}$. Lo spazio D, quindi, poiché era stato definito come $\mathsf{D} = (\mathsf{K} \otimes \mathsf{L}) \ominus \mathsf{H}$, ha ora dimensione pari a $\dim \mathsf{K} \times \dim \mathsf{L} - \dim \mathsf{H} = (r-1) \dim \mathsf{H}$.

Introduciamo ora un nuovo spazio di Hilbert R con $\dim \mathsf{R} = r$. Sarà:

$$\dim \mathsf{K} \otimes \mathsf{L} = \dim \mathsf{R} \otimes \mathsf{H} \tag{2.29}$$

e quindi

$$\mathsf{K} \otimes \mathsf{L} \cong \mathsf{R} \otimes \mathsf{H}. \tag{2.30}$$

Fissiamo basi ortonormali in tutti gli spazi K, L, R e H; sia $|\phi_{\mathsf{R}}\rangle \in \mathsf{R}$ il vettore che ha la prima componente pari a 1 e tutte le altre nulle.

Ricordando la convenzione di Kronecker per la rappresentazione del prodotto tensoriale di matrici per cui

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}, \tag{2.31}$$

sono chiare le sostituzioni

$$I_{\mathsf{H}} \dot{+} 0_{\mathsf{H,D}} \longrightarrow |\phi_{\mathsf{R}}\rangle \otimes I_{\mathsf{H}} \tag{2.32}$$

e

$$\rho \oplus 0_{\mathsf{D}} \longrightarrow |\phi_{\mathsf{R}}\rangle\langle\phi_{\mathsf{R}}| \otimes \rho. \ \blacksquare \tag{2.33}$$

L'eq.(2.26) è la generalizzazione di eq.(1.33): infatti, poiché $I_{\mathsf{K}} \otimes \Sigma$ è un operatore positivo, si può scrivere $I_{\mathsf{K}} \otimes \Sigma = C^\dagger C$ con $C \in \mathsf{B}(\mathsf{K} \otimes \mathsf{L})$ opportuno. A questo punto si verifica che in effetti l'operatore CU è una contrazione. Il Teorema(4), tuttavia, non sarebbe stato direttamente applicabile al caso generale di una mappa con spazi di partenza e di arrivo non isomorfi.

2.4 Sommario del processo di dilatazione unitaria

Per concludere, ricapitoliamo per punti i passi percorsi:

1. Data una quantum operation $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$, se ne sceglie una decomposizione di Kraus qualunque $\sum_i M_i^\dagger \cdot M_i$ con $\{M_i\} \subset \mathsf{B}(\mathsf{H}, \mathsf{K})$.

2. Se la quantum operation M è trace-preserving, i.e. $\mathrm{M}(I_{\mathsf{K}}) = I_{\mathsf{H}}$, si passa al punto successivo. Altrimenti si costruiscono con il Lemma(1) gli operatori $\{\widetilde{M}_j\} \subset \mathsf{B}(\mathsf{H}, \mathsf{K})$ complementari alla mappa: quelli, cioè, per cui $\sum_i M_i^\dagger M_i + \sum_j \widetilde{M}_j^\dagger \widetilde{M}_j = I_{\mathsf{H}}$.

3. Si introduce uno spazio di ancilla L di dimensione sufficientemente grande da poter trovare un set di vettori ortonormali $\{|l_i\rangle, |\widetilde{l}_j\rangle\}$ in numero pari alla somma delle cardinalità di $\{M_i\}$ e $\{\widetilde{M}_j\}$.

4. Si aumenta la dimensione di L (aggiungendo corrispondentemente entrate nulle ai vettori ortonormali di cui al punto sopra) finché $\dim \mathsf{K} \times \dim \mathsf{L} = n \dim \mathsf{H}$ con $0 < n \in \mathbb{N}$.

5. Si costruisce l'operatore $M = \sum_i M_i \otimes |l_i\rangle + \sum_j \widetilde{M}_j \otimes |\widetilde{l}_j\rangle$. Automaticamente si ha che $M \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{L})$ è un'isometria in quanto $M^\dagger M = \sum_i M_i^\dagger M_i + \sum_j \widetilde{M}_j^\dagger \widetilde{M}_j = I_{\mathsf{H}}$.

6. Si introduce un secondo [9] spazio di ancilla R con dimensione pari a $\dim \mathsf{K} \times \dim \mathsf{L} - \dim \mathsf{H}$, cioè tale che $\mathsf{K} \otimes \mathsf{L} \cong \mathsf{R} \otimes \mathsf{H}$. Si fissa in R una base ortonormale $\{|r_k\rangle\}$.

7. Si costruisce l'isometria $P \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{L})$ tramite la relazione $P = |r_1\rangle \otimes I_{\mathsf{H}}$, dove $|r_1\rangle \in \mathsf{R}$ è il vettore che ha prima componente pari a 1 e tutte le altre nulle.

8. Tramite il Lemma(2) di Gram-Schmidt, si estende l'isometria M di cui al punto 5 a un operatore unitario $U \in \mathsf{B}(\mathsf{K} \otimes \mathsf{L})$ aggiungendo colonne alla destra di M.

9. L'estensione unitaria è conclusa, in quanto $UP = M$.

10. L'azione della mappa M è ricostruita tramite l'equazione

$$\mathrm{M}(X) = P^\dagger U^\dagger (X \otimes \Sigma) U P \tag{2.34}$$

dove $\Sigma \in \mathsf{B}(\mathsf{L})$ è un proiettore non nullo definito come $\Sigma = \sum_i |l_i\rangle\langle l_i|$. La mappa duale $\mathrm{M}^\tau : \mathsf{T}(\mathsf{H}) \longrightarrow \mathsf{T}(\mathsf{K})$ è data da

$$\mathrm{M}^\tau(\rho) = \mathrm{Tr}_{\mathsf{L}}[(I_{\mathsf{K}} \otimes \Sigma)\ U(|r_1\rangle\langle r_1| \otimes \rho)U^\dagger]. \tag{2.35}$$

[9] Una seconda ancilla è necessaria nel caso generale in cui $\dim \mathsf{K} \neq \dim \mathsf{H}$. Se $\dim \mathsf{K} = \dim \mathsf{H}$ il secondo spazio di ancilla si identifica con L.

Capitolo 3

Teoria della maggiorizzazione

3.1 Insiemi ordinati

Ricordiamo la seguente:

Definizione 5 *Dato un insieme* A*, si dice che una relazione* $\mathcal{R}$ *in* A *è una* relazione d'ordine parziale *in* A *se essa gode delle proprietà seguenti:*

1. ***transitiva****: se* $(x, y) \in \mathcal{R}$ *e* $(y, z) \in \mathcal{R}$ *allora* $(x, z) \in \mathcal{R}$*;*

2. ***antisimmetrica****:* $(x, y) \in \mathcal{R}$ *implica* $(y, x) \notin \mathcal{R}$*.*

Un ordinamento in A *viene detto* totale *se, per ogni coppia di elementi* $x, y \in \mathsf{A}$*, con* $x \neq y$*, è possibile scrivere* $(x, y) \in \mathcal{R}$ *o* $(y, x) \in \mathcal{R}$*.*

In seguito, introducendo un ordinamento parziale o totale, invece di scrivere $(x, y) \in \mathcal{R}$, useremo la notazione più compatta $x \prec y$.

3.2 Nozioni generali

È possibile confrontare due quantità vettoriali; le relazioni che si ottengono, che non definiscono tuttavia un ordinamento (nemmeno parziale), vengono dette in genere *relazioni di maggiorizzazione*.

Sia $x = (x_1,\ ...,\ x_n)$ un elemento di $\mathbb{R}^n$. Indichiamo con $x^{\downarrow}$ il vettore ottenuto da x riarrangiandone le componenti in ordine decrescente.

Definizione 6 *Siano $x, y \in \mathbb{R}^n$. Si dice che x è* maggiorizzato *da y, i.e. $x \prec y$, se*

$$\sum_{j=1}^{k} x_j^{\downarrow} \leq \sum_{j=1}^{k} y_j^{\downarrow}, \quad 1 \leq k \leq n, \tag{3.1}$$

e

$$\sum_{j=1}^{n} x_j^{\downarrow} = \sum_{j=1}^{n} y_j^{\downarrow}. \tag{3.2}$$

La nozione di maggiorizzazione qui definita ha un'interpretazione naturale. Prendiamo l'esempio di un vettore $x \in \mathbb{R}^n$ con $x_i \geq 0$ e $\sum_i x_i = 1$. Vale sempre

$$\left(\frac{1}{n},\ ...,\ \frac{1}{n}\right) \prec x \prec (1,\ 0,\ ...,\ 0); \tag{3.3}$$

leggendo il vettore x come una distribuzione di probabilità, si può dire che la scrittura $x \prec y$ significa che il vettore x è "più disordinato" del vettore y.

Si era detto che la relazione di maggiorizzazione non introduce un ordinamento parziale su $\mathbb{R}^n$. Infatti è riflessiva e transitiva ma non antisimmetrica: se $x \prec y$ e $y \prec x$ si può solo affermare che $x = Py$, dove P è una matrice che permuta le componenti del vettore cui è applicata.

Tuttavia quest'ostacolo è aggirabile nel modo seguente: introducendo una relazione d'equivalenza su $\mathbb{R}^n$ definita dalla relazione $x \sim y$ se $x = Py$ con P permutazione, costruiamo l'insieme quoziente $\mathbb{R}^n/\sim$. Allora la relazione $\prec$ definisce un ordinamento parziale sull'insieme quoziente.

Definizione 7 *Una matrice $A = (a_{ij})$ quadrata $(n \times n)$ è detta* bistocastica *se $a_{ij} \geq 0$ per ogni i, j e se*

$$\sum_{i=1}^{n} a_{ij} = 1 \quad \textit{per ogni } j, \tag{3.4}$$

$$\sum_{j=1}^{n} a_{ij} = 1 \quad \textit{per ogni } i. \tag{3.5}$$

Se $U = (u_{ij})$ è una matrice unitaria, la matrice $(|u_{ij}|^2)$ è chiaramente bistocastica; tale matrice viene detta *unistocastica*. Se U è reale ortogonale, la matrice bistocastica che si ottiene viene detta *ortostocastica*.

Il seguente risultato, di cui non diamo la dimostrazione (si veda [10]), lega le relazioni di maggiorizzazione alle matrici unistocastiche:

Teorema 10 *Dati due vettori $x, y \in \mathbb{R}^n$, $x \prec y$ se e solo se esiste una matrice unistocastica A tale per cui*

$$x = Ay. \tag{3.6}$$

Un altro risultato, dovuto a Birkhoff, chiarisce il significato di maggiorizzazione:

Teorema 11 (Birkhoff) *L'insieme delle matrici bistocastiche è un insieme convesso i cui vertici sono le matrici di permutazione.*

Anche di questo tralasciamo la dimostrazione. Si può tuttavia notare che un vettore è maggiorizzato da un altro se e solo se le sue componenti possono essere ottenute "mediando" quelle del vettore maggiorizzante. In altre parole, $x \prec y$ significa che x è combinazione convessa di un certo numero di permutazioni di y. È chiaro quindi perché un vettore maggiorizzato viene interpretato come "più disordinato" del vettore maggiorizzante.

3.3 Applicazioni

3.3.1 Funzioni Schur-convesse

Definizione 8 *Una funzione* $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ *è detta* Schur-convessa *se* $x \prec y$ *implica* $f(x) \leq f(y)$.

La definizione può sembrare inappropriata, in quanto la condizione di Schur-convessità è una condizione di monotonicità piuttosto che di vera e propria convessità. Tuttavia, leggendo x come combinazione lineare convessa di permutazioni di y, si capisce il motivo della definizione.

Esempi di funzioni Schur-convesse sono:

$$\begin{aligned} f(x) &= \sum_i x_i^k, \quad k \geq 1; \\ f(x) &= -\prod_i x_i; \\ f(x) &= \sum_i x_i \ln(x_i). \end{aligned} \tag{3.7}$$

3.3.2 Distribuzioni di probabilità consistenti con uno stato

Cominciamo con una riscrittura del Teorema(3):

Teorema 12 *Sia* H *uno spazio di Hilbert e sia* $\rho \in \mathsf{T}(\mathsf{H})$ *uno stato con* $\rho = \sum_{j=1}^m |\psi_j\rangle\langle\psi_j|$ *dove i vettori* $\{|\psi_j\rangle\}$ *non sono normalizzati. Un altro insieme di vettori* $\{|\phi_i\rangle\}$ *descrive lo stesso stato, i.e.* $\rho = \sum_{i=1}^n |\phi_i\rangle\langle\phi_i|$ *con* $n \geq m$, *se e solo se esiste una matrice unitaria* $U \in \mathsf{M}_n$ *tale per cui*

$$|\phi_i\rangle = \sum_j U_{ij}|\psi_j\rangle. \tag{3.8}$$

Dim. La dimostrazione ricalca esattamente quella di Teorema(3). L'unica cosa da notare è che, poiché in generale si è preso $n \geq m$, bisogna aggiungere all'insieme $\{|\psi_j\rangle\}$ dei vettori fittizi di norma nulla in modo tale da pareggiare le cardinalità dei due ensembles.■

A questo punto abbiamo tutti gli elementi che servono per dimostrare il seguente [11]:

Teorema 13 (Nielsen) *Sia $\rho \in \mathsf{T}(\mathsf{H})$ una matrice densità. Sia (p_i) una distribuzione di probabilità. Allora esiste un insieme $\{|\phi_i\rangle\}$ di stati normalizzati (ma non ortogonali) tali che:*

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i| \tag{3.9}$$

se e solo se $(p_i) \prec (\lambda_j)$, dove (λ_j) è il vettore degli autovalori di ρ.

Dim. È sempre inteso che se il vettore (p_i) ha più entrate di (λ_j), quest'ultimo viene completato da una serie di zeri.

[Se] Sia $(p_i) \prec (\lambda_j)$. Per il Teorema(10) possiamo trovare una matrice unitaria $U = (u_{ij})$ per cui

$$p_i = \sum_j |u_{ij}|^2 \lambda_j. \tag{3.10}$$

Data la diagonalizzazione $\rho = \sum_j |\psi_j\rangle\langle\psi_j|$ con $\langle\psi_k|\psi_l\rangle = \lambda_k \delta_{kl}$, definiamo gli stati $\{|\phi_i\rangle\}$ tramite l'equazione

$$|\phi_i\rangle = \frac{1}{\sqrt{p_i}} \sum_j u_{ij} |\psi_j\rangle \tag{3.11}$$

in cui, eventualmente, si sono aggiunti all'insieme $\{|\psi_j\rangle\}$ alcuni vettori di norma nulla in modo tale che le cardinalità di $\{|\phi_i\rangle\}$ e di $\{|\psi_j\rangle\}$ siano uguali. Chiaramente, grazie al Teorema(12), è immediato verificare che $\sum_i p_i |\phi_i\rangle\langle\phi_i| =$

ρ. Resta quindi solo da dimostrare che gli stati $\{|\phi_i\rangle\}$ sono normalizzati. Effettuando il conto:

$$\langle\phi_i|\phi_i\rangle = \frac{1}{p_i}\sum_{jk} u_{ij}^* u_{ik}\langle\psi_j|\psi_k\rangle = \frac{1}{p_i}\sum_j |u_{ij}|^2\lambda_j = 1 \tag{3.12}$$

si ottiene il risultato.

[Solo se] Data la diagonalizzazione $\rho = \sum_j |\psi_j\rangle\langle\psi_j|$ con $\langle\psi_k|\psi_l\rangle = \lambda_k\ \delta_{kl}$, supponiamo che esista un insieme di stati normalizzati $\{|\phi_i\rangle\}$ e una distribuzione di probabilità (p_i) per cui:

$$\rho = \sum_i p_i|\phi_i\rangle\langle\phi_i|. \tag{3.13}$$

Per il Teorema(12) deve esistere una matrice unitaria $U = (u_{ij})$ tale che:

$$\sqrt{p_i}|\phi_i\rangle = \sum_j u_{ij}|\psi_j\rangle; \tag{3.14}$$

moltiplicando quest'ultima relazione per la sua aggiunta si ha:

$$p_i = \sum_{jk} u_{ij}^* u_{ik}\langle\psi_j|\psi_k\rangle = \sum_j |u_{ij}|^2\lambda_j \tag{3.15}$$

e quindi, per il Teorema(10), si ottiene $(p_i) \prec (\lambda_j)$.■

Dal precedente Teorema si ottiene il seguente:

Corollario 7 *Sia* $\rho \in \mathsf{T}(\mathsf{H})$ *uno stato con* $\mathrm{rank}(\rho) = r$. *Allora per ogni* $n \geq r$ *esiste un insieme di* n *stati normalizzati* $\{|\phi_i\rangle\}$ *in termini dei quali* ρ *può essere scritto come miscela equiprobabile:*

$$\rho = \sum_{i=1}^{n} \frac{|\phi_i\rangle\langle\phi_i|}{n}. \tag{3.16}$$

Dim. Banale, dal momento che, per costruzione, $(\frac{1}{n},\ ...,\ \frac{1}{n}) \prec (\lambda_j)$.■

3.3.3 Condizioni sulla realizzazione unitaria di *quantum operations*

Nel Teorema(1) abbiamo visto come associare a una mappa $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ un operatore positivo $R_{\mathrm{M}} \in \mathsf{L}(\mathsf{K} \otimes \mathsf{H})$ tramite la relazione

$$R_{\mathrm{M}} = \mathrm{M}^{\tau} \otimes \mathrm{I}\ (|I\rangle\rangle\langle\langle I|). \tag{3.17}$$

Si è anche dimostrato che vi è corrispondenza biunivoca tra gli insiemi $\mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ e $\{R \in \mathsf{L}(\mathsf{K} \otimes \mathsf{H}) : \ R \geq 0,\ \mathrm{Tr}_1[R] = K\}$. Poiché per spazi di Hilbert finiti $0 < \mathrm{Tr}[K] < \infty$, abbiamo allora un'iniezione:

$$\begin{cases} \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K) \longrightarrow \{\text{stati in } \mathsf{T}(\mathsf{K} \otimes \mathsf{H})\} \\ \mathrm{M} \longmapsto \rho_{\mathrm{M}} = \dfrac{1}{\mathrm{Tr}[K]} R_{\mathrm{M}}. \end{cases} \tag{3.18}$$

È possibile quindi trasferire alle mappe tutti i risultati che abbiamo relativi alla realizzabilità di stati quantistici in termini delle proprietà degli ensembles.

Sfruttando il Teorema(13), è immediato il seguente:

Teorema 14 *Sia* $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ *una quantum operation con decomposizione di Kraus cononica data da* $\mathrm{M} = \sum_{j=1}^{k} K_j^{\dagger} \cdot K_j$*, cioè tale che* $\langle K_i, K_j \rangle_{HS} = \mathrm{Tr}[K_i^{\dagger} K_j] = \|K_i\|_2^2\ \delta_{ij}$.
Allora qualunque altra decomposizione di Kraus $\mathrm{M} = \sum_{i=1}^{n} M_i^{\dagger} \cdot M_i$ *deve soddisfare la relazione di maggiorizzazione:*

$$\left(\|M_i\|_2^2\right) \prec \left(\|K_j\|_2^2\right). \tag{3.19}$$

Facciamo ora riferimento al risultato finale ottenuto per le dilatazioni unitarie di quantum operations e riassunto in Teorema(9) dall'equazione:

$$\mathrm{M}(X) = \langle \phi_{\mathsf{R}} | U^{\dagger} (X \otimes \Sigma) U | \phi_{\mathsf{R}} \rangle \tag{3.20}$$

in cui, data $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ quantum operation, $X \in \mathsf{B}(\mathsf{K})$ è l'input, $\Sigma \in \mathsf{L}(\mathsf{L})$ è un proiettore non nullo fissato, $U \in \mathsf{L}(\mathsf{K} \otimes \mathsf{L})$ è l'operatore unitario che realizza la mappa e $|\phi_{\mathsf{R}}\rangle \in \mathsf{R}$ è uno stato fissato; gli spazi di Hilbert K e H sono fissati dalla mappa M, mentre L e R sono costruiti in modo tale che $\mathsf{K} \otimes \mathsf{L} \cong \mathsf{R} \otimes \mathsf{H}$.

Dal momento che, per come è stato costruito U, si ha che gli operatori:

$$\{(I_{\mathsf{K}} \otimes \langle l_i|)U(|\phi_{\mathsf{R}}\rangle \otimes I_{\mathsf{H}})\} = \{M_i\} \tag{3.21}$$

costituiscono [1] una decomposizione di Kraus per M, possiamo riscrivere il Teorema precedente come:

Teorema 15 *Sia* $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ *una quantum operation con decomposizione di Kraus canonica data da* $\mathrm{M} = \sum_{j=1}^{k} K_j^\dagger \cdot K_j$*, cioè tale che* $\langle K_i, K_j \rangle_{HS} = \mathrm{Tr}[K_i^\dagger K_j] = \|K_i\|_2^2 \, \delta_{ij}$.
Allora qualunque realizzazione unitaria

$$\mathrm{M}(X) = \langle \phi_{\mathsf{R}}|U^\dagger(X \otimes \Sigma)U|\phi_{\mathsf{R}}\rangle \tag{3.22}$$

deve soddisfare la relazione di maggiorizzazione:

$$\left(\mathrm{Tr}\left[\langle \phi_{\mathsf{R}}|U^\dagger|l_i\rangle\langle l_i|U|\phi_{\mathsf{R}}\rangle\right]\right) \prec \left(\|K_j\|_2^2\right). \tag{3.23}$$

Dal momento che $\{|l_i\rangle\} \subset \mathsf{L}$ costituisce una base ortonormale per $\mathsf{Rng}(\Sigma)$, il vettore $\left(\mathrm{Tr}\left[\langle \phi_{\mathsf{R}}|U^\dagger|l_i\rangle\langle l_i|U|\phi_{\mathsf{R}}\rangle\right]\right)$ ha un numero di entrate pari a $\mathrm{rank}(\Sigma)$. Perché la relazione di maggiorizzazione possa essere soddisfatta deve quindi valere:

$$\dim \mathsf{L} \geq \mathrm{rank}(\Sigma) \geq k \tag{3.24}$$

dove k è la cardinalità della decomposizione di Kraus canonica. Questa è una condizione necessaria sulla dimensione dello spazio di ancilla L affinché sia possibile costruire una dilatazione unitaria della mappa.

[1] L'insieme $\{|l_i\rangle\} \subset \mathsf{L}$ è una base ortonormale per $\mathsf{Rng}(\Sigma)$.

Questo risultato deve essere confrontato con quello riportato in nota alla dimostrazione del Teorema(7) e ottenuto con metodi totalmente differenti.

Capitolo 4

Teoria dei *frames*

4.1 Nozioni generali

La teoria dei *frames* nasce nell'ambito della ricerca su decomposizioni di segnali e serie di Fourier non armoniche. In genere, per ricostruire un vettore di uno spazio di Hilbert, è necessario avere a disposizione una base. Tuttavia è anche possibile utilizzare insiemi di vettori che riescono sempre ad analizzare l'intero spazio ma che hanno, rispetto alle basi, proprietà più deboli. In questo modo sono più semplici da trattare e da costruire e hanno una maggiore flessibilità rispetto a una base. Come testo si faccia riferimento a [12].

Definizione 9 *Dato uno spazio di Hilbert* H*, una sequenza di vettori* $\{|x_n\rangle\} \subset \mathsf{H}$ *è detta* frame *per* H *se esistono costanti reali* $0 < a \leq b < +\infty$ *tali per cui*

$$a \ \||v\rangle\|^2 \leq \sum_n |\langle x_n|v\rangle|^2 \leq b \ \||v\rangle\|^2 \tag{4.1}$$

per ogni $|v\rangle \in \mathsf{H}$*.*

Se $a = b$*, il frame viene detto* tight *(letteralmente,* stretto*); se* $a = b = 1$*, viene detto* normalized tight*. Un frame è* esatto *se cessa di essere un frame*

nel caso in cui gli venga tolto un elemento; un frame non esatto viene detto over-completo.

È immediato verificare che una base ortonormale $\{|e_n\rangle\}$ è un *normalized tight frame*. Ma pure le sequenze:

$$\begin{aligned}
&\{|e_1\rangle,\ 0,\ |e_2\rangle,\ 0,\ |e_3\rangle,\ 0,\ ...\} \\
&\{\frac{1}{\sqrt{2}}|e_1\rangle,\ \frac{1}{\sqrt{2}}|e_1\rangle,\ \frac{1}{\sqrt{2}}|e_2\rangle,\ \frac{1}{\sqrt{2}}|e_2\rangle,\ ...\} \\
&\{|e_1\rangle,\ \frac{1}{\sqrt{2}}|e_2\rangle,\ \frac{1}{\sqrt{2}}|e_2\rangle,\ \frac{1}{\sqrt{3}}|e_3\rangle,\ \frac{1}{\sqrt{3}}|e_3\rangle,\ \frac{1}{\sqrt{3}}|e_3\rangle,\ ...\}
\end{aligned} \tag{4.2}$$

sono normalized tight frames.

Esempi di sequenze che non costituiscono frames sono $\{\frac{|e_n\rangle}{n}\}$ (per cui non è possibile trovare un $a > 0$ che soddisfi eq.(4.1)) e $\{n|e_n\rangle\}$ (per cui, invece, non è possibile trovare la costante $b < +\infty$).

Concludendo, diamo il seguente risultato:

Proposizione 2 *Sia* $\{|x_n\rangle\}$ *un frame generico con costanti di frame* $0 < a \leq b < +\infty$. *Allora* $\||x_n\rangle\| \leq b$ *per ogni* n.

Per la dimostrazione si veda [12].

4.2 *Frames* e operatori

Sia H uno spazio di Hilbert (eventualmente di dimensione infinita). Sia $\{|x_n\rangle\}_{n\in\mathbb{I}} \subset \mathsf{H}$ una sequenza qualsiasi di vettori con $\mathbb{I}$ opportuno insieme di indici discreti. Sia K un secondo spazio di Hilbert con dimensione pari alla cardinalità di $\mathbb{I}$ [1] e sia $\{|e_n\rangle\}$ una sua base ortonormale. Si dice *operatore di*

[1] Funziona tutto anche nel caso in cui $\mathbb{I}$ abbia cardinalità infinita.

preframe l'operatore $T \in \mathsf{L}(\mathsf{K}, \mathsf{H})$ definito dalla relazione [2]

$$T|e_n\rangle = |x_n\rangle \tag{4.3}$$

per ogni $n \in \mathbb{I}$. Per spazi di Hilbert finiti, è possibile rappresentare l'operatore T tramite la matrice che ha come colonne i vettori $\{|x_n\rangle\}$. Vale il seguente:

Teorema 16 *Sia* H *uno spazio di Hilbert e sia* $\{|x_n\rangle\} \subset \mathsf{H}$ *una sequenza qualsiasi di vettori con operatore di preframe* T*. Le seguenti affermazioni sono equivalenti:*

1. $\{|x_n\rangle\}$ *è un frame per* H*;*

2. *l'operatore* $T^\dagger$ *è lineare, limitato e iniettivo.*

Dim. Poiché $\langle e_n|T^\dagger|v\rangle = (T|e_n\rangle)^\dagger|v\rangle = \langle x_n|v\rangle$ si ha che

$$T^\dagger|v\rangle = \sum_n \langle x_n|v\rangle|e_n\rangle \tag{4.4}$$

e

$$\|T^\dagger|v\rangle\|^2 = \sum_n |\langle x_n|v\rangle|^2, \tag{4.5}$$

per ogni $|v\rangle \in \mathsf{H}$. Confrontando le ultime due equazioni con eq.(4.1), si ottiene il risultato. ■

Da eq.(4.5) si ottengono immediatamente i seguenti:

Corollario 8 *Sia* H *uno spazio di Hilbert e sia* $\{|x_n\rangle\} \subset \mathsf{H}$ *una sequenza qualsiasi di vettori con operatore di preframe* T*. Allora* $\{|x_n\rangle\}$ *è un normalized tight frame per* H *se e solo se* $T^\dagger \in \mathsf{L}(\mathsf{H}, \mathsf{K})$ *è un'isometria, i.e.* $TT^\dagger = I_{\mathsf{H}}$.

[2] Se stiamo trattando con spazi di dimensione infinita, si avrà $T \in \mathsf{B}(\mathsf{H})$ senza la necessità di introdurre uno spazio K: infatti, anche se overcompleto, il frame ha sempre cardinalità numerabile.

Dim. Da eq.(4.5) con $\|T^\dagger|v\rangle\|^2 = \||v\rangle\|^2$.■

Il precedente Corollario può essere letto nel modo seguente: data un'isometria $T \in \mathsf{B}(\mathsf{H},\mathsf{K})$, le sue righe formano un normalized tight frame per H.

Corollario 9 *Sia* $\{|x_n\rangle\}$ *un normalized tight frame per* H. *Allora* $\sum_n \||x_n\rangle\|^2 = \dim \mathsf{H}$.

Dim. Se $T^\dagger$ è un'isometria, $T^\dagger T \in \mathsf{B}(\mathsf{K})$ è il proiettore sul sottospazio $\tilde{\mathsf{H}} \subseteq \mathsf{K}$ isomorfo a H. Notando che $\sum_n \||x_n\rangle\|^2 = \mathrm{Tr}[T^\dagger T]$, si ottiene il risultato.■

Per giungere a un risultato di cui faremo uso in seguito, è necessario richiamare la seguente:

Proposizione 3 *Se* $A \in \mathsf{B}(\mathsf{H})$ *è tale che* [3] $\|A\| < 1$ *allora* $I - A$ *è invertibile.*

Dim. Sia $B = \sum_{n=0}^{\infty} A^n$. La serie converge assolutamente dal momento che $\|A\| < 1$. Sia $S_k = \sum_{n=0}^{k} A^n$. Allora

$$(I - A)S_k = (I - A)(I + \sum_{n=1}^{k} A^n) = I - A^{k+1} \longrightarrow I; \tag{4.6}$$

d'altra parte deve essere pure

$$(I - A)S_k \longrightarrow (I - A)B. \tag{4.7}$$

Ma allora $B = (I - A)^{-1}$.■

Corollario 10 *Se* $A \in \mathsf{B}(\mathsf{H})$ *è tale che* $\|I - A\| < 1$ *allora* A *è invertibile.*

Dim. Per la Proposizione precedente, poiché $\|I - A\| < 1$, si ha l'invertibilità di $I - (I - A) = A$.■

Abbiamo ora tutti gli elementi per dimostrare il seguente:

[3] Con $\|\cdot\|$ indichiamo una qualunque norma su $\mathsf{B}(\mathsf{H})$ tale per cui $\|I\| = 1$.

Teorema 17 *Ogni* $T \in \mathsf{B}(\mathsf{H})$ *può essere scritto nella forma* $T = a(U_1 + U_2 + U_3)$*, dove gli* $\{U_i\}$ *sono operatori unitari e* $a \in \mathbb{R}^+$*.*

Dim. Fissato $0 < \alpha < 1$, sia

$$S = \frac{I}{2} + \frac{1-\alpha}{2}\frac{T}{\|T\|}. \tag{4.8}$$

Poiché $\|I - S\| < 1$, per il Corollario(10) si ha l'invertibilità di S. È possibile quindi scrivere la decomposizione polare di S come

$$S = UP = \frac{1}{2}U(W + W^\dagger) = \frac{1}{2}(UW + UW^\dagger) \tag{4.9}$$

dove U, W sono unitari [4]. Concludendo, si ha:

$$T = \frac{\|T\|}{1-\alpha}(UW + UW^\dagger - I); \tag{4.10}$$

si è costruita una decomposizione di T nella forma richiesta. ■

In termini di frames, vedendo T come operatore di preframe, è possibile riscrivere il precedente Teorema come segue:

Teorema 18 *Qualunque frame per uno spazio di Hilbert di dimensione infinita è il multiplo di una somma di tre basi ortonormali.*

La condizione sulla dimensione dello spazio è necessaria in quanto, per frame su spazi finiti, l'operatore di preframe è rappresentabile tramite una matrice rettangolare: questo impedisce la sua decomposizione in somma di operatori unitari.

Il seguente risultato, di cui non diamo la dimostrazione, specializzando il frame, indebolisce le ipotesi sullo spazio:

[4] Si è utilizzato anche il risultato [6] per cui un operatore hermitiano contrattivo può sempre essere decomposto in una somma del tipo $\frac{1}{2}(W + W^\dagger)$ con W unitario. L'operatore hermitiano P che compare in eq.(4.9) è in effetti contrattivo in quanto $\|S\| \leq \frac{1}{2} + \frac{1}{2} - \frac{\alpha}{2} < 1$.

Corollario 11 *Qualunque base può essere scritta come combinazione lineare di due basi ortonormali.*

4.3 *Frames* e *quantum operations*

Si è visto, grazie al Corollario(8), il legame che esiste tra isometrie e normalized tight frames. Isometrie compaiono anche nel Teorema(3) e sono legate alla libertà esistente nel definire una decomposizione di Kraus data una quantum operation. Mettendo insieme questi due risultati si giunge al seguente:

Teorema 19 *Sia* $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ *una quantum operation generica. Sia* k *la cardinalità delle sue decomposizioni di Kraus minimali e sia* L *uno spazio di Hilbert con* $\dim \mathsf{L} = k$*. Allora c'è una corrispondenza biunivoca tra normalized tight frames per* L *e decomposizioni di Kraus per* M*.*

Dim. Sia $\{K_i\}_{i=1,\ldots,k}$ l'insieme degli operatori di Kraus di una decomposizione canonica di M. Da questi, tramite una matrice unitaria $U \in \mathsf{M}_k$, è possibile ottenere tutte le altre decomposizioni minimali. Ogni matrice unitaria $k \times k$ è in corrispondenza biunivoca con una base ortonormale di L: è noto infatti come le righe di una matrice unitaria formino una base ortonormale. Per quanto riguarda le decomposizioni di Kraus non minimali, sappiamo che sono ottenibili da quelle minimali tramite una matrice isometrica $T \in \mathsf{M}_{n,k}$ con $n > k$. Ogni isometria $n \times k$ è in corrisponedenza biunivoca con un normalized tight frame per L: è noto [5] infatti come le righe di una matrice isometrica formino un normalized tight frame.

[5] Vedi commento al Corollario(8).

Si è quindi costruita la seguente corrispondenza:

$$\begin{aligned} &\text{dec. canonica} \longleftrightarrow \text{base standard;} \\ &\text{dec. minimale} \longleftrightarrow \text{base ortonormale;} \\ &\text{dec. generica} \longleftrightarrow \text{normalized tight frame.}\blacksquare \end{aligned} \tag{4.11}$$

Riferendosi a L come allo spazio di ancilla utilizzato nel Teorema(6), si chiarisce il significato fisico della libertà che esiste nella definizione di una decomposizione di Kraus per una quantum operation: cambiare decomposizione di Kraus per la mappa equivale a cambiare frame per l'ancilla. Si prenda infatti la forma di Stinespring per una mappa $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ data in eq.(2.6):

$$\mathrm{M}(X) = T^{\dagger}(X \otimes I_{\mathsf{L}})T \tag{4.12}$$

dove la contrazione $T = \sum_{i=1}^{k} T_i \otimes |l_i\rangle$ è ottenuta a partire da una decomposizione di Kraus minimale $\{T_i\}$ per M. Applichiamo ora il Teorema(3) per ottenere una generica decomposizione di Kraus tramite una matrice isometrica $A = (a_{rs}) \in \mathsf{M}_{n,k}$:

$$M_j = \sum_{i=1}^{k} a_{ji} T_i. \tag{4.13}$$

Invertendo l'equazione precedente si ha:

$$T_r = \sum_{j=1}^{n} (A^{\dagger})_{rj} M_j = \sum_{j=1}^{n} a_{jr}^{*} M_j; \tag{4.14}$$

possiamo allora riscrivere la contrazione di Stinespring come:

$$\begin{aligned} T &= \sum_{i=1}^{k} T_i \otimes |l_i\rangle = \\ &= \sum_{i=1}^{k} \sum_{j=1}^{n} a_{ji}^{*} M_j \otimes |l_i\rangle = \\ &= \sum_{j=1}^{n} M_j \otimes |x_j\rangle \end{aligned} \tag{4.15}$$

dove ora $|x_j\rangle = \sum_{i=1}^{k} a_{ji}^{*}|l_i\rangle$ è un elemento di un normalized tight frame per L [6].

L'operazione che in questo modo si compie non ha un vero e proprio significato fisico per il sistema principale il quale, infatti, è soggetto sempre alla medesima quantum operation; è l'effetto sull'ancilla a cambiare e, studiando quest'aspetto della mappa, è possibile approfondire la conoscenza di alcune sue proprietà [7].

[6] In quanto colonna j-esima di $A^{\dagger}$.

[7] Vedi capitolo seguente.

Capitolo 5

Quantum operations estremali

5.1 Insiemi convessi

Da [13]: sia Q un sottoinsieme generico di uno spazio vettoriale su $\mathbb{R}$. Presi due suoi elementi qualunque $x, y \in \mathsf{Q}$, l'insieme

$$\{z = \theta x + (1-\theta)y,\ 0 \leq \theta \leq 1\} \tag{5.1}$$

viene detto *segmento* congiungente x e y.

Definizione 10 *Se, per ogni $x, y \in \mathsf{Q}$, il segmento congiungente x e y è per intero contenuto in Q, l'insieme Q viene detto* convesso.

Sono insiemi convessi: un insieme contenente un unico elemento; un segmento di linea; un sottospazio di $\mathbb{R}^n$. Non sono insiemi convessi: un insieme con cardinalità finita maggiore di 1; l'unione di due o più sottospazi di $\mathbb{R}^n$ nessuno dei quali è sottospazio degli altri.

Vale la seguente proprietà:

Proposizione 4 *L'intersezione di due insiemi convessi è convessa.*

La generalizzazione immediata del concetto di segmento è data dalla *combinazione lineare convessa*: dati un numero finito di elementi $\{x_i\} \in \mathsf{Q}$ si definisce come combinazione convessa la somma

$$\sum_i p_i x_i \tag{5.2}$$

dove $p_i \geq 0$ per ogni i e $\sum_i p_i = 1$.

È chiaro che, se un insieme è convesso, allora qualunque combinazione convessa di suoi elementi gli appartiene. Inoltre, qualunque elemento di un insieme convesso può essere espresso in termini di combinazione convessa di elementi dell'insieme. Esistono tuttavia elementi che *non* possono essere combinazione convessa di *altri* elementi: è questo il caso dei cosiddetti *punti estremali* [1].

Se si ha a che fare con un insieme convesso, è di fondamentale importanza riuscire a caratterizzare i suoi punti estremali: la sola conoscenza di questi, infatti, permette di comprendere la struttura dell'intero insieme.

5.2 Il Teorema di Choi

Convesso è anche l'insieme delle mappe completamente positive $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ con $\mathrm{M}(I_\mathsf{K}) = K \leq I_\mathsf{H}$, insieme che indichiamo con $\mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$. Per individuarne i punti estremali esiste il seguente [14]:

Teorema 20 (Choi) *Una mappa* $\mathrm{T} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ *è estremale se e solo se ammette una decomposizione di Kraus* $\mathrm{T} = \sum_i T_i^\dagger \cdot T_i$ *con* $\{T_i^\dagger T_j\} \subset \mathsf{B}(\mathsf{H})$ *insieme di elementi linearmente indipendenti.*

Dim. Prima di tutto bisogna sottolineare il fatto che se i $\{T_i^\dagger T_j\}$ sono linearmente indipendenti, allora sono linearmente indipendenti anche i singoli

[1] Si vedano, come esempio geometrico, i vertici di un poliedro convesso.

$\{T_i\}$. Procediamo per assurdo: supponiamo che gli operatori $\{T_i\}$ siano linearmente dipendenti, cioè che esista un vettore non nullo (λ_i) per cui $\sum_i \lambda_i T_i = 0$. Moltiplicando a sinistra il primo membro per il suo aggiunto si ottiene

$$\sum_{ij} \lambda_i^* \lambda_j T_i^\dagger T_j = 0 \tag{5.3}$$

che è la condizione di dipendenza lineare per i $\{T_i^\dagger T_j\}$. Nel seguito della dimostrazione, quindi, tratteremo sempre con decomposizioni di Kraus minimali.

[Se] Supponiamo che la mappa $\mathrm{T} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ abbia una decomposizione di Kraus minimale $\sum_i T_i^\dagger \cdot T_i$ con i $\{T_i^\dagger T_j\}$ linearmente indipendenti. Procedendo per assurdo supponiamo anche che la mappa T non sia estremale, cioè che esistano due mappe $\mathrm{X}, \mathrm{Y} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ tali per cui

$$\mathrm{T} = \frac{1}{2}(\mathrm{X} + \mathrm{Y}). \tag{5.4}$$

Siano $\sum_j X_j^\dagger \cdot X_j$ e $\sum_k Y_k^\dagger \cdot Y_k$ loro decomposizioni di Kraus; allora

$$\mathrm{T} = \sum_i T_i^\dagger \cdot T_i = \frac{1}{2} \sum_j X_j^\dagger \cdot X_j + \frac{1}{2} \sum_k Y_k^\dagger \cdot Y_k. \tag{5.5}$$

Dal momento che i $\{T_i\}$ sono linearmente indipendenti e $\frac{1}{2}\sum_j X_j^\dagger \cdot X_j + \frac{1}{2}\sum_k Y_k^\dagger \cdot Y_k$ costituisce un'altra decomposizione di Kraus per T, deve essere possibile esprimere gli $\{X_j\}$ e gli $\{Y_k\}$ come combinazione lineare dei $\{T_i\}$. Sia ad esempio:

$$X_j = \sum_i a_{ji} T_i. \tag{5.6}$$

Poiché deve valere $\sum_j X_j^\dagger X_j = \sum_j \sum_{il} a_{ji}^* a_{jl} T_i^\dagger T_l = \sum_i T_i^\dagger T_i = K$, data l'indipendenza lineare dei $\{T_i^\dagger T_l\}$, si può concludere che

$$\sum_j a_{ji}^* a_{jl} = \delta_{il}. \tag{5.7}$$

Cioè (a_{ij}) è un'isometria e quindi, per il Teorema(3), T = X, i.e. T è estremale.

[Solo se] Sia T una mappa estremale e $\sum_i T_i^\dagger \cdot T_i$ una sua decomposizione di Kraus minimale, cioè con i $\{T_i\}$ linearmente indipendenti. Vogliamo dimostrare che la relazione $\sum_{ij} \lambda_{ij} T_i^\dagger T_j = 0$ implica che $(\lambda_{ij}) = 0$. Dal momento che $T_j^\dagger T_i = (T_i^\dagger T_j)^\dagger$ possiamo sempre prendere (λ_{ij}) hermitiana e, a meno di effettuare un riscalamento, $-I \leq (\lambda_{ij}) \leq I$.
Data allora una matrice hermitiana $\Lambda = (\lambda_{ij})$ con $-I \leq \Lambda \leq I$ per cui $\sum_{ij} \lambda_{ij} T_i^\dagger T_j = 0$, definiamo le mappe:

$$\begin{aligned} \mathrm{T}_+ &= \sum_i T_i^\dagger \cdot T_i + \sum_{ij} \lambda_{ij} T_i^\dagger \cdot T_j \\ \mathrm{T}_- &= \sum_i T_i^\dagger \cdot T_i - \sum_{ij} \lambda_{ij} T_i^\dagger \cdot T_j. \end{aligned} \tag{5.8}$$

Poiché $0 \leq I + \Lambda$, definiamo $A = (a_{ij})$ in modo tale che $A^\dagger A = I + \Lambda$. Costruiamo allora gli operatori $W_j = \sum_i a_{ji} T_i$ che non sono nulli vista l'indipendenza lineare dei $\{T_i\}$. Si ha:

$$\sum_j W_j^\dagger \cdot W_j = \sum_{il} (A^\dagger A)_{il} T_i^\dagger \cdot T_l = \mathrm{T}_+; \tag{5.9}$$

questa relazione, unitamente al fatto che $\sum_{ij} \lambda_{ij} T_i^\dagger T_j = 0$ per cui $\mathrm{T}_+(I_{\mathsf{K}}) = K$, ci assicura che $\mathrm{T}_+ \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ (analogamente si procede per T_- definendo l'operatore B tale che $B^\dagger B = I - \Lambda$).
D'altra parte è vero anche che

$$\mathrm{T} = \frac{1}{2}(\mathrm{T}_+ + \mathrm{T}_-). \tag{5.10}$$

Ma T è estremale per ipotesi e quindi deve essere

$$\mathrm{T} = \mathrm{T}_+ = \mathrm{T}_- \tag{5.11}$$

cioè A deve essere un'isometria e questa situazione si verifica solo se $\Lambda = 0$.■

Dalla dimostrazione si capisce anche che, se una decomposizione di Kraus minimale qualunque verifica la condizione di Choi, allora *tutte* le decomposizioni di Kraus minimali di quella mappa la verificano.

È notevole un'altra conseguenza del Teorema precedente: la condizione di indipendenza lineare per i $\{T_i^\dagger T_j\}$ limita la cardinalità delle decomposizioni di Kraus minimali per una mappa estremale. Sia infatti $\dim \mathsf{H} = h$ e $\dim \mathsf{K} = k$. Per una mappa qualunque, la decomposizione di Kraus è minimale se i $\{T_i\} \subset \mathsf{B}(\mathsf{H}, \mathsf{K})$ sono linearmente indipendenti: non ve ne possono essere, quindi, più di $h \times k$. Per una mappa estremale, invece, deve valere anche l'indipendenza lineare dei $\{T_i^\dagger T_j\} \subset \mathsf{B}(\mathsf{H})$: questi, allora, non possono essere più di h^2 e una decomposizione minimale non può avere cardinalità superiore a h.

5.3 Mappe ancillari

5.3.1 Mappe ancillari dirette

Si era detto, alla fine del capitolo precedente, che lo studio dell'effetto di una quantum operation sull'ancilla, invece che sul sistema principale, può servire per comprendere la struttura della mappa. Per questo motivo, a partire dalla forma di Stinespring per una quantum operation data nel Teorema(6), si definiscono le "mappe ancillari":

Definizione 11 *Sia* $\mathrm{T} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ *definita da:*

$$\mathrm{T}(X) = T^\dagger (X \otimes I_{\mathsf{L}}) T \tag{5.12}$$

con $T \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{L})$ *contrazione. Si definisce allora la* mappa ancillare

associata a eq.(5.12) [2] *tramite la relazione:*

$$\widetilde{\mathrm{T}}(\Lambda) = T^\dagger(I_{\mathsf{K}} \otimes \Lambda)T. \tag{5.13}$$

Vale il seguente:

Teorema 21 *La mappa ancillare definita sopra è una quantum operation in* $\mathsf{CP}(\mathsf{B}(\mathsf{L}), \mathsf{B}(\mathsf{H}), K)$.

Dim. Costruiamo l'operatore $E \in \mathsf{B}(\mathsf{K} \otimes \mathsf{L}, \mathsf{L} \otimes \mathsf{K})$ tramite l'equazione:

$$E = \sum_{i=1}^{\dim \mathsf{K}} \sum_{j=1}^{\dim \mathsf{L}} (|l_j\rangle \otimes |k_i\rangle)\ (\langle k_i| \otimes \langle l_j|) \tag{5.14}$$

dove $\{|k_i\rangle\}$ è una base ortonormale per K e analogamente $\{|l_j\rangle\}$ per L. Identificando i due spazi isomorfi $\mathsf{K}\otimes\mathsf{L}$ e $\mathsf{L}\otimes\mathsf{K}$, è immediato verificare che l'operatore E è unitario. Utilizzando E possiamo riscrivere la mappa ancillare come:

$$\widetilde{\mathrm{T}}(\Lambda) = T^\dagger E^\dagger(\Lambda \otimes I_{\mathsf{K}})ET. \tag{5.15}$$

A questo punto, grazie al Teorema(6), possiamo affermare che $\widetilde{\mathrm{T}}$ è in effetti una CP-map e possiamo estrarne una decomposizione di Kraus: si ha $\widetilde{\mathrm{T}} = \sum_i \widetilde{T}_i^\dagger \cdot \widetilde{T}_i$ dove

$$\widetilde{T}_i = (I_{\mathsf{L}} \otimes \langle k_i|)ET = \sum_j |l_j\rangle\langle k_i|T_j \tag{5.16}$$

con $\{\widetilde{T}_i\} \subset \mathsf{B}(\mathsf{H}, \mathsf{L})$. Resta da controllare la normalizzazione della mappa: già da eq.(5.13) si vede che $\widetilde{\mathrm{T}}(I_{\mathsf{L}}) = \mathrm{T}(I_{\mathsf{K}}) = K$.■

Per come è definita, è inevitabile che la mappa ancillare risenta della scelta sulla decomposizione di Kraus utilizzata per costruire la dilatazione di Stinespring della mappa principale. Non è possibile aggirare quest'ostacolo, in quanto, come si era già notato nella sezione 4.3 "*Frames* e *quantum*

[2] È fondamentale il fatto che *la* mappa ancillare è associata alla *particolare* contrazione T usata per rappresentare la mappa T.

operations", la libertà isometrica presente nella rappresentazione di Kraus si riflette sullo spazio di ancilla il quale viene modificato profondamente; la mappa principale non risente di questa modifica poiché l'ancilla viene "tracciata via" al termine dei calcoli; la mappa ancillare, invece, *deve* cambiare proprio per come è stata definita.

Noi utilizzeremo le mappe ancillari per caratterizzare le mappe estremali sfruttando il Teorema di Choi. Poiché quest'ultimo è incentrato sulle decomposizioni di Kraus minimali, d'ora in avanti tratteremo solo con mappe ancillari *minimali* che definiamo essere tutte e sole quelle originate da una contrazione di Stinespring costruita a partire da una decomposizione di Kraus minimale.

È possibile a questo punto riscrivere il Teorema di Choi nel modo seguente:

Teorema 22 *Una mappa* $\mathrm{T} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ *è estremale se e solo se ammette una mappa ancillare minimale* $\widetilde{\mathrm{T}} \in \mathsf{CP}(\mathsf{B}(\mathsf{L}), \mathsf{B}(\mathsf{H}), K)$ *invertibile a sinistra.*

Dim. Dalla definizione di mappa ancillare minimale si ricava:

$$\widetilde{\mathrm{T}}(\Lambda) = \sum_{ij} \lambda_{ij} T_i^\dagger T_j \tag{5.17}$$

dove i $\{T_i\}$ costruiscono una decomposizione di Kraus minimale per T. D'altra parte, una mappa generica M ammette inversa sinistra se e solo se $\mathrm{M}(f) = 0$ implica $f = 0$. La condizione di Choi, quindi, non è altro che la condizione di invertibilità sinistra per la mappa ancillare.■

Come già notato in precedenza per le decomposizioni di Kraus minimali, anche per le mappe ancillari si può affermare che, se una mappa ancillare minimale qualunque verifica la condizione di invertibilità a sinistra, allora *tutte* le mappe ancillari minimali la verificano.

5.3.2 Esempio

Intuitivamente, il Teorema(22) suggerisce che una mappa estremale causi sull'ancilla una trasformazione che è in corrispondenza biunivoca con gli "outcomes" del sistema principale. È possibile chiarire e rendere più rigorosa quest'idea come segue.

Sia $\mathrm{M} : \mathsf{B}(\mathsf{K}) \longrightarrow \mathsf{B}(\mathsf{H})$ una quantum operation trace-preserving. Tramite il Teorema(6) scriviamo l'azione della sua duale come:

$$\mathrm{M}^{\tau}(\rho) = \mathrm{Tr}_{\mathsf{L}}[V\rho V^{\dagger}] \tag{5.18}$$

dove $\rho \in \mathsf{T}(\mathsf{H})$ è lo stato di input e $V \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{L})$ è un'isometria, i.e. $V^{\dagger}V = I_{\mathsf{H}}$, costruita a partire da una decomposizione di Kraus minimale $\{E_i\} \subset \mathsf{B}(\mathsf{H}, \mathsf{K})$.

Sia $\{|l_i\rangle\}$ una base ortonormale per lo spazio di ancilla L. Allora:

$$\begin{aligned} \mathrm{M}^{\tau}(\rho) &= \sum_i \langle l_i|V\rho V^{\dagger}|l_i\rangle = \\ &= \sum_i \mathrm{Tr}[\langle l_i|V\rho V^{\dagger}|l_i\rangle] \ \frac{\langle l_i|V\rho V^{\dagger}|l_i\rangle}{\mathrm{Tr}[\langle l_i|V\rho V^{\dagger}|l_i\rangle]} = \\ &= \sum_i \mathrm{Tr}[(I_{\mathsf{K}} \otimes |l_i\rangle\langle l_i|) \ V\rho V^{\dagger}] \ \sigma_i \end{aligned} \tag{5.19}$$

dove i $\sigma_i \in \mathsf{T}(\mathsf{K})$ sono gli stati normalizzati $\sigma_i = \frac{\langle l_i|V\rho V^{\dagger}|l_i\rangle}{\mathrm{Tr}[\langle l_i|V\rho V^{\dagger}|l_i\rangle]} = \frac{E_i\rho E_i^{\dagger}}{\mathrm{Tr}[E_i^{\dagger}E_i\rho]}$. Sfruttando l'invarianza della traccia sotto permutazioni cicliche dei suoi argomenti e ricordando la definizione di mappa ancillare, si ottiene:

$$\begin{aligned} \mathrm{M}^{\tau}(\rho) &= \sum_i \mathrm{Tr}[(I_{\mathsf{K}} \otimes |l_i\rangle\langle l_i|) \ V\rho V^{\dagger}] \ \sigma_i = \\ &= \sum_i \mathrm{Tr}[V^{\dagger}(I_{\mathsf{K}} \otimes |l_i\rangle\langle l_i|)V \ \rho] \ \sigma_i = \\ &= \sum_i \mathrm{Tr}[\widetilde{\mathrm{M}}(|l_i\rangle\langle l_i|) \ \rho] \ \sigma_i \end{aligned} \tag{5.20}$$

dove $\widetilde{\mathrm{M}} : \mathsf{B}(\mathsf{L}) \longrightarrow \mathsf{B}(\mathsf{H})$ è la mappa ancillare associata a M tramite V.

Vedendo $\{|l_i\rangle\langle l_i|\}$ come una POVM su L, si può allora affermare che *l'evoluzione attraverso* M *di uno stato* $\rho \in \mathsf{T}(\mathsf{H})$ *avviene mediando i risultati di una misura effettuata sull'evoluto attraverso* $\widetilde{\mathrm{M}}$ *di una POVM su* L.

Supponiamo ora che M sia pure estremale. Sia allora $\widetilde{\mathrm{M}}$ una sua mappa ancillare minimale (e, per il Teorema(22), invertibile). A causa dell'invertibilità di $\widetilde{\mathrm{M}}$, quindi, *l'evoluzione di uno stato* $\rho \in \mathsf{T}(\mathsf{H})$ *attraverso una mappa estremale è univocamente determinata dal risultato di una misurazione sull'ancilla* [3].

In conclusione, sottolineiamo il fatto che la nozione di mappa ancillare discende in modo naturale dal concetto di misurazione indiretta. Sia infatti $\rho \in \mathsf{T}(\mathsf{H})$ lo stato del sistema principale; lasciando interagire quest'ultimo con uno stato puro di *environment* $|\omega\rangle\langle\omega| \in \mathsf{T}(\mathsf{R})$ ed effettuando una misura su R tramite una POVM $\{\Pi_r\}$, la probabilità di ottenere il risultato k-esimo risulta:

$$\begin{aligned} p_k &= \mathrm{Tr}[U(\rho \otimes |\omega\rangle\langle\omega|)U^\dagger \; I_{\mathsf{H}} \otimes \Pi_k] = \\ &= \mathrm{Tr}[\rho \otimes |\omega\rangle\langle\omega| \; U^\dagger(I_{\mathsf{H}} \otimes \Pi_k)U] = \\ &= \mathrm{Tr}[\rho \; (I_{\mathsf{H}} \otimes \langle\omega|)U^\dagger(I_{\mathsf{H}} \otimes \Pi_k)U(I_{\mathsf{H}} \otimes |\omega\rangle) = \\ &= \mathrm{Tr}[\rho \; \widetilde{\mathrm{M}}(\Pi_k)]; \end{aligned} \tag{5.21}$$

questo significa che lo schema di misurazione indiretta sull'ancilla con una POVM $\{\Pi_r\}$ equivale allo schema di misurazione diretta sul sistema principale con POVM $\{\widetilde{\mathrm{M}}(\Pi_r)\}$.

[3] Confronta a questo proposito l'interpretazione di una quantum operation qualsiasi in termini di canali rumorosi classici data in sezione 1.3.1 "QO's e canali rumorosi"; lì, però, l'univocità della corrispondenza in generale non vale.

5.3.3 Mappe ancillari duali

A partire da una mappa $\mathrm{T} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ e da una sua decomposizione di Kraus $\mathrm{T} = \sum_i T_i^\dagger \cdot T_i$ si costruisce immediatamente la sua duale $\mathrm{T}^\tau \in \mathsf{CP}(\mathsf{T}(\mathsf{H}), \mathsf{T}(\mathsf{K}))$ tramite la relazione:

$$\mathrm{T}^\tau = \sum_i T_i \cdot T_i^\dagger. \tag{5.22}$$

Analogamente, data la CP-map ancillare associata $\widetilde{\mathrm{T}} = \sum_j \widetilde{T}_j^\dagger \cdot \widetilde{T}_j$ con $\widetilde{T}_j = \sum_i |l_i\rangle\langle k_j| T_i$, è possibile costruire la sua duale:

$$\begin{aligned} \widetilde{\mathrm{T}}^\tau &= \sum_j \widetilde{T}_j \cdot \widetilde{T}_j^\dagger = \\ &= \sum_j \sum_{lk} |l_l\rangle\langle k_j| T_l \cdot T_k^\dagger |k_j\rangle\langle l_k| = \\ &= \sum_{lk} \mathrm{Tr}[T_l \cdot T_k^\dagger] \ |l_l\rangle\langle l_k|. \end{aligned} \tag{5.23}$$

Inserendo l'argomento, ricordando l'espressione esplicita del prodotto interno di Hilbert-Schmidt e sfruttando l'invarianza della traccia sotto permutazioni cicliche degli argomenti si ottiene:

$$\begin{aligned} \widetilde{\mathrm{T}}^\tau(\rho) &= \sum_{lk} \mathrm{Tr}[T_l \rho T_k^\dagger] \ |l_l\rangle\langle l_k| = \\ &= \sum_{lk} \langle T_l^\dagger T_k, \rho\rangle_{HS} \ |l_l\rangle\langle l_k|. \end{aligned} \tag{5.24}$$

Per una mappa estremale, $\{T_l^\dagger T_k\}$ è un insieme di elementi linearmente indipendenti; si può quindi dire che $\{T_l^\dagger T_k\}$ è una base per $\mathsf{span}\{T_l^\dagger T_k\} \subseteq \mathsf{B}(\mathsf{H})$. D'altra parte, $\{|l_l\rangle\langle l_k|\}$ è una base ortonormale per $\mathsf{span}\{|l_l\rangle\langle l_k|\}$. È vero pure che $\mathsf{span}\{T_l^\dagger T_k\} \cong \mathsf{span}\{|l_l\rangle\langle l_k|\}$ in quanto sono due spazi vettoriali con la medesima dimensione.

Facendo ora ricorso al Corollario(11), scriviamo

$$T_l^\dagger T_k = aE_{lk} + bF_{lk}, \quad \text{per ogni } l, k, \tag{5.25}$$

dove $\{E_{lk}\}$ e $\{F_{lk}\}$ sono due basi ortonormali per $\mathsf{span}\{T_l^\dagger T_k\}$ e $a, b \in \mathbb{R}$. In questo modo è possibile riscrivere eq.(5.24) nella forma:

$$\widetilde{\mathrm{T}}^\tau(\rho) = \sum_{lk} \langle aE_{lk} + bF_{lk}, \rho\rangle_{HS} \; |l_l\rangle\langle l_k|. \tag{5.26}$$

Identificando i due spazi isomorfi $\mathsf{span}\{T_l^\dagger T_k\}$ e $\mathsf{span}\{|l_l\rangle\langle l_k|\}$, la mappa ancillare duale assume l'espressione:

$$\widetilde{\mathrm{T}}^\tau(\rho) = (aU + bV)(\rho) \tag{5.27}$$

dove U e V sono due operatori lineari su $\mathsf{T}(\mathsf{H})$ le cui restrizioni [4] a $\mathsf{span}\{T_l^\dagger T_k\}$ sono operatori unitari. Visto che, inoltre, il loro nucleo coincide proprio con il complemento ortogonale di $\mathsf{span}\{T_l^\dagger T_k\}$, si può affermare che $U, V : \mathsf{L}(\mathsf{H}) \longrightarrow \mathsf{L}(\mathsf{H})$ sono della forma

$$U = \widetilde{U} \oplus 0 \qquad V = \widetilde{V} \oplus 0 \tag{5.28}$$

dove $\widetilde{U}, \widetilde{V} : \mathsf{span}\{T_l^\dagger T_k\} \longrightarrow \mathsf{span}\{T_l^\dagger T_k\}$ sono operatori unitari.

[4] Restrizioni e non compressioni in quanto $\mathsf{span}\{T_l^\dagger T_k\}$ è per essi un sottospazio invariante.

Capitolo 6

Distinguibilità tra mappe quantistiche

6.1 Norme di operatori

6.1.1 Norme invarianti unitarie

In questa sezione tratteremo sempre con lo spazio vettoriale (di Hilbert) $\mathbb{C}^n$, con $n < \infty$, dotato del prodotto scalare *standard* $\langle\cdot|\cdot\rangle$ e della norma $\|\cdot\|$ a esso associata. Come testo di riferimento si consideri [10].

Definizione 12 *Dato* $A \in \mathsf{L}(\mathbb{C}^n)$ *si definisce come* norma *di* A *lo scalare:*

$$\|A\| = \sup_{\||v\rangle\|=1} \|A|v\rangle\|. \tag{6.1}$$

Indichiamo con $|A|$ l'operatore positivo $(A^\dagger A)^{1/2}$ e con $s(A)$ il vettore costituito dai valori singolari di A con le componenti arrangiate in ordine decrescente, cioè in modo tale che $s_1(A) \geq s_2(A) \geq \cdots \geq s_n(A)$. Allora:

$$\|A\| = \| \, |A| \, \| = s_1(A). \tag{6.2}$$

Da questa relazione si capisce pure che la norma definita sopra è *invariante unitaria*, nel senso che:

$$\|A\| = \|UAV\|, \tag{6.3}$$

dove U e V sono due operatori unitari qualunque in $\mathsf{L}(\mathbb{C}^n)$. Di norme invarianti unitarie, che noi indicheremo con il simbolo $|||\cdot|||$, ne esistono infinite, oltre alla norma data in Definizione(12): vi sono, ad esempio, le *p-norme* di Schatten e le *k-norme* di Ky-Fan. In ogni caso, normalizziamo tutte le norme invarianti unitarie in modo tale che:

$$\left|\left|\left| \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \right|\right|\right| = 1. \tag{6.4}$$

6.1.2 *p*-norme di Schatten

Le p-norme di Schatten sono definite dall'equazione [1]:

$$\|A\|_p = \left(\sum_{j=1}^{n} (s_j(A))^p \right)^{1/p}, \tag{6.5}$$

per ogni $1 \leq p < \infty$. Si definisce inoltre:

$$\|A\|_\infty = s_1(A) = \|A\|. \tag{6.6}$$

Per $p = 1$ si ottiene la *norma-traccia*: $\|A\|_1 = \mathrm{Tr}[|A|]$. Per $p = 2$ si ottiene invece la *norma di Hilbert-Schmidt*: $\|A\|_2 = \mathrm{Tr}[A^\dagger A]$. La norma di Hilbert-Schmidt riveste un ruolo di particolare importanza tra le norme invarianti unitarie: discende infatti dal prodotto scalare di Hilbert-Schmidt $\langle A, B\rangle = \mathrm{Tr}[A^\dagger B]$ definito su $\mathsf{L}(\mathbb{C}^n)$. Poiché

$$\|A\|_2 = \left(\sum_{i,j=1}^{n} |a_{ij}|^2 \right)^{1/2}, \tag{6.7}$$

[1] Si nota che le p-norme sono già normalizzate.

la norma di Hilbert-Schmidt non è nient'altro che la norma euclidea (standard) su $\mathsf{L}(\mathbb{C}^n)$ visto come spazio vettoriale isomorfo a $\mathbb{C}^{n^2}$.

6.1.3 k-norme di Ky-Fan

Le k-norme di Ky-Fan sono definite dall'equazione [2]:

$$\|A\|_{(k)} = \sum_{j=1}^{k} s_j(A), \quad \text{per } 1 \leq k \leq n. \tag{6.8}$$

Valgono le relazioni:

$$\begin{aligned} &\|A\|_{(1)} = \|A\|_\infty = s_1(A) \quad \text{e} \\ &\|A\|_{(n)} = \|A\|_1. \end{aligned} \tag{6.9}$$

Il risultato principale riguardante le k-norme è il seguente:

Teorema 23 *Siano $A, B \in \mathsf{L}(\mathbb{C}^n)$. Se*

$$\|A\|_{(k)} \leq \|B\|_{(k)} \tag{6.10}$$

per ogni $1 \leq k \leq n$, allora

$$|||A||| \leq |||B||| \tag{6.11}$$

per ogni norma $|||\cdot|||$ invariante unitaria.

6.1.4 Proprietà generali delle norme invarianti unitarie

Per ogni $A, B \in \mathsf{L}(\mathbb{C}^n)$, qualunque norma invariante unitaria, oltre a essere *subadditiva*:

$$|||A + B||| \leq |||A||| + |||B|||, \tag{6.12}$$

[2] Anche le k-norme sono già normalizzate.

(proprietà, quest'ultima, implicita nel concetto stesso di norma [3]) è pure *submoltiplicativa*:

$$|||AB||| \leq |||A||| \; |||B|||. \tag{6.13}$$

Un'altra disuguaglianza soddisfatta dalle norme invarianti unitarie è la *disuguaglianza di Hölder* per cui:

$$|||AB||| \leq ||| \; |A|^p \; |||^{1/p} \; ||| \; |B|^q \; |||^{1/q}, \tag{6.14}$$

valida per ogni $p > 1$ e q tale che $\frac{1}{p} + \frac{1}{q} = 1$.

Dalla disuguaglianza di Hölder discende la *disuguaglianza di Cauchy-Schwarz*:

$$||| \; |AB|^{1/2} \; ||| \leq (|||A||| \; |||B|||)^{1/2}. \tag{6.15}$$

La relazione di dualità tra norme invarianti unitarie viene definita tramite il prodotto scalare di Hilbert-Schmidt:

Definizione 13 *Data una norma invariante unitaria* $|||\cdot|||$*, si definisce la* norma duale $|||\cdot|||'$ *tramite l'equazione:*

$$|||A|||' = \sup_{|||B|||=1} |\langle A, B\rangle| = \sup_{|||B|||=1} |\operatorname{Tr}[A^\dagger B]|. \tag{6.16}$$

Per la norma duale, è possibile dimostrare le seguenti proprietà:

1. $|\operatorname{Tr}[A^\dagger B]| \leq |||A||| \; |||B|||'$ per ogni norma invariante unitaria;
2. $\|A\|'_p = \|A\|_q$ per $1 \leq p \leq \infty$ con $\frac{1}{p} + \frac{1}{q} = 1$;
3. $\|A\|'_{(k)} = \max\{\|A\|_{(1)}, \frac{1}{k}\|A\|_{(n)}\}$ per $1 \leq k \leq n$;
4. l'unica norma invariante unitaria che sia duale di se stessa è la norma di Hilbert-Schmidt $\|\cdot\|_2$.

[3] Tramite la disuguaglianza triangolare.

6.1.5 Applicazione alle *quantum operations*

Le definizioni di norme invarianti unitarie che abbiamo dato fino a ora riguardano gli operatori lineari "quadrati", con gli spazi di partenza e di arrivo uguali. È possibile generalizzare tutto al caso di operatori lineari in $\mathsf{L}(\mathbb{C}^n, \mathbb{C}^m)$: anche per questi esiste la decomposizione a valori singolari e, poiché qualunque norma di operatori è definita univocamente in funzione dei valori singolari degli argomenti, esistono pure norme invarianti unitarie per operatori "rettangolari".

Abbiamo visto che una quantum operation $\mathrm{M} : \mathsf{L}(\mathsf{K}) \longrightarrow \mathsf{L}(\mathsf{H})$ è individuata univocamente dando un insieme di operatori $\{M_i\} \subset \mathsf{L}(\mathsf{H}, \mathsf{K})$ i quali determinano una decomposizione di Kraus per la mappa M. Che relazione esiste tra la "vicinanza" di operatori di Kraus e la "vicinanza" delle mappe che essi rappresentano? Vale il seguente:

Teorema 24 *Siano* $\mathrm{M}, \mathrm{N} : \mathsf{L}(\mathsf{K}) \longrightarrow \mathsf{L}(\mathsf{H})$ *due quantum operations. Se esistono due loro decomposizioni di Kraus (scelte in modo tale da avere la stessa cardinalità* [4]*)* $\mathrm{M} = \sum_{i=1}^{n} M_i^\dagger \cdot M_i$ *e* $\mathrm{N} = \sum_{i=1}^{n} N_i^\dagger \cdot N_i$ *tali che:*

$$|||M_j - N_j||| \longrightarrow 0 \quad \textit{per ogni } j, \tag{6.17}$$

per una qualche norma $|||\cdot|||$ *invariante unitaria, allora*

$$|||\mathrm{M}(X) - \mathrm{N}(X)||| \longrightarrow 0 \tag{6.18}$$

per ogni $X \in \mathsf{B}(\mathsf{K})$.

[4] Questo è *sempre* possibile.

Dim. Si ha:

$$
\begin{aligned}
|||\mathrm{M}(X) - \mathrm{N}(X)||| &= ||| \sum_{i=1}^{n} M_i^\dagger X M_i - \sum_{i=1}^{n} N_i^\dagger X N_i ||| = \\
&= ||| \sum_{i=1}^{n} M_i^\dagger X (M_i - N_i) - \sum_{i=1}^{n} (N_i^\dagger - M_i^\dagger) X N_i ||| \leq \\
&\leq ||| \sum_{i=1}^{n} M_i^\dagger X (M_i - N_i) ||| + ||| \sum_{i=1}^{n} (M_i^\dagger - N_i^\dagger) X N_i ||| \leq \\
&\leq \sum_{i=1}^{n} |||M_i^\dagger X|||\ |||M_i - N_i||| + \sum_{i=1}^{n} |||M_i^\dagger - N_i^\dagger|||\ |||X N_i|||
\end{aligned}
\tag{6.19}
$$

e, poiché $X, \{M_i\}$ e $\{N_i\}$ sono tutti operatori limitati, si ottiene la tesi.■

Per quanto riguarda l'enunciato opposto, cioè l'esistenza, per due mappe "vicine", di decomposizioni di Kraus "vicine", la questione è ancora aperta.

È noto che se due mappe sono vicine, in generale, le eventuali decomposizioni di Kraus vicine dovranno essere cercate non tra quelle canoniche, bensì tra quelle minimali o over-complete (tra quelle, cioè, ottenute da quelle canoniche tramite una combinazione lineare unitaria o isometrica). Questo fatto è strettamente analogo a ciò che succede per le matrici hermitiane. Prendiamo, ad esempio, le due matrici:

$$
A = \begin{pmatrix} 1+\varepsilon & 0 \\ 0 & 1-\varepsilon \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{pmatrix}. \tag{6.20}
$$

Queste sono chiaramente matrici hermitiane e, per $\varepsilon \to 0$, si ha $A \to B$ componente per componente e quindi $|||A - B||| \to 0$ per ogni norma $||| \cdot |||$ invariante unitaria. Inoltre gli autovalori di A e B sono i medesimi: $1+\varepsilon$ e $1-\varepsilon$. Tuttavia gli autospazi delle due matrici, per $\varepsilon > 0$, restano distinti: gli autovettori di A sono $(1,0)$ e $(0,1)$, mentre quelli di B sono $\frac{1}{\sqrt{2}}(1,1)$ e $\frac{1}{\sqrt{2}}(1,-1)$. Gli autospazi collassano improvvisamente per $\varepsilon = 0$ quando $A = B = I_2$.

Nell'esempio precedente si sono considerati solo gli autovettori che definiscono una diagonalizzazione (i.e. autovettori ortogonali e normalizzati). Interpretando A e B come stati (a meno di un fattore costante di normalizzazione), però, bisogna ancora considerare la libertà isometrica che esiste nel definire i possibili ensembles corrispondenti (nel caso di una mappa, le possibili decomposizioni di Kraus corrispondenti).

La risposta definitiva a questo problema non è ancora stata trovata.

6.2 Distinguibilità tra stati

6.2.1 *Trace distance*

Dalla 1-norma di Schatten (o norma-traccia) si definisce:

Definizione 14 *Dati due stati* $\rho, \sigma \in \mathsf{T}(\mathsf{H})$ *si definisce la loro* trace distance *come*

$$\mathrm{D}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1. \tag{6.21}$$

Poiché è originata da una norma, la trace distance soddisfa automaticamente tutte le proprietà di distanza:

1. $\mathrm{D}(\rho, \sigma) \geq 0$ per ogni $\rho, \sigma \in \mathsf{T}(\mathsf{H})$ ed è $\mathrm{D}(\rho, \sigma) = 0$ se e solo se $\rho = \sigma$;

2. $\mathrm{D}(\rho, \sigma) = \mathrm{D}(\sigma, \rho)$;

3. $\mathrm{D}(\rho, \sigma) \leq \mathrm{D}(\rho, \tau) + \mathrm{D}(\tau, \sigma)$ per ogni $\rho, \sigma, \tau \in \mathsf{T}(\mathsf{H})$.

Si verifica che $\mathrm{D}(\rho, \sigma) \leq 1$ con l'uguaglianza se e solo se ρ e σ hanno supporti ortogonali tra loro [5].

[5] E quindi è possibile discriminarli *senza* errore e con probabilità unitaria.

Si verifica pure che la trace distance è invariante per trasformazioni unitarie degli stati, nel senso che

$$\mathrm{D}(\rho,\sigma) = \mathrm{D}(U\rho U^\dagger, U\sigma U^\dagger) \tag{6.22}$$

per ogni operatore $U \in \mathsf{L}(\mathsf{H})$ unitario. Le mappe trace-preserving sono invece contrattive [1]:

Teorema 25 *Siano $\rho,\sigma \in \mathsf{T}(\mathsf{H})$ due stati qualunque e sia $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}),\mathsf{B}(\mathsf{H}),I)$ una mappa trace-preserving. Allora*

$$\mathrm{D}(\mathrm{M}^\tau(\rho),\mathrm{M}^\tau(\sigma)) \leq \mathrm{D}(\rho,\sigma). \tag{6.23}$$

Il senso fisico è chiaro: l'applicazione di una quantum operation *non può*, in alcun caso, migliorare la distinguibilità tra stati.

6.2.2 *Fidelity*

Dati due operatori densità $\rho,\sigma \in \mathsf{T}(\mathsf{H})$, la *fidelity* tra questi, definita come

$$\mathrm{F}(\rho,\sigma) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right)^2, \tag{6.24}$$

"quantifica" la possibilità di distinguere i due stati. Per comprendere la fisica che è contenuta nel concetto di fidelity, esiste il seguente [15]:

Teorema 26 (Uhlmann) *Dati due stati $\rho,\sigma \in \mathsf{T}(\mathsf{H})$, si ha che*

$$\mathrm{F}(\rho,\sigma) = \max_{|\psi\rangle,|\varphi\rangle} |\langle\psi|\varphi\rangle|^2 \tag{6.25}$$

dove il massimo è preso su tutte le purificazioni $|\psi\rangle \in \mathsf{H}\otimes\mathsf{H}$ di ρ e $|\varphi\rangle \in \mathsf{H}\otimes\mathsf{H}$ di σ.

Dal Teorema di Uhlmann discendono alcune proprietà della fidelity:

1. $0 \leq \mathrm{F}(\rho, \sigma) \leq 1$;

2. $\mathrm{F}(\rho, \sigma) = 1$ se e solo se $\rho = \sigma$;

3. $\mathrm{F}(\rho, \sigma) = 0$ se e solo se ρ e σ hanno supporti ortogonali;

4. $\mathrm{F}(\rho, \sigma) = \mathrm{F}(U\rho U^\dagger, U\sigma U^\dagger)$ per ogni operatore $U \in \mathsf{L}(\mathsf{H})$ unitario.

Analogamente al caso della trace distance vale il seguente [1]:

Teorema 27 *Siano $\rho, \sigma \in \mathsf{T}(\mathsf{H})$ due stati qualunque e sia $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), I)$ una mappa trace-preserving. Allora*

$$\mathrm{F}(\mathrm{M}^\tau(\rho), \mathrm{M}^\tau(\sigma)) \geq \mathrm{F}(\rho, \sigma). \tag{6.26}$$

È possibile dimostrare che le due nozioni di distinguibilità date dalla trace distance e dalla fidelity sono perfettamente equivalenti [6]: se due stati sono "vicini" o "lontani" nel senso della trace distance, sono "vicini" o "lontani" anche nel senso della fidelity. Valgono infatti le seguenti disuguaglianze [16]:

$$\begin{aligned} 1 - \sqrt{\mathrm{F}(\rho, \sigma)} \leq \mathrm{D}(\rho, \sigma) \leq \sqrt{1 - \mathrm{F}(\rho, \sigma)}, \\ (1 - \mathrm{D}(\rho, \sigma))^2 \leq \mathrm{F}(\rho, \sigma) \leq 1 - \mathrm{D}(\rho, \sigma)^2. \end{aligned} \tag{6.27}$$

6.3 Distinguibilità tra mappe

6.3.1 Norma di completa limitatezza

Partendo dalla trace distance tra stati, può sembrare naturale definire una distanza tra mappe (generiche, anche non quantum operations) tramite la relazione:

$$\mathrm{D}(\mathrm{M}, \mathrm{N}) = \sup_\rho \ \mathrm{D}(\mathrm{M}^\tau(\rho), \mathrm{N}^\tau(\rho)). \tag{6.28}$$

[6] Tuttavia la trace distance è una distanza mentre la fidelity no.

Questa nozione di distanza, tuttavia, non funziona del tutto, in quanto originata da una norma del tipo [7]:

$$\|\mathrm{M}\| = \sup_{\|\rho\|_1=1} \|\mathrm{M}^\tau(\rho)\|_1 \tag{6.32}$$

la quale non è stabile nei confronti del prodotto tensore. Infatti, presa una mappa T limitata, la norma $\|\mathrm{T} \otimes \mathrm{I}_n\|$ può crescere con n, anche se $\|T\|$ è ben definita [8].

Si introduce allora la *norma di completa limitatezza* (in inglese, *norm of complete boundedness* o *cb-norm*) definita come:

$$\|\mathrm{M}\|_{\mathrm{cb}} = \sup_n \|\mathrm{M} \otimes \mathrm{I}_n\| = \sup_n \sup_{\|\rho\|_1=1} \|(\mathrm{M} \otimes \mathrm{I}_n)^\tau(\rho)\|_1. \tag{6.33}$$

Per ogni $X \in \mathsf{T}(\mathsf{H})$ e per ogni M, N mappe generiche, si verificano le seguenti proprietà:

1. $\|\mathrm{M}^\tau(X)\|_1 \leq \|\mathrm{M}\|_{\mathrm{cb}} \|X\|_1$;

[7] Si è visto che, per operatori, si ha:

$$\begin{aligned} \|X\| = \|X\|_\infty &= \sup_{\|Y\|_1=1} |\operatorname{Tr}[Y^\dagger X]| \\ \|Y\|_1 &= \sup_{\|X\|=1} |\operatorname{Tr}[X^\dagger Y]|. \end{aligned} \tag{6.29}$$

Si definiscono allora le norme di mappe come:

$$\begin{aligned} \|\mathrm{M}\| &= \sup_{\|X\|=1} \|\mathrm{M}(X)\| = \sup_{\|Y\|_1=1} \sup_{\|X\|=1} |\operatorname{Tr}[Y^\dagger \mathrm{M}(X)]| \\ \|\mathrm{M}^\tau\|_1 &= \sup_{\|Y\|_1=1} \|\mathrm{M}^\tau(Y)\|_1 = \sup_{\|X\|=1} \sup_{\|Y\|_1=1} |\operatorname{Tr}[X^\dagger \mathrm{M}^\tau(Y)]|. \end{aligned} \tag{6.30}$$

Dalle ultime due equazioni si vede che:

$$\|\mathrm{M}\| = \|\mathrm{M}^\tau\|_1 \tag{6.31}$$

relazione che ci permette di usare indifferentemente, per indicare la norma di una mappa, l'una o l'altra scrittura.

[8] Come esempio si veda la mappa trasposizione $\Theta(X) = X^T$ in [17] e [18].

2. $\|\mathrm{M} \circ \mathrm{N}\|_{\mathrm{cb}} \leq \|\mathrm{M}\|_{\mathrm{cb}} \|\mathrm{N}\|_{\mathrm{cb}}$;

3. $\|\mathrm{M} \otimes \mathrm{N}\|_{\mathrm{cb}} = \|\mathrm{M}\|_{\mathrm{cb}} \|\mathrm{N}\|_{\mathrm{cb}}$.

Inoltre, dalla prima proprietà discende che per una quantum operation deve essere $\|\mathrm{M}\|_{\mathrm{cb}} \leq 1$ con l'uguaglianza se e solo se la mappa è trace-preserving.

Se due mappe sono vicine nel senso della cb-norm, gli stati di output che si ottengono sono vicini nel senso della trace distance:

$$\begin{aligned} \mathrm{D}(\mathrm{M}^{\tau}(\rho), \mathrm{N}^{\tau}(\rho)) &= \frac{1}{2}\|\mathrm{M}^{\tau}(\rho) - \mathrm{N}^{\tau}(\rho)\|_1 = \\ &= \frac{1}{2}\|(\mathrm{M}^{\tau} - \mathrm{N}^{\tau})(\rho)\|_1 \leq \\ &\leq \frac{1}{2}\|\mathrm{M} - \mathrm{N}\|_{\mathrm{cb}}; \end{aligned} \tag{6.34}$$

anche questo risultato discende dalla prima proprietà della cb-norm ricordando che per uno stato vale $\|\rho\|_1 = 1$.

6.3.2 *Fidelity* tra mappe

Nel Teorema(1) abbiamo visto come associare a una mappa $\mathrm{M} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ un operatore positivo $R_{\mathrm{M}} \in \mathsf{L}(\mathsf{K} \otimes \mathsf{H})$ tramite la relazione

$$R_{\mathrm{M}} = \mathrm{M}^{\tau} \otimes \mathrm{I}\ (|I\rangle\rangle\langle\langle I|). \tag{6.35}$$

Si è anche dimostrato che vi è corrispondenza biunivoca tra gli insiemi $\mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ e $\{R \in \mathsf{L}(\mathsf{K} \otimes \mathsf{H}) : \ R \geq 0,\ \mathrm{Tr}_1[R] = K\}$. Poiché per spazi di Hilbert finiti $0 < \mathrm{Tr}[K] < \infty$, abbiamo allora un'iniezione:

$$\begin{cases} \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K) \longrightarrow \{\text{stati in } \mathsf{T}(\mathsf{K} \otimes \mathsf{H})\} \\ \mathrm{M} \longmapsto \rho_{\mathrm{M}} = \dfrac{1}{\mathrm{Tr}[K]} R_{\mathrm{M}}. \end{cases} \tag{6.36}$$

È allora possibile definire una fidelity tra quantum operations semplicemente trasferendo alle mappe la definizione e le proprietà della fidelity tra stati [16]:

Definizione 15 *Date due mappe* $\mathrm{M}, \mathrm{N} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ *si definisce la* fidelity *tra queste tramite la relazione*

$$\mathrm{F}(\mathrm{M}, \mathrm{N}) = \mathrm{F}(\rho_{\mathrm{M}}, \rho_{\mathrm{N}}). \tag{6.37}$$

Chiaramente, tutte le proprietà di simmetria, positività, limitatezza, etc. valide per la fidelity tra stati valgono pure, senza alcuna modifica, per la fidelity tra mappe.

La fidelity tra stati è invariante per trasformazioni unitarie; trasferiamo questa proprietà alla fidelity tra mappe dicendo che quest'ultima è invariante per applicazioni successive di canali unitari, che definiamo essere quelle CP-maps trace-preserving del tipo $\mathrm{U} = U^{\dagger} \cdot U$ con U unitario:

Teorema 28 *La fidelity tra mappe è invariante per composizioni con canali unitari:*

$$\mathrm{F}(\mathrm{M}, \mathrm{N}) = \mathrm{F}(\mathrm{U} \circ \mathrm{M}, \mathrm{U} \circ \mathrm{N}). \tag{6.38}$$

Dim. Visto che $(\mathrm{U} \circ \mathrm{M}) \otimes \mathrm{I} = (\mathrm{U} \otimes \mathrm{I}) \circ (\mathrm{M} \otimes \mathrm{I})$, si ha che

$$\begin{aligned} \rho_{\mathrm{U}\circ\mathrm{M}} &= (U \otimes I)\rho_{\mathrm{M}}(U^{\dagger} \otimes I), \\ \rho_{\mathrm{U}\circ\mathrm{N}} &= (U \otimes I)\rho_{\mathrm{N}}(U^{\dagger} \otimes I); \end{aligned} \tag{6.39}$$

dall'invarianza della fidelity tra stati si ottiene allora l'invarianza della fidelity tra mappe.■

Sempre in analogia con il risultato per gli stati, esiste il seguente Teorema che afferma che nessuna operazione di *post-processing*, classica o quantistica, è in grado di aumentare la discriminabilità tra mappe:

Teorema 29 *La fidelity tra due mappe* $\mathrm{M}, \mathrm{N} \in \mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$ *non diminuisce per composizione con una quantum operation qualunque:*

$$\mathrm{F}(\mathrm{M}, \mathrm{N}) \leq \mathrm{F}(\mathrm{R} \circ \mathrm{M}, \mathrm{R} \circ \mathrm{N}) \tag{6.40}$$

per $\mathrm{R} \in \mathsf{CP}(\mathsf{B}(\mathsf{H}), \mathsf{B}(\mathsf{L}), K')$ *generica.*

Dim. Il procedimento ricalca quello seguito nella dimostrazione precedente; si utilizza, però, il Teorema(27).■

Concludendo, sottolineiamo il fatto che la fidelity tra mappe è stata definita solo tra due quantum operations appartenenti al medesimo insieme $\mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$. È possibile, infatti, che la fidelity tra due mappe con diverso operatore di normalizzazione K risulti comunque pari a 1. Se si vuole, quindi, che rimanga valida la proprietà per cui due quantum operations sono uguali se e solo se la loro fidelity è unitaria, è necessario ridursi al confronto solo all'interno di un unico insieme $\mathsf{CP}(\mathsf{B}(\mathsf{K}), \mathsf{B}(\mathsf{H}), K)$.

Conclusione

Principali risultati ottenuti

A partire dalle dilatazioni di Stinespring, si è data una dimostrazione costruttiva dell'esistenza di dilatazioni unitarie per quantum operations generiche. Utilizzando poi gli strumenti della teoria della maggiorizzazione, si è introdotta una classificazione per queste dilatazioni unitarie.

Si è pure affrontato il problema della caratterizzazione delle mappe estremali: basandosi sul Teorema di Choi, si sono definite le mappe ancillari associate a una mappa data e, tramite queste, si è riscritto il Teorema e la condizione necessaria e sufficiente per l'estremalità da esso fornita. È risultato che le mappe estremali sono tutte e sole quelle che possiedono mappe ancillari invertibili. Si è fornita un'interpretazione fisica.

Ultimo argomento trattato è stato quello relativo ai problemi che esistono nel definire una distanza soddisfacente tra quantum operations: si sono presentati i risultati in questo campo forniti dalla cb-norm e dalla fidelity tra mappe.

Prospettive di ricerca

Il risultato riguardante le dilatazioni unitarie per mappe completamente positive sembra poter essere esteso anche al caso di mappe completamente limitate. Si è inoltre considerata la possibilità di definire dilatazioni unitarie che conservino la potenza, cioè tali che la dilatazione della potenza k-esima di una mappa sia uguale alla potenza k-esima della dilatazione. Questo potrebbe portare a conseguenze teoriche interessanti.

Tra tutte le operazioni quantistiche, particolare importanza rivestono quelle bistocastiche e quelle *random*-unitarie: esistono diversi teoremi di caratterizzazione e di estremalità, ma nessuno fornisce un'interpretazione fisica chiara dei risultati matematici.

Nell'ambito della distanza tra mappe, rimane aperto il problema riguardante l'esistenza di decomposizioni di Kraus "vicine" per mappe "vicine". Si sono inoltre fatte ipotesi di generalizzazione del concetto di fidelity tra mappe nel caso di spazi di Hilbert di dimensione infinita.

Bibliografia

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

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

[3] G. M. D'Ariano, P. Lo Presti, `quant-ph/0101100`.

[4] J. I. Cirac, W. Dür, B. Kraus, M. Lewenstein, `quant-ph/0007057`.

[5] M. Ozawa, in *Quantum communications and measurement*, a cura di V. P. Belavkin, O. Hirota, R. L. Hudson, 109, (Plenum Press, 1955).

[6] P. R. Halmos, *A Hilbert space problem book*, (Springer-Verlag, seconda edizione, 1982).

[7] R. F. Werner, in *Quantum Information- an introduction to basic theoretical concepts and experiments*, Springer tracts in modern Physics **173**, (Springer-Verlag, 2000).

[8] W. F. Stinespring, *Positive functions on C^*-algebras*, Proc. Am. Math. Soc. **6**, 211-216, (1955).

[9] S. L. Campbell, C. D. Meyer Jr., *Generalized inverses of linear transformations*, (Dover, 1991).

[10] R. Bathia, *Matrix analysis*, (Springer-Verlag, 1997).

[11] M. A. Nielsen, *Probability distributions consistent with a mixed state*, Phys. Rev. A **62** 052308, (2000).

[12] P. G. Casazza, *The art of frame theory*, Taiwanese Journal of Math. **4** 2, 129-201, (2000).

[13] M. Marcus, H. Minc, *A survey of matrix theory and matrix inequalities*, (Dover, 1992).

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

[15] A. Uhlmann, Rep. Math. Phys. **9**, 273, (1976).

[16] M. Raginsky, *A fidelity measure for quantum channels*, Phys. Lett. A **290**, 11, (2001).

[17] V. I. Paulsen, *Completely bounded maps and dilations*, (Longman scientific and technical, 1986).

[18] D. Aharonov, A. Kitaev, N. Nisan, `quant-ph/9806029`.