Indice

Introduzione

L'esistenza del quanto d'azione di Planck introduce in fisica classica una situazione completamente nuova dal punto di vista della descrizione del processo di misura: ogni interazione tra sistema atomico osservato e strumento di misura non è più riducibile ad una registrazione, da parte dello strumento, del valore della grandezza misurata sul sistema, ma comporta una importante modifica anche del sistema stesso, che non è eliminabile né praticamente, né concettualmente. L'interazione puó anche essere uguale a zero, ma in tal caso non si compie alcuna osservazione e non si acquisisce alcuna conoscenza sulle proprietà del sistema atomico. Se l'interazione è invece diversa da zero, essa non può essere resa arbitrariamente piccola e non è quindi neppure concettualmente eliminabile, come avveniva in fisica classica. Questo carattere perturbativo della misurazione comporta la necessità dell'abbandono dello schema classico della doppia registrazione da parte dell'apparato prima e dell'osservatore poi, a favore di un nuovo schema che indichi esplicitamente la natura simmetrica e non più unidirezionale del processo di interazione tra apparato misuratore e sistema atomico misurato.

Nella formulazione standard della meccanica quantistica, le grandezze fisiche osservabili sono rappresentate da operatori autoaggiunti nello spazio di Hilbert descrivente il sistema. La distribuzione di probabilità del risultato di una misura è data dalla regola di Born e lo stato del sistema dopo la misura (lo stato ridotto) deriva dalle proprietà spettrali degli operatori autoaggiunti, tramite una proiezione. Questa formulazione, però, si rivela inadeguata nell'ambito di alcuni tipi di misure, come quelle approssimate (misura di osservabili a spettro continuo), le misure congiunte di osservabili non compatibili (per le quali non è applicabile la proiezione per lo stato ridotto) e per la stima di parametri non associati ad alcuna osservabile. Tali problemi sono risolti tramite la definizione di POVM (Positive Operator-Valued Measures) e "strumento".

Esponiamo nel primo capitolo i preliminari della teoria quantistica della misurazione, fornendo peraltro i mezzi necessari alla comprensione di tutto il lavoro. Dopo aver enunciato i quattro postulati della meccanica quantistica, focalizziamo la nostra attenzione sul terzo, che fornisce una descrizione degli effetti della misurazione quantistica su un sistema tramite le misure generalizzate. Sono quindi introdotte le nozioni di POVM e "strumento", che forniscono rispettivamente la distribuzione di probabilità e la riduzione di stato di una misura. La POVM generalizza la misura a valori proiettivi associata alle osservabili. I proiettori sono sostituiti da operatori positivi in generale non ortogonali, i quali risolvono l'identità e forniscono distribuzioni di probabilità normalizzate. Il capitolo si chiude con la definizione di "strumento" e di POVM associata.

Nel secondo capitolo risulta chiaro il titolo di questo lavoro: la misurazione quantistica è estrinsecamente (*i.e.* in modo eliminabile) affetta da rumore, nel senso che suddetto rumore è originato dalla scelta a caso tra apparati diversi nell'ambito del processo di misura. Il nostro intento non è altro che eliminare questo rumore estrinseco e caratterizzare quelle POVMs che sono soggette al solo rumore intrinseco, indissolubile dal formalismo della teoria quantistica. Dimostriamo, all'inizio del capitolo, che l'insieme delle POVMs risulta convesso, che cioè una combinazione lineare convessa di due POVMs è ancora una POVM. Formalizziamo quindi il problema del rumore notando che scrivere una POVM $\mathbf{\Pi}$ come $\sum_i p_i \mathbf{\Pi}^{(i)}$, con $p_i \geq 0$ e $\sum_i p_i = 1$, ha un significato fisico chiaro: $\mathbf{\Pi}$ descrive un composito apparato di misura in cui ogni singolo apparato $\mathbf{\Pi}^{(i)}$ è selezionato a caso e dove p_i è la probabilità dell'i-esimo apparato. È proprio questa randomizzazione degli apparati che genera rumore: cerchiamo dunque di identificare le POVMs che non posso-

no essere scritte come combinazione lineare convessa di altre POVMs, quelle *estremali.*
Sono proposte innanzitutto due condizioni necessarie per l'estremalità delle POVMs e a seguire due esempi che negano le implicazioni inverse.
Viene quindi enunciata la condizione necessaria e sufficiente per l'estremalità delle POVMs: questo risultato è presentato, in un primo momento, applicato a POVMs con elementi di rango 1 e poi generalizzato a rango generico. Per quanto riguarda il caso a rango 1 si è eseguita una dimostrazione costruttiva mentre per la sua generalizzazione vengono proposte due diverse dimostrazioni. La prima dimostrazione trovata risulta originale e particolarmente agile, derivando da una semplice manipolazione della definizione di POVM non estremale; la seconda, invece, è basata su una rivisitazione del teorema di Choi per l'estremalità delle mappe completamente positive, adattato a delle mappe $\Phi(f)$ da noi definite affinchè sussistesse una corrispondenza biunivoca tra l'insieme di tali mappe e quello delle POVMs.

Nel terzo capitolo viene introdotta una nuova interpretazione del concetto di osservabile. Dopo una breve introduzione al problema agli autovalori, limitiamo la nostra analisi agli autovettori che vivono in uno spazio di Hilbert. Fissato quindi il significato di osservabile in relazione alle misurazioni proiettive, ne forniamo una sorta di generalizzazione tramite le misure generalizzate del terzo postulato, e quindi delle POVMs. Notato che le POVMs commutanti sono una generalizzazione banale della risoluzione ortonormale tramite randomizzazione dei risultati della misura, fissiamo la decomposizione a valori singolari delle misure generalizzate associate a tali POVM, e definiamo dunque la nostra osservabile in funzione delle misure generalizzate.

Nel quarto capitolo vengono riportati i tratti fondamentali della *teoria della maggiorizzazione.* Questa teoria ha la sua principale motivazione nella definizione di cosa si intende per una distribuzione di probabilità più disordinata di un'altra. Nel capitolo si pone particolare attenzione al legame della maggiorizzazione col concetto di entropia e quindi di disordine, nonchè alle relazioni tra i vettori degli autovalori di due matrici. Sono enunciati solo i teoremi principali, enfatizzando le connessioni tra maggiorizzazione e meccanica quantistica.

Nel quinto capitolo viene descritta la *teoria dei frames.* I frames sono una generalizzazione delle basi: un frame per uno spazio di Hilbert $\mathcal{H}$ è un insieme di vettori, non necessariamente linearmente indipendenti, che spannano $\mathcal{H}$ e godono di altre proprietà presentate nel capitolo. Essi furono per la prima volta introdotti da Duffin e Schaeffer nel contesto delle serie di Fourier non armoniche, e, a causa delle condizioni meno stringenti cui devono obbedire, rispetto alle basi, i frames sono diventati fondamentali per lo sviluppo delle moderne tecniche di *sampling* e per diversi problemi di *detection.* Nella prima parte di questo capitolo ci occupiamo però solo la teoria astratta dei frames, tramite le definizioni e la presentazione dei teoremi principali, con particolare enfasi alla loro interpretazione come operatori.
Nella seconda parte trattiamo una interessante connessione tra la meccanica quantistica e i frames: mostriamo infatti che la famiglia dei *tight* frames (caso particolare di frames per cui la formula di ricostruzione risulta particolarmente semplice) normalizzati per lo spazio in cui giace un sistema quantistico coincide con quella delle POVMs con elementi di rango 1, definiti su tale spazio. Questa fondamentale equivalenza permette di applicare idee e risultati della misurazione quantistica alla teoria dei frames, e viceversa. Dopo aver definito le matrici di misurazione associate alla POVM e ripreso il teorema di Neumark adattato a queste matrici, si illustra brevemente il problema di costruire misurazioni ottimizzate per distinguere stati puri non ortogonali. Nell'ultima parte, quindi, si trasportano i precedenti risultati della teoria della misurazione quantistica ai frames, tramite la definizione delle matrici di frame associate ai tight frames, la derivazione di un analogo di Neumark per i frames, e la presentazione dell'idea di base per una costruzione di tight frames ottimali per un sottospazio $\mathcal{U}$ dato un insieme di vettori che spannano $\mathcal{U}$.

Capitolo 1

Teoria quantistica della misurazione

In questo primo capitolo vengono forniti i preliminari di teoria quantistica della misurazione. Si presentano innanzitutto i quattro postulati della meccanica quantistica, con particolare attenzione al terzo postulato dove viene definito il processo di misurazione quantistica tramite le misure generalizzate. Si dimostra quindi l'equivalenza di queste misure con quelle proiettive, caratterizzate dalla ripetibilità. Si defiscono poi la POVM (Positive Operator-Valued Measures) e lo "strumento" della misura, atti a dare una descrizione matematica rispettivamente della riduzione e della distribuzione di probabilità, elementi costituenti la statistica della misura sperimentata da un osservatore che applica la meccanica quantistica al sistema oggetto. Per quanto riguarda le POVMs si presentano anche casi in cui il loro utilizzo si rivela particolarmente utile, ad esempio nelle misurazioni non ideali per la risoluzione sperimentale o nella dimostrazione di teoremi generali di *quantum estimation*. Il capitolo si conclude con la definizione di "strumento" e un esempio di strumento e relativa POVM ad esso associata.

1.1 I postulati della meccanica quantistica

Introduciamo i seguenti preliminari di *teoria quantistica della misurazione* elencando i postulati della meccanica quantistica (per una completa descrizione dei postulati si veda la Sez. 2.2 di [1]).

Postulato 1

Ad ogni sistema fisico isolato è associato uno spazio vettoriale complesso in cui sia definito un prodotto interno (uno spazio di Hilbert $\mathcal{H}$) chiamato *spazio degli stati* del sistema. Lo stato del sistema è completamente descritto da un vettore normalizzabile $|\psi\rangle \in \mathcal{H}$ detto *vettore di stato.*

Postulato 2

L'evoluzione di un sistema quantistico chiuso è descritta da una trasformazione unitaria: lo stato del sistema a un tempo t_1 è infatti legato allo stato dello stesso sistema $|\psi^{'}\rangle$ al tempo t_2 da un operatore unitario U, che dipende soltanto dalla differenza tra i due tempi $t_2 - t_1$, in tal modo

$$|\psi^{'}\rangle = U|\psi\rangle$$

Postulato 3

Le misurazioni quantistiche pure sono descritte da un insieme $\{M_m\}$ di operatori, detti *operatori di misura*, che agiscono nello spazio degli stati $\mathcal{H}$ del sistema che stiamo misurando [1]. L'indice m è riferito al risultato della misura dell'esperimento in questione, tra gli esiti possibili della misurazione. Se lo stato del sistema quantistico appena prima della misura è $|\psi\rangle$, allora la probabilità che si verifichi il risultato m è data dalla Born rule:

$$p(m) = \langle\psi|M_m^{\dagger}M_m|\psi\rangle = \mathrm{Tr}(M_m^{\dagger}M_m|\psi\rangle\langle\psi|) \tag{1.1}$$

e lo stato del sistema dopo la misurazione è

$$|\psi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}. \tag{1.2}$$

L'operatore di misura soddisfa la relazione di completezza

$$\sum_m M_m^{\dagger}M_m = \mathbb{I} \tag{1.3}$$

[1]Un operatore M è un operatore di misura se e solo se è una contrazione *i.e.* $\|M\| \leq 1$

che permette alle probabilità di sommarsi ad uno

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

Postulato 4

Lo spazio degli stati $\mathcal{H}$ di un sistema fisico composto, i cui sistemi componenti hanno spazi degli stati $\mathcal{H}_1, \ldots, \mathcal{H}_n$, è dato dal prodotto tensore

$$\mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_n.$$

Se l'i-esimo sistema è descritto dallo stato $|\psi_i\rangle$, allora lo stato congiunto del sistema totale è

$$|\psi\rangle = |\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle.$$

1.2 Misurazioni quantistiche e POVMs

Lo schema di misurazione più generale permesso dalla meccanica quantistica è quindi descritto dal terzo postulato [1]. Un caso particolare del postulato delle misure generalizzate è quello delle misure proiettive, o di Von Neumann: misure ripetibili corrispondenti ai proiettori ortogonali M_m, *i.e.* operatori hermitiani tali che $M_m M_n = \delta_{m,n} M_m$. Una misura di Von Neumann è descritta da un operatore hermitiano M nello spazio degli stati $\mathcal{H}$ del sistema con una decomposizione spettrale $M = \sum_m m P_m$, dove P_m è il proiettore sull'autospazio di M con autovalore m. I possibili risultati della misura corrispondono agli autovalori m dell'osservabile M, ottenuti con probabilità

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

e la riduzione di stato è

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

Per dimostrare che le misure generalizzate possono essere ricondotte a quelle proiettive, usiamo un sistema quantistico composto, con uno schema di misura indiretta. Consideriamo il sistema quantistico descritto dallo spazio di

Hilbert $\mathcal{H}$ e un sistema d'*ancilla* con spazio degli stati $\mathcal{K}$, avente una base in corrispondenza biunivoca con i possibili risultati della misura. Preso uno stato fissato $|0\rangle \in \mathcal{K}$, consideriamo un operatore lineare $U \in \mathcal{L}(\mathcal{H} \otimes \mathcal{K})$ che, su stati della forma $|\psi\rangle \otimes |0\rangle$, $\forall |\psi\rangle \in \mathcal{H}$, agisca come segue

$$U|\psi\rangle \otimes |0\rangle = \sum_m M_m|\psi\rangle \otimes |m\rangle,$$

dove $\{|m\rangle\}$ è un insieme ortonormale $\in \mathcal{K}$. L'operatore U, la cui esistenza è assicurata dalla precedente relazione che lo definisce, è isometrico nel sottospazio $\mathcal{H}' = \mathsf{span}\{|\psi\rangle \otimes |0\rangle, |\psi\rangle \in \mathcal{H}\} \simeq \mathcal{H}$, infatti

$$\langle\varphi|\langle 0|U^\dagger U|\psi\rangle|0\rangle = \sum_{l,l'} \langle\varphi|M_l^\dagger M_{l'}|\psi\rangle\langle l|l'\rangle = \sum_l \langle\varphi|M_l^\dagger M_{l'}|\psi\rangle = \langle\varphi|\psi\rangle.$$

Tramite la procedura di Gram-Schmidt, possiamo estendere U ad un operatore unitario nello spazio totale $\mathcal{H}\otimes\mathcal{K}$. U descrive l'interazione sistema-ancilla; una volta finita tale interazione facciamo una misura proiettiva descritta dalla risoluzione ortonormale su $\mathcal{H} \otimes \mathcal{K}$

$$P_l = \mathbb{I} \otimes |l\rangle\langle l|,$$

i.e. una misura solo sull'ancilla. Supponiamo ora che la misura sia effettuata sul sistema totale preparato nello stato congiunto $U|\psi\rangle \otimes |0\rangle$, il risultato l si verifica con probabilità

$$p(l) = \langle\psi|\langle 0|U^\dagger P_l U|\psi\rangle|0\rangle = \sum_{m,m'} \langle\varphi|M_m^\dagger M_{m'}|\psi\rangle\langle m|P_l|m'\rangle = \langle\psi|M_l^\dagger M_l|\psi\rangle,$$

i.e. la Born rule (1.1). Lo stato congiunto del sistema totale dopo la misura è dato da

$$\frac{P_l U|\psi\rangle \otimes |0\rangle}{\sqrt{\langle\psi|U^\dagger P_l U|\psi\rangle}} = \frac{M_l|\psi\rangle \otimes |l\rangle}{\|M_l|\psi\rangle\|},$$

e segue che lo stato dell'ancilla dopo la misura è $|l\rangle$, mentre quello del sistema è

$$\frac{M_l|\psi\rangle}{\|M_l|\psi\rangle\|},$$

ovvero la riduzione di stato (1.2). Dunque le misure proiettive e generalizzate sono equivalenti, entrambe si riferiscono alla stessa distribuzione di probabilità e riduzione di stato. La caratteristica saliente delle misurazioni von Neumann è la ripetibilità. Se infatti eseguiamo una misura nello stato inziale $|\psi\rangle$, ottenendo l'autovalore m e quindi lo stato

$$|\psi_m\rangle = \frac{P_m|\psi\rangle}{\sqrt{\langle\psi|P_m|\psi\rangle}}$$

e applichiamo l'operatore P_m a $|\psi_m\rangle$, troviamo nuovamente il risultato m con probabilità $\langle\psi|P_m|\psi\rangle = 1$ e senza variazioni di stato.

Quando lo stato dopo la misurazione non è rilevante, e ciò che conta è solo la distribuzione statistica dei risultati, la misurazione può essere descritta mediante le POVMs[2], che mappano uno stato quantistico ρ in una distribuzione di probabilità [1] [2].
Una POVM è un insieme $\mathbf{\Pi}$ di operatori Π_m tali che:

- ogni operatore Π_m è positivo
- è verificata $\forall\, \Pi_m$ la relazione di completezza $\sum_m \Pi_m = \mathbb{I}$, che garantisce che la somma delle probabilità sia uguale ad uno.

La probabilità del risultato m è $p(m) = \langle\psi|\Pi_m|\psi\rangle$, essa diventa il risultato generale (1.1) definendo gli elementi della POVM come segue:

$$\Pi_m \equiv M_m^\dagger M_m \tag{1.4}$$

e quindi $M_m = U_m\sqrt{\Pi_m}$, dove $\{U_m\}$ è una qualsiasi famiglia di operatori unitari. Secondo la precedente estensione, le POVMs possono essere collegate alle misure proiettive. Infatti una risoluzione ortogonale $\{P_l\}$ in uno spazio di Hilbert esteso $\mathcal{H}\otimes\mathcal{K}$ in generale corrisponde ad una POVM non ortogonale $\mathbf{\Pi}$ nello spazio $\mathcal{H}$ del sistema con una preparazione in uno stato fissato, sia $|0\rangle$, dell'ancilla, ovvero $\Pi_l = \langle 0|P_l|0\rangle$. Il *teorema di Neumark* [3] descrive

[2] L'acronimo POVM sta per Positive Operators-Valued Measure (misura a valori negli operatori positivi).

la relazione inversa: $\forall$ POVM con elementi $\Pi_l \in \mathcal{L}(\mathcal{H})$, $\exists$ una risoluzione ortonormale P_l in uno spazio di Hilbert esteso $\mathcal{H} \otimes \mathcal{K}$ con una preparazione pura $|0\rangle \in \mathcal{K}$ dell'ancilla. Senza dimostrare il teorema, forniamo qui di seguito una delle possibili estensioni di Neumark, cioè

$$P_k = U^\dagger \mathbb{I} \otimes |k\rangle\langle k| U,$$

dove $\{|k\rangle\}$ è una risoluzione ortogonale in $\mathcal{K}$ e U è una delle infinite estensioni unitarie dell'operatore lineare che agisce come segue:

$$U|\psi\rangle \otimes |0\rangle = \sum_k V_k \sqrt{\Pi_k} |\psi\rangle \otimes |k\rangle$$

dove $\{V_k\}$ è una qualsiasi famiglia di operatori unitari. Esistono comunque altre estensioni di Neumark diverse da quella qui presentata, che estendono anche l'intero schema di misura, *i.e.* inclusa la riduzione di stato, e non solo la POVM. Il teorema di Neumark qui enunciato si riferisce ad osservabili con spettro discreto. Una sua generalizzazione che comprende anche osservabili con spettro continuo è stata ottenuta da Ozawa [4]. Concludiamo quindi che i vari schemi di misura, espressi con un'opportuno formalismo e adeguate estensioni, sono tra loro equivalenti.

Ci sono comunque casi in cui le POVMs si rivelano uno strumento particolarmente utile. Ad esempio nelle misurazioni non ideali per la risoluzione sperimentale: nella misura del numero dei fotoni di un modo di radiazione ν [5]. Idealmente si ha l'osservabile:

$$N = \sum_{n=1}^{\infty} n |n\rangle\langle n|$$

ma per esprimere correttamente la situazione ideale bisogna utilizzare la POVM:

$$\Pi_\eta(n) = \sum_{k=n}^{\infty} \binom{k}{n} \eta^n (1-\eta)^{k-n} |k\rangle\langle k|$$

dove η è un parametro complesso reale compreso tra 0 e 1, detto efficienza quantica del rivelatore. Questa POVM può essere vista come il prodotto di

una misura effettuata con un rivelatore ideale preceduto da un *beam splitter* di trasmissività η, che fa interagire il modo della radiazione in esame con un altro modo preparato in uno stato di vuoto.
Un altro esempio di POVM è l'*heterodyne detector* ideale [5], che fornisce la misurazione ideale di quadrature coniugate[3]. In questo tipo di misurazioni la POVM del *detector* ideale è della forma:

$$d\Pi(z,\bar{z}) = \int \frac{d^2z}{\pi^2} e^{\bar{\lambda}z-\lambda\bar{z}} : D_s(\lambda) :_A d^2z \tag{1.5}$$

dove il simbolo $: \cdot :_A$ denota l'ordine antinormale e $D_s(\lambda)$ è l'operatore di spostamento

$$D_s(\lambda) = \exp{(\lambda a^\dagger - \bar{\lambda}a)}. \tag{1.6}$$

Introducendo gli stati coerenti $|z\rangle = D_s(z)|0\rangle$, la (1.5) diventa:

$$d\Pi(z,\bar{z}) = \frac{d^2z}{\pi^2}|z\rangle\langle z|, \tag{1.7}$$

per cui la POVM ideale per l'*heterodyne detector* è il proiettore sugli stati coerenti.
L'utilizzo più rilevante delle POVMs è nella dimostrazione di teoremi generali di *quantum estimation*. Uno di questi è il teorema sull'impossibilità di distinguere con certezza stati tra loro non ortogonali. Mentre è sempre possibile, almeno in linea di principio, distinguere stati diversi di un oggetto, in meccanica quantistica ciò può essere fatto solo se gli stati sono ortogonali. Per dimostrare questa caratteristica dei sistemi quantistici introduciamo uno *scenario* a cui si ricorre spesso in quantum computation e in quantum

[3]La quadratura X e la sua coniugata Y rappresentano l'equivalente ottico della posizione e del momento di un oscillatore armonico e sono definite come:

$$X = \frac{1}{2}[a + a^\dagger], \qquad Y = \frac{i}{2}[a^\dagger - a];$$

esse soddisfano la relazione di commutazione

$$[X, Y] = i/2$$

information. Prendiamo due sistemi, chiamiamoli A (Alice) e B (Bob); essi comunicano tra di loro scambiandosi un "oggetto" quantistico, come una particella o un modo della radiazione a una certa frequenza e polarizzazione. Il sistema scambiato è in uno stato $|\psi_l\rangle$ scelto tra un insieme di stati fissati, labellati con un indice $l = 1, \ldots, N$ e noti sia ad Alice che a Bob. Alice spedisce lo stato $|\psi_l\rangle$ a Bob che deve poi identificare l'indice l dello stato ricevuto. Se gli stati sono ortogonali Bob può discriminarli con certezza utilizzando la POVM ortonormale $\{P_l\}$, con $P_l = |\psi_l\rangle\langle\psi_l|$. Infatti la probabilità associata ad ogni elemento di questa POVM è:

$$p(j|l) = \langle\psi_l|P_j|\psi_l\rangle = \delta_{jl}$$

e quindi se si ottiene il risultato l, Bob può essere sicuro di aver ricevuto lo stato $|\psi_l\rangle$. Se invece gli stati sono non ortogonali, non è possibile costruire una misura quantistica che possa discriminarli. Supponiamo che gli stati possibili siano due, allora ciascuno di essi può essere decomposto in una parte parallela e una perpendicolare all'altro; se si trova l'indice 1 come risultato della misura non è possibile sapere se è stato osservato lo stato $|\psi_1\rangle$ o la componente di $|\psi_2\rangle$ parallela a $|\psi_1\rangle$, analogamente per l'indice 2. Per trattare la questione in un modo più rigoroso, costruiamo una POVM con due elementi $\{\Pi_1, \Pi_2\}$ in corrispondenza biunivoca con gli eventi:

- evento 1: trasmissione dello stato $|\psi_1\rangle$
- evento 2: trasmissione dello stato $|\psi_2\rangle$.

In una discrimanazione perfetta tra gli stati si deve ottenere:

$$\langle\psi_1|\Pi_1|\psi_1\rangle = \langle\psi_2|\Pi_2|\psi_2\rangle = 1. \tag{1.8}$$

Poichè per completezza $\Pi_1 + \Pi_2 = \mathbb{I}$, si ha:

$$\langle\psi_1|\Pi_1 + \Pi_2|\psi_1\rangle = 1$$

e perciò, dato che $\langle\psi_1|\Pi_1|\psi_1\rangle = 1$, deve essre $\langle\psi_1|\Pi_2|\psi_1\rangle = 0$, da cui segue $\sqrt{\Pi_2}|\psi_1\rangle = 0$. Se ora decomponiamo $|\psi_2\rangle$ in termini di $|\psi_1\rangle$ e di un vettore

$|\varphi\rangle$ ortonormale a $|\psi_1\rangle$ otteniamo $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$, con $|\beta| < 1$ perchè $|\psi_1\rangle$ e $|\psi_2\rangle$ non sono ortogonali. Dallo sviluppo di $|\psi_2\rangle$ segue

$$\sqrt{\Pi_2}|\psi_2\rangle = \alpha\sqrt{\Pi_2}|\psi_1\rangle + \beta\sqrt{\Pi_2}|\varphi\rangle = \beta\sqrt{\Pi_2}|\varphi\rangle$$

e quindi $\langle\psi_2|\Pi_2|\psi_2\rangle = |\beta|^2\langle\varphi|\Pi_2|\varphi\rangle$. Poichè

$$\langle\varphi|\Pi_2|\varphi\rangle \leq \langle\varphi|\Pi_1 + \Pi_2|\varphi\rangle = \langle\varphi|\mathbb{I}|\varphi\rangle = \langle\varphi|\varphi\rangle = 1,$$

risulta $\langle\psi_2|\Pi_2|\psi_2\rangle \leq |\beta|^2 < 1$ in contraddizione con la (1.8), per cui non si può avere una discriminazione perfetta tra gli stati non ortogonali.
È possibile però costruire una POVM che in certi casi distingua stati non ortogonali se si ammette che essa possa dare risultati inconclusivi. Consideriamo infatti i due stati $|\psi_1\rangle = |0\rangle$ e $|\psi_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e la POVM:

- $\Pi_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|$
- $\Pi_2 = \frac{\sqrt{2}}{1+\sqrt{2}}\frac{(|0\rangle+|1\rangle)(\langle 0|-\langle 1|)}{2}$
- $\Pi_3 = \mathbb{I} - \Pi_1 - \Pi - 2$

Si può facilmente verificare che $\Pi_l \geq 0$ e $\sum_l \Pi_l = \mathbb{I}$, perciò i tre operatori costituiscono una POVM. Supponiamo ora che Bob abbia ricevuto lo stato $|\psi_1\rangle = 0$ e che esegua le misure descritte dalla POVM $\mathbf{\Pi} = (\Pi_1, \Pi_2, \Pi_3)$. Si ha:

- $\langle\psi_1|\Pi_1|\psi_1\rangle = 0$, cioè una probabilità uguale a zero di osservare il risultato Π_1. Quindi se dovesse trovare Π_1, potrebbe concludere di aver ricevuto lo stato $|\psi_2\rangle$.
- $\langle\psi_1|\Pi_1|\psi_1\rangle \geq 0$ e $\langle\psi_2|\Pi_2|\psi_2\rangle = 0$, cioè una probabilità diversa da zero di osservare Π_2 avendo ricevuto $|\psi_1\rangle$ e nulla se Alice gli ha inviato $|\psi_2\rangle$, per cui se osserva Π_2 può concludere di aver ricevuto $|\psi_1\rangle$.
- $\langle\psi_1|\Pi_3|\psi_1\rangle = \langle\psi_2|\Pi_3|\psi_2\rangle = \frac{1}{\sqrt{2}}$, che non gli fornisce nessuna informazione sull'identità dello stato ricevuto.

In nessun caso Bob commette errori nell'identificare lo stato, ma questa infallibilità comporta che a volte la misura non gli fornisca nessuna informazione. L'impossibilità di discriminare con esattezza tra stati non ortogonali è legata all'impossibilità di clonare stati quantistici stabilita dal *no-cloning theorem*, ed entrambe sono conseguenza dell'unitarietà della meccanica quantistica. Il teorema del *no-cloning* [1] stabilisce che non è possibile costruire un congegno che produca copie di stati quantistici non ortogonali, mentre non proibisce di copiare stati ortogonali. Supponiamo infatti di poter costruire un dispositivo quantistico in grado di clonare lo stato puro non noto $|\psi\rangle$, tramite uno stato ancillare $|s\rangle$, che verrà trasformato in una copia perfetta di $|\psi\rangle$. Inizialmente si ha lo stato $|E\rangle \otimes |\psi\rangle \otimes |s\rangle$, dove $|E\rangle$ rappresenta lo stato normalizzato che descrive l'ambiente esterno al sistema, in modo tale che esso possa essere considerato isolato. Descrivendo l'azione del dispositivo di *cloning* tramite un operatore unitario U, lo stato globale si trasforma nel seguente modo:

$$|E\rangle \otimes |\psi\rangle \otimes |s\rangle \longmapsto U(|E\rangle \otimes |\psi\rangle \otimes |s\rangle) = |E\rangle \otimes |\psi\rangle \otimes |\psi\rangle$$

Se cerchiamo di clonare due stati puri $|\psi\rangle$ e $|\varphi\rangle$, otteniamo:

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

$$U(|E\rangle \otimes |\varphi\rangle \otimes |s\rangle) = |E\rangle \otimes |\varphi\rangle \otimes |\varphi\rangle).$$

Se ora prendiamo il prodotto scalare delle due equazioni precedenti, si vede che deve essere verificata la relazione:

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2 \tag{1.9}$$

quindi il prodotto scalare tra i due stati deve essere uguale a zero o a uno, cioè $|\psi\rangle$ o $|\varphi\rangle$ devono essere ortogonali oppure coincidenti. Si può quindi concludere che non è possibile costruire un dispositivo quantistico generale che cloni stati quantistici generici. Se questo fosse possibile, la relazione (1.9) non sarebbe verificata e quindi l'evoluzione descritta da U non sarebbe unitaria. Il legame tra il teorema di *no-discriminating* e quello di *no-cloning* è dovuto al fatto che, se si potesse discriminare tra stati quantistici, si potrebbe conoscere esattamente lo stato di un singolo sistema quantistico e quindi, tramite la preparazione, produrne copie perfette. Se invece fosse possibile clonare uno stato non noto, si potrebbe produrre una grande quantità di copie da utilizzare per eseguire misure con precisione arbitraria, avendo sempre a disposizione una copia perfetta del sistema originale su cui eseguire ulteriori misurazioni. I due teoremi sono stati dimostrati separatamente, ma alla base di entrambi c'è l'unitarietà della meccanica quantistica. Permettere il cloning di stati non ortogonali o la loro perfetta discriminazione comporta la rinuncia alla richiesta che l'evoluzione di un sistema quantistico chiuso sia descritta da un operatore unitario.

1.3 POVM e strumento

Fino ad ora abbiamo fatto una descrizione delle misure in cui i possibili risultati sono eventi che si escludono a vicenda (l'indice dell'operatore di misura appartiene ad un insieme numerabile di valori) e, inoltre, si trattava di misure pure, *i.e.* la riduzione di stato lascia stati puri in stati puri. Questo schema venne esteso da Ozawa [4], come generalizzazione della descrizione precedente tramite le proprietà topologiche dell'insieme degli eventi e dello spazio delle probabilità. Gli stati quantistici formano un insieme convesso, con una struttura simile a quella dello spazio delle probabilità. Quindi usando uno schema di misura in una combinazione lineare convessa di stati, si ottiene una combinazione lineare convessa di statistiche corrispondenti ad ogni stato. Se consideriamo lo stato corrispondente all'unione di due eventi disgiunti (*i.e.* due stati possibili risultati di una misura) dobbiamo prendere la combinazione convessa degli stati di ogni evento. Segue che:

$$\rho_{(a\cup b)} = \frac{p_a}{p_{(a\cup b)}}\rho_a + \frac{p_b}{p_{(a\cup b)}}\rho_b \tag{1.10}$$

dove $\frac{p_a}{p_{(a\cup b)}}$ è la frazione degli eventi in cui il risultato a si verifica, e analogamente $\frac{p_b}{p_{(a\cup b)}}$, mentre ρ_a e ρ_b sono gli stati condizionati dagli eventi a e b rispettivamente. Definendo ora M_a e M_b come le contrazioni corrispondenti agli eventi a e b, si ottiene:

$$p_a = \mathrm{Tr}(M_a^\dagger M_a \rho), \quad p_b = \mathrm{Tr}(M_b^\dagger M_b \rho), \quad p_{(a\cup b)} = \mathrm{Tr}[(M_a^\dagger M_a + M_b^\dagger M_b)\rho]$$

e l'equazione (1.10) diventa

$$\rho_{(a\cup b)} = \frac{M_a \rho M_a^\dagger + M_b \rho M_b^\dagger}{\mathrm{Tr}(M_a \rho M_a^\dagger + M_b \rho M_b^\dagger)}$$

che può essere generalizzata come segue:

$$\rho_{(a\cup b)} = \frac{\mathcal{I}_{(a\cup b)}(\rho)}{\mathrm{Tr}[\mathcal{I}_{(a\cup b)}(\rho)]} .$$

La mappa $\mathcal{I}$, definita su tutti i possibili eventi Δ in uno spazio delle probabilità Ω che supporta una $\sigma - algebra$, ha le seguenti proprietà:

- $\mathcal{I}_\Delta(\rho) \geq 0 \qquad \forall \rho \geq 0, \qquad \forall \Delta$
- $\mathrm{Tr}[\mathcal{I}_\Delta(\rho)] \leq 1 \qquad \forall \rho, \qquad \forall \Delta$
- $\mathrm{Tr}[\mathcal{I}_\Omega(\rho)] = 1$
- $\mathcal{I}_{(\cup_n \Delta_n)}(\rho) = \sum_n \mathcal{I}_{\Delta_n}(\rho) \qquad$ con $\{\Delta_n\}$ numerabili e disgiunti
- $\mathcal{I}_\emptyset = 0$

La prima proprietà significa che $\mathcal{I}_\Delta$ mappa, $\forall \Delta$ fissato, operatori positivi $\rho \geq 0$ in operatori positivi, *i.e.* in stati non normalizzati. Questa mappa è chiamata *positive map*, ma noi vogliamo qualcosa in più dalla mappa $\mathcal{I}$. Vogliamo che sia positiva anche in uno spazio di Hilbert esteso $\mathcal{H} \otimes \mathcal{K}$ $\forall$ estensione $\mathcal{K}$, effettuando la misura non solo in uno stato locale in $\mathcal{H}$, ma in generale in uno stato entangled in $\mathcal{H} \otimes \mathcal{K}$ (tale che l'operatore risultante sia ancora uno stato non normalizzato). Ma dobbiamo ora fare attenzione: l'estensione banale $\mathcal{I} \otimes \mathbb{I}$ di una mappa positiva $\mathcal{I}$ non è necessariamente positiva [4]. Una mappa le cui estensioni banali sono tutte positive è chiamata *mappa completamente positiva* (CP map); se inoltre preserva la traccia,

[4] Consideriamo come esempio la mappa di trasposizione rispetto alla base standard in $\mathcal{H} = \mathbb{C}^2$

viene detta *trace preserving* CP map. Possiamo ora introdurre il concetto di *strumento*.
Uno *strumento* $\mathcal{I}$ è una misura dello spazio di Borel, a valori nelle mappe lineari, dagli operatori classe traccia agli operatori di classe traccia di $\mathcal{H}$, con le seguenti proprietà:

- $\mathcal{I}_\Delta$ è una CP map $\forall \Delta \subset \Omega$
- $\mathcal{I}_\Omega$ è trace preserving
- $\mathrm{Tr}[\mathcal{I}_\Delta(\rho)] \leq \mathrm{Tr}(\rho) \qquad \forall \rho \geq 0, \qquad \Delta \subset \Omega$
- $\mathcal{I}_{(\cup_n \Delta_n)}(\rho) = \sum_n \mathcal{I}_{\Delta_n}(\rho) \qquad$ con $\{\Delta_n\}$ numerabili e disgiunti
- $\mathcal{I}_\emptyset = 0$

Dato uno strumento sono automaticamente definiti:

- la Born rule $p(\Delta) = \mathrm{Tr}[\mathcal{I}_\Delta(\rho)]$
- la riduzione di stato $\rho \rightarrow \rho_\Delta = \frac{\mathcal{I}_\Delta(\rho)}{\mathrm{Tr}[\mathcal{I}_\Delta(\rho)]}$

i.e. è cioè definita una misura

- una POVM $\mathbf{\Pi}$ su Ω indotta dalla strumento tramite la relazione

$$\mathrm{Tr}[\Pi_\Delta \rho] = \mathrm{Tr}[\mathcal{I}_\Delta(\rho)], \qquad \forall \rho.$$

Quindi, con uno strumento, possiamo estendere la riduzione di stato e le POVMs a qualunque spazio delle probabilità, pur non descrivendo misure pure.

Un esempio di strumento e relativa POVM si ottiene considerando l'insieme $\Omega = \{0, 1\}$ e due diversi schemi di misurazione pura, definiti su di esso, descritti dagli operatori $\{M_0, M_1\}$ e $\{N_0, N_1\}$ rispettivamente. Se si considera uno schema casuale in cui gli operatori M_i e N_i sono scelti a caso, con probabilità p e $1 - p$, si ottiene il seguente strumento

- $\mathcal{I}_\emptyset = 0$

- $\mathcal{I}_0(\rho) = pM_0\rho M_0^\dagger + (1-p)N_0\rho N_0^\dagger$
- $\mathcal{I}_1(\rho) = pM_1\rho M_1^\dagger + (1-p)N_1\rho N_1^\dagger$
- $\mathcal{I}_\Omega = p(M_0\rho M_0^\dagger + M_1\rho M_1^\dagger) + (1-p)(N_0\rho N_0^\dagger + N_1\rho N_1^\dagger)$

Al precedente strumento è associata la POVM:

- $\Pi_\emptyset = 0$
- $\Pi_0 = pM_0^\dagger M_0 + (1-p)N_0^\dagger N_0$
- $\Pi_1 = pM_1^\dagger M_1 + (1-p)N_1^\dagger N_1$

Utilizzando quindi l'invarianza della traccia per permutazioni cicliche si dimostra che:

$$\mathrm{Tr}[\Pi_\Delta \rho] = \mathrm{Tr}[\mathcal{I}_\Delta(\rho)], \qquad \forall \rho.$$

Capitolo 2

POVMs estremali

Dopo aver esposto la teoria generale della misurazione quantistica nel primo capitolo, focalizziamo ora la nostra attenzione sulle POVMs. Questo capitolo è strutturato nel modo seguente: dimostrato che l'insieme delle POVMs è convesso, proponiamo due condizioni necessarie per descrivere le POVMs estremali, *i.e.* che non possono essere scritte come combinazione convessa di altre POVMs di tale insieme. Le due condizioni dimostrate non risultano però esaustive, non permettono infatti di dire, data una POVM, se questa è estremale o meno. Riportiamo poi due esempi che dimostrano come le condizioni di supporti disgiunti e di indipendenza lineare per gli elementi di una POVM di rango generico non siano anche sufficienti. Viene quindi proposta la condizione necessaria e sufficiente per l'estremalità delle POVMs, prima applicata ad elementi di rango 1 e poi enunciata nel caso di rango generico. Tale condizione è dimostrata in due modi diversi: il primo risulta del tutto originale mentre il secondo deriva da un adattamento del teorema di Choi per l'estremalità delle mappe completamente positive [6]. Si è trovata in letteratura [7] un'ulteriore dimostrazione, che fa riferimento alla stessa condizione necessaria e sufficiente, sviluppata tramite il teorema di Stinespring e la corrispondenza biunivoca tra POVMs e mappe lineari positive e unitali definite su una C^*-algebra abeliana.

2.1 La struttura convessa delle POVMs

Dimostriamo ora che, come gli stati, anche le POVMs possono essere pensate quali elementi di un insieme convesso.
Consideriamo l'insieme $\mathcal{D}$ delle POVMs, ovvero

$$\mathcal{D} = \{\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_d), \Pi_l \geq 0, \sum_{l=1}^{d} \Pi_l = \mathbb{I}\} \tag{2.1}$$

Dimostrare che $\mathcal{D}$ è convesso significa verificare che una combinazione lineare convessa tra due generiche POVMs è ancora una POVM. Può capitare che POVMs diverse abbiano cardinalità diverse; in questo caso estenderemo la POVM che ha la cardinalità minore aggiungendo elementi nulli, tale che sia possibile effettuare una somma tra gli elementi omonomi. Ovviamente le relazioni di completezza e di positività non vengono alterate dagli elementi nulli immessi nella POVM. Sia

$$\mathbf{\Pi}' = \lambda \mathbf{\Pi}^{(1)} + (1 - \lambda)\mathbf{\Pi}^{(2)},$$

con $\mathbf{\Pi}^{(1)}, \mathbf{\Pi}^{(2)} \in \mathcal{D}$ e $0 < \lambda < 1$. L'operatore Π_l' è positivo poichè sono positivi sia gli elementi delle POVMs che i coefficienti della combinazione, inoltre

$$\sum_{l=1}^{max(d_1,d_2)} \Pi_l' = \lambda \sum_{l=1}^{max(d_1,d_2)} \Pi_l^{(1)} + (1 - \lambda) \sum_{l=1}^{max(d_1,d_2)} \Pi_l^{(2)} = \mathbb{I} \,, \tag{2.2}$$

i.e. $\mathbf{\Pi}'$ è una POVM.

2.2 POVMs estremali

Descriviamo tale struttura convessa caratterizzando le POVMs estremali, cioè quelle $\mathbf{\Pi}$ che non possono essere scritte come combinazione lineare convessa di altre POVMs e che, come detto in precedenza, risultano affette solo da rumore intrinseco nel processo di misurazione.

2.2.1 Condizioni necessarie per l'estremalità di una POVM

Consideriamo POVMs $\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_n)$, con $\mathrm{rank}(\Pi_l) \geq 1$ [1]

Teorema 2.1 *Sia* $\mathbf{\Pi}$ *una* POVM*, se* $\mathbf{\Pi}$ *è estremale allora i suoi elementi* Π_l *hanno supporti disgiunti* [2]*.* □

Dimostrazione. La relazione dell'enunciato è equivalente alla seguente: se almeno due elementi della POVM $\mathbf{\Pi}$ non hanno supporti disgiunti allora $\mathbf{\Pi}$ non è estremale.
Dalla nuova ipotesi di supporti non disgiunti, $\exists$ almeno due indici, siano 1 e 2, tali che

$$\mathrm{Supp}(\Pi_1) \cap \mathrm{Supp}(\Pi_2) = \mathrm{N}, \tag{2.3}$$

dove N è il sottospazio generato dai vettori che vivono nell'intersezione degli span degli autovettori di Π_1 e Π_2. Consideriamo ora l'operatore M, hermitiano, definito nel modo seguente: $M = \lambda P_{\mathrm{N}}$, con

$$\lambda = \min_{|\psi\rangle \in N} \{\langle\psi|\Pi_1|\psi\rangle, \langle\psi|\Pi_2|\psi\rangle\} > 0$$

e P_{N} il proiettore su N; in questo modo gli operatori $(\Pi_l - M)$ che tratteremo in seguito risulteranno positivi. Costruiamo quindi i due nuovi insiemi $\mathbf{\Pi}'$ e $\mathbf{\Pi}''$ di operatori, definendo questi ultimi nel modo seguente:

$$\begin{aligned} \Pi'_1 &= \Pi_1 + M\,, \qquad & \Pi''_1 &= \Pi_1 - M\,, \\ \Pi'_2 &= \Pi_2 - M\,, \qquad & \Pi''_2 &= \Pi_2 + M\,, \\ \Pi'_{l>2} &= \Pi_l\,, \qquad & \Pi''_{l>2} &= \Pi_l\,. \end{aligned} \tag{2.4}$$

[1]Ricordiamo che il rango di un operatore è la dimensione del range dell'operatore stesso, ovvero $\mathrm{rank}(O) = \dim\big(\mathrm{Rng}(O)\big)$, dove $\mathrm{Rng}(O) = \{Ox, x \in \mathcal{H}\}$.

[2]Due supporti si dicono disgiunti se non hanno sottospazi in comune, *i.e.* la loro intersezione contiene solamente il vettore nullo.

Si verifica facilmente, per le considerazioni precedenti, che $\mathbf{\Pi}'$ e $\mathbf{\Pi}''$ sono due POVMs e risulta

$$\mathbf{\Pi} = \frac{1}{2}\mathbf{\Pi}' + \frac{1}{2}\mathbf{\Pi}'' \tag{2.5}$$

i.e. la POVM $\mathbf{\Pi}$ non è estremale. ■

Teorema 2.2 *Se la* POVM $\mathbf{\Pi}$ *è estremale allora i suoi elementi diversi da zero risultano linearmente indipendenti.* □

Dimostrazione. Come nel precedente teorema, consideriamo nella dimostrazione l'enunciato negato: se gli elementi diversi da zero della POVM sono linearmente dipendenti allora $\mathbf{\Pi}$ non è estremale. Supponiamo quindi che:

$$\sum_{l=1}^{n} \lambda_l \Pi_l = 0, \tag{2.6}$$

per qualche λ_l diverso da zero. Riscalando tutti i λ_l, senza perdita di generalità, possiamo prendere $-1 \leq \lambda_l \leq 1$. Definiamo ora gli operatori $\Pi_l^{\pm} = (1 \pm \lambda_l)\Pi_l$: essi costituiscono due POVMs e differiscono almeno per due elementi, poichè ci sono per ipotesi λ_l diversi da zero. Dato che $\Pi_l = \frac{1}{2}\Pi_l^{+} + \frac{1}{2}\Pi_l^{-}$, possiamo quindi concludere che la POVM $\mathbf{\Pi}$ non è estremale. ■

2.2.2 Esempi

I due teoremi sopra dimostrati offrono però solo condizioni necessarie, che non ci permettono quindi di dire se una POVM è estremale o meno nel caso in cui i supporti siano disgiunti o gli elementi linearmente indipendenti. Vediamo ora due esempi, in uno spazio di Hilbert bidimensionale, che confutano le seguenti implicazioni:

1. Supporti disgiunti degli elementi $\Pi_l \Rightarrow$ POVM $\mathbf{\Pi}$ estremale ,

2. Elementi Π_l linearmente indipendenti $\Rightarrow$ POVM $\mathbf{\Pi}$ estremale .

Figura 2.1: Vettori generanti le POVMs $\boldsymbol{\Pi}^{'}$ e $\boldsymbol{\Pi}^{''}$. In entrambi sono tratteggiati i vettori associati all'altra POVM.

Per la prima, consideriamo due POVMs di cardinalità 6, $\boldsymbol{\Pi}^{'}$ e $\boldsymbol{\Pi}^{''}$, i cui elementi diversi da zero sono i proiettori corrispondenti ai vettori della Figura 2.1.
In componenti, si ha:

$$\boldsymbol{\Pi}^{'} = \left(\frac{2}{3}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, 0 \,, \frac{1}{6}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & 3 \end{pmatrix}, 0 \,, \frac{1}{6}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & 3 \end{pmatrix}, 0 \right)$$

$$\boldsymbol{\Pi}^{''} = \left(0 \,, \frac{2}{3}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 0 \,, \frac{1}{6}\begin{pmatrix} 3 & \sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}, 0 \,, \frac{1}{6}\begin{pmatrix} 3 & -\sqrt{3} \\ -\sqrt{3} & 1 \end{pmatrix} \right).$$

Definiamo ora la POVM $\boldsymbol{\Pi}$ con elementi $\Pi_l = \frac{1}{2}\Pi_l^{'} + \frac{1}{2}\Pi_l^{''}$, come la Figura 2.2 mostra. Ovviamente $\boldsymbol{\Pi}$ non è estremale ma, dalla figura, si deduce che gli elementi Π_l hanno supporti disgiunti. Da semplici calcoli risulta che tali elementi sono linearmente dipendenti.

La seconda implicazione è negata dalla POVM

$$\boldsymbol{\Pi} = \left(\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \right),$$

i suoi elementi sono linearmente indipendenti e possono essere espressi come $\Pi_l = \frac{1}{2}\Pi_l^{'} + \frac{1}{2}\Pi_l^{''}$, dove:

$$\boldsymbol{\Pi}^{'} = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

Figura 2.2: Vettori generanti la POVM $\mathbf{\Pi}$.

$$\mathbf{\Pi}'' = \left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right).$$

Quindi $\mathbf{\Pi}$ non è estremale. Si può notare che $\mathrm{Supp}(\Pi_1) \cap \mathrm{Supp}(\Pi_2) \neq 0$.

2.2.3 Condizioni necessarie e sufficienti

Per una completa descrizione delle POVMs che risultano estremali in $\mathcal{D}$ occorre però avere condizioni necessarie e sufficienti. La prima che prendiamo in considerazione vale solo per POVMs con elementi di rango 1 e risulta essere un caso particolare della seconda condizione, applicabile invece a rango generico. Per quest'ultima riportiamo due diverse dimostrazioni che portano comunque allo stesso risultato.
Per POVMs con elementi di rango 1, le precedenti condizioni necessarie, diventano anche sufficienti[3].

[3] Risulta evidente che se la POVM $\mathbf{\Pi}$ è costituito da elementi Π_l con $\mathrm{rank}(\Pi_l) = 1$, allora tali elementi sono linearmente indipendenti se e solo se risultano avere supporti disgiunti, *i.e.* le due condizioni, per rango unitario, risultano coincidenti

Teorema 2.3 *Una* POVM $\mathbf{\Pi} = (\Pi_1, \dots, \Pi_n)$*, con* $\mathrm{rank}(\Pi_l) = 1\ \forall\, l$*, è estremale se e solo se i suoi elementi* Π_l *sono linearmente indipendenti.* □

Dimostrazione. L'implicazione necessaria è stata precedentemente provata, quindi rimane da dimostrare che essa risulta anche sufficiente. Dobbiamo mostrare che, se $\mathbf{\Pi}$ non è estremale, allora i suoi elementi sono linearmente dipendenti (o equivalentemente hanno supporti non disgiunti).
$\mathbf{\Pi}$ non è estremale, quindi $\exists$ due POVMs $\mathbf{\Pi}'$ e $\mathbf{\Pi}''$ (siano della stessa cardinalità, senza perdita di generalità) tali che $\mathbf{\Pi} = \frac{1}{2}\mathbf{\Pi}' + \frac{1}{2}\mathbf{\Pi}''$ [4]. Imposteremo una dimostrazione costruttiva, nel senso che andremo a verificare che, per ogni possibile scelta di $\mathbf{\Pi}'$ e $\mathbf{\Pi}''$, la tesi risulta soddisfatta. Per avere $\mathbf{\Pi}$ di rango 1, $\mathbf{\Pi}'$ e $\mathbf{\Pi}''$ devono avere elementi di rango 1, o al più nulli. Tali elementi devono chiaramente risultare non proporzionali tra di loro, altrimenti tali sarebbero anche anche quelli di $\mathbf{\Pi}$. Definiamo ora i due seguenti insiemi di indici:

$$I^{\parallel} = \{i : \Pi_i' \propto \Pi_i''\}$$

$$I^{\nparallel} = \{j : \Pi_j' \not\propto \Pi_j''\}$$

e consideriamo l'espressione $\mathbf{\Pi} = \frac{1}{2}\mathbf{\Pi}' + \frac{1}{2}\mathbf{\Pi}''$.
Per ogni $i \in I^{\nparallel}$, deve essere $\Pi_i' = 0$ o $\Pi_i'' = 0$ per non avere un Π_i di rango 2. Se invece avessimo la somma tra Π_i', con $i \in I^{\parallel}$, e Π_j'', con $j \in I^{\nparallel}$, o viceversa, $\mathbf{\Pi}$ avrebbe elementi linearmente dipendenti. Rimane quindi da analizzare la situazione in cui gli elementi di $\mathbf{\Pi}'$ e $\mathbf{\Pi}''$ sono linearmente indipendenti, tutti quelli proporzionali si sommano tra loro, e gli altri con gli elementi nulli (Fig. 2.3). Se $\mathbf{\Pi}'$ e $\mathbf{\Pi}''$ non hanno elementi proporzionali, allora gli elementi di $\mathbf{\Pi}$

[4] Notiamo che i coefficienti della combinazione lineare convessa possono sempre essere presi uguali ad $\frac{1}{2}$, infatti scrivere $\mathbf{\Pi} = \lambda\mathbf{\Pi}^1 + (1-\lambda)\mathbf{\Pi}^2$ è equivalente a

$$\frac{1}{2}\mathbf{\Pi}^1 + (\lambda - \frac{1}{2})\mathbf{\Pi}^1 + (1-\lambda)\mathbf{\Pi}^2 = \frac{1}{2}\mathbf{\Pi}^1 + \frac{1}{2}\mathbf{\Pi}' \qquad \text{se } \lambda \geq \frac{1}{2}$$

oppure

$$\frac{1}{2}\mathbf{\Pi}^2 + (\frac{1}{2} - \lambda)\mathbf{\Pi}^2 + \lambda\mathbf{\Pi}^1 = \frac{1}{2}\mathbf{\Pi}^2 + \frac{1}{2}\mathbf{\Pi}'' \qquad \text{se } \lambda \leq \frac{1}{2}$$

.

Figura 2.3: Le righe corrispondono agli elementi di $\mathbf{\Pi}'$, $\mathbf{\Pi}''$, e $\mathbf{\Pi}$, rispettivamente. Le prime due colonne contengono gli elementi che corrispondono (stesso colore) a quelli a loro proporzionali nell'altra POVM, questi elementi si sommano nella POVM risultante. Le altre colonne si riferiscono invece a quegli elementi che non hanno una tale corrispondenza, e si sommano con le entrate nulle (cerchi vuoti).

saranno $\{\frac{1}{2}\Pi'_i\} \cup \{\frac{1}{2}\Pi''_i\}$. Visto che

$$\sum_i \frac{1}{2}\Pi'_i - \sum_i \frac{1}{2}\Pi''_i = \frac{1}{2}\mathbb{1} - \frac{1}{2}\mathbb{1} = 0 \ ,$$

allora gli elementi di $\mathbf{\Pi}$ sono linearmente dipendenti e la tesi è verificata. D'altra parte, se ci sono p coppie di elementi proporzionali, ovvero $\Pi''_i = \lambda_i \Pi'_i$ per $i \in I^{\parallel} = \{1, \ldots, p\}$, allora si ha

$$\sum_{i>p} \Pi''_i - \sum_{i>p} \Pi'_i = (\mathbb{1} - \sum_{i=1}^{p} \Pi''_i) - (\mathbb{1} - \sum_{i=1}^{p} \Pi'_i) = \sum_{i=1}^{p} (1 - \lambda_i)\Pi'_i \ .$$

Dato che gli operatori $\{\Pi'_i\}$ e $\{\Pi''_i, i > p\}$ sono proporzionali agli elementi di $\mathbf{\Pi}$, concludiamo che gli elementi di $\mathbf{\Pi}$ sono linearmente dipendenti e la tesi risulta correta anche in questo ultimo caso. ■

Consideriamo ora POVMs a rango generico, e riportiamo due diverse versioni della stessa condizione necessaria e sufficiente per la loro estremalità.
Osservazione. $\mathbf{\Pi}$ non è estremale se può essere scritta come combinazione lineare convessa di altre POVMs estremali

$$\mathbf{\Pi} = \sum_j \lambda_j \mathbf{\Pi}^{(j)}$$

con $\sum_j \lambda_j = 1$. Se ora esplicitiamo la sommatoria isolando il primo termine $\mathbf{\Pi}^{(1)}$ (supposto $\lambda_1 \neq 0$) si ottiene

$$\mathbf{\Pi} = \mathbf{\Pi}^{(1)} + \sum_{j>1} \lambda_j \mathbf{\Pi}^{(j)} + (\lambda_1 - 1)\mathbf{\Pi}^{(1)} = \mathbf{\Pi}^{(1)} + \mathbf{\Delta}.$$

Prendiamo in considerazione $\mathbf{\Delta} = (\Delta_1, \ldots, \Delta_n)$, dove gli operatori Δ_i devono soddisfare la relazione $\sum_i \Delta_i = 0$, visto che $\sum_i \Pi_i = \sum_i \Pi_i^{(1)} = \mathbb{I}$. Ogni operatore Δ_i può essere decomposto in una parte positiva $[\Delta_i]^+$ e una negativa $[\Delta_i]^-$, dove positività e negatività sono associate agli autovalori positivi e negativi. La definizione dei $\Delta_i = [\Delta_i]^+ - [\Delta_i]^-$ comporta che

$$[\Delta_i]^- = (1 - \lambda_1)\Pi_i^1 < \Pi_i^1. \tag{2.7}$$

Quindi possiamo dire che $\mathbf{\Pi}$ non è estremale se si possono riscrivere i suoi elementi come $\Pi_i = \Pi_i' + \Delta_i$, dove $\mathbf{\Pi}'$ è una POVM, $[\Delta_i]^- < \Pi_i'$ e alcuni Δ_i diversi a zero.

Possiamo quindi enunciare il teorema che racchiude i precedenti risultati e li amplia fornendo una condizione necessaria e sufficiente per l'estremalità delle POVMs:

Teorema 2.4 *Siano $|v_{ij}\rangle$ gli autovettori dell'i-esimo elemento della POVM $\mathbf{\Pi}$, $\mathbf{\Pi}$ è estremale se e solo se gli operatori*

$$|v_{ij}\rangle\langle v_{ij'}| \tag{2.8}$$

con $1 \leq j, j' \leq \operatorname{rank} \Pi_i$, $i = 1, ..., n$ *sono linearmente indipendenti.* □

Dimostrazione. (condizione necessaria)
Supponiamo che esista qualche $\lambda_{ijj'} \neq 0$ tale che

$$\sum_{ijj'} \lambda_{ijj'} |v_{ij}\rangle\langle v_{ij'}| = 0 \tag{2.9}$$

Definendo l'operatore hermitiano $\Delta_i = \mu \sum_{jj'} (\lambda_{ijj'} + \bar{\lambda}_{ijj'}) |v_{ij}\rangle\langle v_{ij'}|$, si ha $\sum_i \Delta_i = 0$, è possibile inoltre scegliere μ tale che $|\Delta_i| < \Pi_i$. Si possono allora costruire due POVMs $\mathbf{\Pi}^+$ e $\mathbf{\Pi}^-$ con elementi $\Pi_i^\pm = \Pi_i \pm \Delta_i$. Essendo $\mathbf{\Pi} = \frac{1}{2}(\mathbf{\Pi}^+ + \mathbf{\Pi}^-)$, $\mathbf{\Pi}$ non è estremale.

(condizione sufficiente)
Supponiamo $\mathbf{\Pi}$ non estremale, per l'osservazione precedente possiamo allora scrivere $\Pi_i = \Pi_i' + \Delta_i$, dove $\mathbf{\Pi}'$ è una POVM,

$$[\Delta_i]^- < \Pi_i' \tag{2.10}$$

e $\sum_i \Delta_i = 0$. Visto che $[\Delta_i]^- < \Pi_i'$, il supporto di Π_i contiene quello di $|\Delta_i|$[5]. Allora Δ_i può essere espresso sulla base degli autovettori $|v_{ij}\rangle$ di Π_i, *i.e.* $\exists\, \lambda_{ijj'} \neq 0$ tali che

$$\Delta_i = \sum_{jj'} \lambda_{ijj'} |v_{ij}\rangle\langle v_{ij'}|. \tag{2.11}$$

Poichè $\sum_i \Delta_i = 0$, concludiamo che $\sum_{ijj'} \lambda_{ijj'} |v_{ij}\rangle\langle v_{ij'}| = 0$, gli operatori $|v_{ij}\rangle\langle v_{ij'}|$ sono linearmente dipendenti. ■

Osservazione. È evidente come la condizione del Teorema 2.3 risulti essere una condizione particolare di quella del Teorema 2.4: se infatti $\text{rank}(\Pi_i) = 1$, l'insieme (2.8) linearmente indipendente diventa

$$\{|v_i\rangle\langle v_i|,\ i = 1, ..., n\}.$$

Questo significa che $\nexists\, \lambda_i \neq 0$ tali che

$$\sum_i \lambda_i |v_i\rangle\langle v_i| = \sum_i \lambda_i \Pi_i = 0,$$

i.e. gli elementi Π_i della POVM $\mathbf{\Pi}$ sono linearmente indipendenti.

La condizione del Teorema 2.4 può essere dimostrata anche adattando il teorema di Choi per l'estremalità delle mappe completamente positive [6].

[5] Risulta fondamentale il minore stretto della (2.10), se la relazione fosse col $\leq$, potrebbe verificarsi il caso in cui $[\Delta_i]^- = \Pi_i'$ e quindi il supporto di Π_i non conterrebbe quello di $|\Delta_i|$.

Definizione 2.1 *Sia*

$$\begin{aligned}\Phi: \quad & \mathcal{H} \to \mathcal{L}(\mathcal{H}) \\ & f \mapsto \Phi(f) = \sum_l V_l^\dagger f \circ V_l\end{aligned} \tag{2.12}$$

una mappa lineare dalla spazio di Hilbert $\mathcal{H}$ allo spazio di operatori $\mathcal{L}(\mathcal{H})$ e definiamo l'azione dei $V_l : \mathcal{H} \to$ funzioni ad n valori*, come segue:*

1. $V_l|\varphi\rangle = \begin{pmatrix} \langle v_{1l}|\varphi\rangle \\ \vdots \\ \langle v_{nl}|\varphi\rangle \end{pmatrix} \quad \forall|\varphi\rangle \in \mathcal{H}$

2. *$(\circ)$ è il prodotto di Shur, ovvero* $f \circ V_l = \begin{pmatrix} f_1\langle v_{1l}| \\ \vdots \\ f_n\langle v_{nl}| \end{pmatrix}$

3. *fissato* $(f,g) = \sum_j f_j g_j$*, sia* $V_l^\dagger g = V_l^\dagger \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = \sum_i |v_{il}\rangle g_i$.

Teorema 2.5 *Consideriamo l'espressione canonica di $\Phi(f) = \sum_l V_l^\dagger f \circ V_l$, in cui cioè $\{V_l\}_l$ è un insieme linearmente indipendente*[6]*. Allora $\{V_l\}$ e $\{W_m\}$ sono decomposizioni equivalenti, i.e. $\Phi(f) = \sum_m W_m^\dagger f \circ W_m$, se e solo se $W_m = \sum_l \mu_{ml} V_l$, con $(\mu_{ml})_{ml}$ isometria, cioè $\sum_m \mu_{im}^\dagger \mu_{mj} = \delta_{ij}$.* □

Dimostrazione. (condizione sufficiente)
Visto che ogni mappa lineare $\Phi : \mathcal{H} \to \mathcal{L}(\mathcal{H})$ è determinata dai suoi valori su e_j, dove e_j è il vettore colonna con la j-esima entrata uguale a uno e zero altrove, consideriamo $\Phi(e_j) = \sum_l V_l^\dagger e_j \circ V_l = \sum_l |v_{jl}\rangle\langle v_{jl}|$. Se $W_m = \sum_l \mu_{ml} V_l$, con $\sum_m \mu_{im}^\dagger \mu_{mj} = \delta_{ij}$, allora possiamo scrivere

$$\sum_l |v_{jl}\rangle\langle v_{jl}| = \sum_{mlk} \mu_{ml}^* \mu_{mk} |v_{jl}\rangle\langle v_{jk}| = \sum_{lkm} \mu_{lm}^\dagger \mu_{mk} |v_{jl}\rangle\langle v_{jk}| = \sum_m |w_{jm}\rangle\langle w_{jm}|$$

[6] $\{V_l\}_l$ insieme linearmente indipendente significa che ogni $\{\langle v_{il}|\}_l$, con $i = 1, ..., n$ è un insieme linearmente indipendente

quindi $\{V_l\}$ e $\{W_m\}$ sono decomposizioni equivalenti.

(condizione necessaria)

Abbiamo che $\Phi(e_j) = \sum_l |v_{jl}\rangle\langle v_{jl}| = \sum_m |w_{jm}\rangle\langle w_{jm}|$.

Allora $|w_{jm}\rangle \in \text{span}\{|v_{jl}\rangle\}$, *i.e.* $\exists(\mu_{ml})_{ml}$ tale che $|w_{jm}\rangle = \sum_l \mu^*_{ml}|v_{jl}\rangle$. Segue che $W_m = \sum_l \mu_{ml}V_l$. Poichè $\{|v_{jl}\rangle\}_l$ è un insieme linearmente indipendente, tale è anche $\{|v_{jl}\rangle\langle v_{jl'}|\}_{ll'}$ (infatti $\{|v_{jl}\rangle\langle v_{jl'}|\}_{ll'}$ è una base dello spazio delle trasformazioni lineari in $\text{span}\{|v_{jl}\rangle\}_l$). Da $\sum_l |v_{jl}\rangle\langle v_{jl}| = \sum_m |w_{jm}\rangle\langle w_{jm}| = \sum_m \sum_{lk} \mu^*_{ml}\mu_{mk}|v_{jl}\rangle\langle v_{jk}|$, si ottiene $\sum_m \mu^\dagger_{lm}\mu_{mk} = \delta_{lk}$. Quindi $(\mu_{ml})_{ml}$ è un' isometria. ■

Teorema 2.6 *Sia* $\Phi : \mathcal{H} \to \mathcal{L}(\mathcal{H})$, *con* $\Phi(f) = \sum_l V_l^\dagger f \circ V_l$. *Allora* Φ *è estremale in* $\mathsf{S}_K = \{\Phi : \mathcal{H} \to \mathcal{L}(\mathcal{H})$ *tale che* $\Phi(f) = \sum_l V_l^\dagger f \circ V_l$ *e* $\sum_l V_l^\dagger V_l = K$ *con* $0 \le K \le \mathbb{I}\}$ *se e solo se, per la sua decomposizione canonica,* $\{V_l^\dagger V_k\}_{lk}$ *è un insieme linearmente indipendente.* □

Dimostrazione. (condizione necessaria)

Assumiamo Φ estremale in S_K, e consideriamo la decomposizione canonica $\Phi(f) = \sum_l V_l^\dagger f \circ V_l$ con $\{V_l\}_l$ linearmente indipendenti. Supponiamo ora che

$$\sum_{lk} \lambda_{lk} V_l^\dagger V_k = 0, \tag{2.13}$$

dobbiamo dimostrare che $(\lambda_{lk})_{lk} = 0$. Possiamo assumere che $(\lambda_{lk})_{lk}$ sia una matrice hermitiana: infatti, poichè

$$(V_l^\dagger V_k)^\dagger = (\sum_i |v_{il}\rangle\langle v_{ik}|)^\dagger = V_l^\dagger V_k$$

dall' espressione (2.13) si può concludere che $\sum_{lk}(\lambda_{lk} \pm \lambda^*_{kl})V_l^\dagger V_k = 0$. Quindi se riusciamo a dimostrare che $(\lambda_{lk} \pm \lambda^*_{kl})_{lk} = 0$, abbiamo automaticamente $(\lambda_{lk})_{lk} = 0$. Riscalando si può assumere $-\mathbb{I} \le (\lambda_{lk})_{lk} \le \mathbb{I}$. Definiamo ora

$$\Psi^{(\pm)}(f) = \Phi(f) \pm \sum_{lk} \lambda_{lk} V_l^\dagger f \circ V_k = \sum_{lk} (\delta_{lk} \pm \lambda_{lk}) V_l^\dagger f \circ V_k \tag{2.14}$$

e quindi $\Phi(f) = \frac{1}{2}(\Psi^{(+)}(f) + \Psi^{(-)}(f))$. Sia $\Lambda = (\lambda_{lk})_{lk}$, definiamo

$$0 \le \mathbb{I} \pm \Lambda = \alpha^{(\pm)\dagger}\alpha^{(\pm)}$$

e

$$W_l^{(\pm)} = \sum_k \alpha_{lk}^{(\pm)} V_k = \begin{pmatrix} \sum_k \alpha_{lk}^{(\pm)} \langle v_{1k}| \\ \vdots \\ \sum_k \alpha_{lk}^{(\pm)} \langle v_{nk}| \end{pmatrix}.$$

Sostituendo in (2.14) si ottiene

$$\begin{aligned} \Psi^{(\pm)}(f) &= \sum_{lk} (\alpha_{lk}^{(\pm)\dagger} \alpha_{lk}) V_l^\dagger f \circ V_k \\ &= \sum_{lk} \alpha_{kl}^{(\pm)*} V_l^\dagger f \circ \alpha_{lk}^{(\pm)} V_k \\ &= \sum_m W_m^{(\pm)\dagger} f \circ W_m^{(\pm)} \end{aligned} \tag{2.15}$$

e quindi $\Psi^{(\pm)} \in S_K$. Dal fatto che $\Phi = \frac{1}{2}(\Psi^{(+)} + \Psi^{(-)})$ e dall'estremalità di Φ, si ottiene $\Phi = \Psi^{(+)} = \Psi^{(-)}$. Dal Teorema 2.5, $(\alpha_{lk})_{lk}$ è un'isometria e quindi $\Lambda = (\lambda_{lk})_{lk} = 0$.

(condizione sufficiente)
Assumiamo $\Phi(f) = \sum_l V_l^\dagger f \circ V_l$ con $\{V_l^\dagger V_k\}_{lk}$ insieme linearmente indipendente. Supponiamo

$$\Phi = \frac{1}{2}(\Psi_1 + \Psi_2),$$

con $\Psi_1(f) = \sum_m W_m^\dagger f \circ W_m$ e $\Psi_2(f) = \sum_k Z_k^\dagger f \circ Z_k$, $\Psi_1, \Psi_2 \in S_K$. Dato che

$$\Phi(f) = \frac{1}{2} \sum_m W_m^\dagger f \circ W_m + \frac{1}{2} \sum_k Z_k^\dagger f \circ Z_k,$$

W_m e Z_k possono essere espressi in funzione di V_l. Sia $W_m = \sum_l \mu_{ml} V_l$, $\forall m$. Allora

$$\sum_l V_l^\dagger V_l = K = \sum_m W_m^\dagger W_m = \sum_{mll'} \mu_{ml}^* \mu_{ml'} V_l^\dagger V_{l'}$$

e quindi $\sum_m \mu_{lm}^\dagger \mu_{ml'} = \delta_{ll'}$: *i.e.* $(\mu_{lm})_{lm}$ è un'isometria e per il Teorema 2.5 concludiamo che $\Phi = \Psi_1$, quindi Φ è estremale in S_K. ■

Dalla definizione di S_K, $S_{\mathbb{I}}$ è l' insieme delle $\Phi : \mathcal{H} \to \mathcal{L}(\mathcal{H})$ tali che

$$\Phi(f) = \sum_l V_l^\dagger f \circ V_l = \sum_{lm} f_m |v_{ml}\rangle\langle v_{ml}| \tag{2.16}$$

e

$$\sum_l V_l^\dagger V_l = \mathbb{I}.$$

Sia

$$\mathcal{D} = \{\mathbf{\Pi} = (\Pi_1, \dots, \Pi_n), \Pi_i \geq 0, \sum_{i=1}^{n} \Pi_i = \mathbb{I}\} \tag{2.17}$$

l'insieme delle POVMs di cardinalità n.

Proposizione 2.1 *Esiste una corrispondenza biunivoca tra $S_\mathbb{I}$ e $\mathcal{D}$.* □

Dimostrazione. Si consideri, $\forall f \in \mathcal{H}$ e $\forall\, \mathbf{\Pi}$ fissata $\in \mathcal{D}$, la mappa

$$\Phi(f) = \sum_i f_i \Pi_i, \tag{2.18}$$

dove le Π_i sono gli elementi della POVM $\mathbf{\Pi}$ ed hanno la seguente decomposizione spettrale $\Pi_i = \sum_j |u_{ij}\rangle\langle u_{ij}|$ con $\||u_{ij}\rangle\|^2 > 0$ ($j = 1, ..., \mathrm{rank}(\Pi_i)$) autovalori diversi da zero dell'elemento e $|u_{ij}\rangle$ i corrispondenti autovettori. Quindi abbiamo $\Phi(f) = \sum_{ij} f_i |u_{ij}\rangle\langle u_{ij}|$. Dalla relazione di completezza $\sum_i \Pi_i = \mathbb{I}$ risulta perciò evidente che $\Phi \in S_\mathbb{I}$, con

$$V_j|\varphi\rangle = \begin{pmatrix} \langle u_{1j}|\varphi\rangle \\ \vdots \\ \langle u_{nj}|\varphi\rangle \end{pmatrix}.$$

Per quanto riguarda la relazione inversa $\Phi(f) = \sum_{lm} f_m |u_{ml}\rangle\langle u_{ml}| \in S_\mathbb{I}$ può sempre essere scritto come $\Phi(f) = \sum_m f_m \Pi_m$ definendo

$$\Pi_m = \sum_l |u_{ml}\rangle\langle u_{ml}| \geq 0,$$

che verifica automaticamente la completezza. Essendo la relazione tra Π_i e $\Phi(f) = \sum_i f_i \Pi_i$ lineare, la corrispondenza risulta biunivoca. ■

Abbiamo ora tutti gli elementi per proporre una seconda versione della dimostrazione del Teorema 2.4.

Teorema 2.7 *Una POVM* $\mathbf{\Pi}$*, con elementi* $\Pi_i = \sum_j |u_{ij}\rangle\langle u_{ij}|$*, è estremale in* $\mathcal{D}$ *se e solo se*

$$\{|u_{ij}\rangle\langle u_{ij'}|,\ 1 \leq j, j' \leq \operatorname{rank}\Pi_i,\ i = 1, ..., n\} \tag{2.19}$$

è un insieme linearmente indipendente. □

Dimostrazione. Usando la Proposizione 2.1, $\mathbf{\Pi}$ è estremale se e solo se la mappa

$$\Phi(f) = \sum_i f_i \Pi_i = \sum_{ij} f_i |u_{ij}\rangle\langle u_{ij}| \tag{2.20}$$

è estremale in $S_{\mathbb{I}}$. Dato che la mappa dell' equazione (2.20) è già in forma canonica ($\{\langle u_{ij}|\}_j$ è un insieme linearmente indipendente perchè gli $|u_{ij}\rangle$ sono gli autovettori di Π_i), basta applicare il Teorema 2.6 a $\Phi(f)$. Concludiamo che

$$\{V_j^\dagger V_{j'}\}_{jj'} = \{|u_{ij}\rangle\langle u_{ij'}|,\ i = 1, ..., n\}_{jj'}$$

deve essere un insieme linearmente indipendente. ■

Osservazione. Col Teorema 2.7 giungiamo, quindi, alla stessa condizione necessaria e sufficiente del Teorema 2.4 per l'estremalità delle POVMs, ma con una dimostrazione molto diversa: nel primo è stato sufficiente manipolare la definizione di POVM non estremale tramite la definizione degli operatori $\mathbf{\Delta}$; nel secondo, invece, il risultato finale deriva da due dimostrazioni preliminari con le quali si è verificato che le decomposizioni equivalenti delle mappe $\Phi(f) = \sum_l V_l^\dagger f \circ V_l$, da noi definite, sono legate da una isometria e una volta trovata la condizione necessaria e sufficiente per l'estremalità di tali mappe, la si è sfruttata per il caso delle POVMs, visto che sussiste una corrispondenza biunivoca tra l'insieme delle $\Phi(f)$ tali che $\sum_l V_l^\dagger V_l = \mathbb{I}$ e quello delle POVMs.

Capitolo 3

Misurazioni e osservabili

In questo capitolo cercheremo di connettere le osservabili alle misure generalizzate e di conseguenza alle POVMs. Per la parte introduttiva sulla definizione del problema agli autovalori si è fatto riferimento a [8] e [9]. Fissiamo quindi le caratteristiche matematiche dell'operatore corrispondente ad un'osservabile e le riferiamo alle POVMs, definendo la decomposizione a valori singolari delle misure generalizzate associate.

3.1 Problema agli autovalori e osservabili

Sia A un operatore lineare. Dalla definizione di equazione agli autovalori, il numero complesso a_m è un autovalore di A e il ket $|m\rangle$ un autovettore associato ad a_m se

$$A|m\rangle = a_m|m\rangle.$$

Se $|m\rangle$ è un autostato di A, ogni multiplo $c|m\rangle$ di questo ket è un autovettore di A appartenente allo stesso autovalore; se esistono diversi autovettori linearmente indipendenti appartenenti allo stesso autovalore a_m, allora ogni combinazione lineare di questi kets è un autoket di A per questo autovalore. L' insieme di autokets di A appartenenti a un dato autovalore a_m forma uno spazio vettoriale, *i.e.* il sottospazio dell' autovalore a_m.
Se A è hermitiano si hanno le seguenti proprietá:

(i) i due spettri di autovalori $\{a_m\}$, $\{a_n^{'}\}$, dove $A|m\rangle = a_m|m\rangle$ e $\langle n|A = a_n^{'}\langle n|$, coincidono;

(ii) tutti gli autovalori sono reali;

(iii) il sottospazio degli autobras di un dato autovalore è lo spazio duale del sottospazio degli autokets dello stesso autovalore;

(iv) l'insieme degli autovettori è completo e può essere normalizzato, *i.e.* $\langle n|m\rangle = \delta_{nm}$.

In generale, dobbiamo considerare anche lo spettro continuo degli autovalori: le quattro proprietà rimangono invariate, a patto di prendere nella relazione di ortogonalità la funzione δ di Dirac. Abbiamo quindi un operatore hermitano A il cui spettro è costituito da una autovalori discreti a_n e continui $a(\nu)$, corrispondenti agli autovettori[1] $\varphi_n^{(r)}$ (o $|nr\rangle$) e $\varphi^{(r)}(\nu,\rho)$ (o $|\nu\rho r\rangle$), rispettivamente. La completezza può essere espressa tramite una generalizzata relazione di chiusura [8]

$$\sum_{nr} |nr\rangle\langle nr| + \sum_{r} \iint |\nu\rho r\rangle \, d\nu \, d\rho \, \langle \nu\rho r| = \mathbb{I}.$$

Tale operatore hermitiano A è detto *osservabile.*

3.2 Misurazioni corrispondenti alle osservabili

Consideriamo ora il problema agli autovalori limitandoci agli autovettori che vivono nello spazio di Hilbert; gli autovalori formeranno quindi un insieme discreto $\{m\}$. Abbiamo introdotto, nel capitolo precedente, le misure proiettive come una classe speciale delle misure generalizzate, e dimostrato che, usando una misura indiretta, esse divengono equivalenti a queste ultime. Puntiamo ora la nostra attenzione su quale sia il significato di osservabile in relazione

[1] L'indice discreto r tiene conto di possibili degenerazioni.

alle misure proiettive [1], e tentiamo di darne una sorta di generalizzazione tramite le misure generalizzate M_l e conseguentemente le POVMs Π_l.
Una misura proiettiva è descritta da un'*osservabile* A: un operatore hermitiano nello spazio degli stati del sistema in questione. L' osservabile ha una decomposizione spettrale

$$A = \sum_m m P_m, \tag{3.1}$$

dove P_m è il proiettore sull' autospazio di A con autovalore m. I possibili risultati della misura sono gli autovalori, m, dell' osservabile. Se lo stato del sistema è $|\psi\rangle$, allora la probabilità di ottenere il risultato m è data da

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

Dalla definizione, il valore medio della misura è:

$$\begin{aligned} \mathbf{E}(A) &= \sum_m m p(m) \\ &= \sum_m m\langle\psi|P_m|\psi\rangle \\ &= \langle\psi|\left(\sum_m m P_m\right)|\psi\rangle \\ &= \langle\psi|M|\psi\rangle. \end{aligned} \tag{3.2}$$

In riferimento all'equazione (3.1) cerchiamo ora di caratterizzare l'osservabile tramite le misure generalizzate M_l e le POVMs $\Pi_l = M_l^\dagger M_l$. Sappiamo che se gli elementi Π_l di una POVM $\mathbf{\Pi}$ commutano, allora possiamo simultaneamente diagonalizzare tutti i Π_l come segue

$$\Pi_l = \sum_m p(l|m) P_m, \tag{3.3}$$

dove P_m è il proiettore sull'm-esimo autospazio e l'autovalore $p(l|m)$ soddisfa le condizioni $p(l|m) \geq 0$ e $\sum_l p(l|m) = 1$ (dato che Π_l è una POVM); $p(l|m)$ può cioè essere interpretato come la probabilità condizionata di misurare l quando il valore vero è m. Da questa diagonalizzazione possiamo vedere che le POVM che commutano sono proprio la generalizzazione banale della

risoluzione ortonormale tramite randomizzazione dei risultati della misura.
Vediamo ora come questa condizione si riflette sulla misura generalizzata M_l, e più specificatamente sulla sua SVD (decomposizione a valori singolari). Si può infatti dimostrare che per ogni matrice $A \in M_{m,n}$ ne esistono due unitarie $V \in M_m$ e $W \in M_n$ tali che

$$A = V \Sigma W^\dagger,$$

dove $\Sigma = \{\Sigma_{ij}\} \in M_{m,n}$ con $\Sigma_{ij} = 0 \;\forall\, i \neq j$ e $\Sigma_{11} \geq \Sigma_{22} \geq \cdots \geq \Sigma_{kk} > \Sigma_{k+1k+1} = \cdots = \Sigma_{qq} = 0$, dove $q = \min(m,n)$ e $k = \mathrm{rank}(A)$. Le entrate Σ_{ll} sono le radici quadrate degli autovalori di $AA^\dagger$, ordinate in ordine decrescente, chiamate valori singolari di A.
Consideriamo la SVD di M_l, sia

$$M_l = X_l \Sigma_l Y_l^\dagger \tag{3.4}$$

con X_l e Y_l unitari: di conseguenza si ottiene la POVM

$$\Pi_l = M_l^\dagger M_l = Y_l \Sigma_l^2 Y_l^\dagger. \tag{3.5}$$

Ma con questa forma le POVMs Π_l e Π_k con $l \neq k$ non commutano, infatti

$$\left[M_l^\dagger M_l, M_k^\dagger M_k\right] = \left[Y_l \Sigma_l^2 Y_l^\dagger, Y_k \Sigma_l^2 Y_k^\dagger\right] \neq 0.$$

Prendendo però i fattori destri della SVD uguali, $\forall\, l$ a meno di una permutazione P_l dei valori singolari (richiesta necessaria a causa dell'ordine decrescente di questi ultimi nella SVD) si ottiene $M_l = X_l \Sigma_l P_l Y^\dagger$ e di conseguenza il commutatore:

$$\left[M_l^\dagger M_l, M_k^\dagger M_k\right] = Y P_l^\dagger \Sigma_l^2 P_l P_k^\dagger \Sigma_k^2 P_k Y^\dagger - Y P_k^\dagger \Sigma_k^2 P_k P_l^\dagger \Sigma_l^2 P_l Y^\dagger = 0 \tag{3.6}$$

essendo Y unitaria. Consideriamo ora l'insieme di vettori ortonormali $|l\rangle$, dove $l = 1, \cdots, N$ con N cardinalità della POVM Π_l; siano

$$Y|l\rangle = |Y(l)\rangle \qquad \Sigma_k |l\rangle = \sigma_l(M_k)|l\rangle \qquad P_k|l\rangle = |P_k l\rangle.$$

Applicando quindi $M_k^\dagger M_k$ agli stati $|Y(l)\rangle$ si ottiene

$$\begin{aligned} M_k^\dagger M_k|Y(l)\rangle &= YP_k^\dagger \Sigma_k^2 P_k Y Y^\dagger |l\rangle \\ &= YP_k^\dagger \Sigma_k^2 |P_k l\rangle \\ &= \sigma_{P_k l}^2(M_k) Y P_k^\dagger |P_k l\rangle \\ &= \sigma_{P_k l}^2(M_k) Y |l\rangle \\ &= \sigma_{P_k l}^2(M_k)|Y(l)\rangle. \end{aligned} \tag{3.7}$$

In definitiva abbiamo un'osservabile $M_k^\dagger M_k$, con autovalori $\sigma_{P_k l}^2(M_k)$ e autovettori $|Y(l)\rangle$ (essendo Y unitario, i vettori $|Y(l)\rangle$ risultano ortonormali e il set $\{|Y(l)\rangle\}$ completo). Vediamo ora cosa comporta l'equazione (3.6): visto che le POVMs commutano, esse saranno simultaneamente diagonalizzabili, sia

$$\Pi_l = \sum_k \epsilon_k^{(l)} |k\rangle\langle k|.$$

Dalla positività e dalla relazione di completezza della Π_l seguono le seguenti: $\epsilon_k^{(l)} \geq 0$ e $\sum_l \epsilon_k^{(l)} = 1$; queste due ultime relazioni ci autorizzano ad interpretare $\epsilon_k^{(l)}$ come la probabilità condizionata $p(l|k)$, la probabilità cioè di misurare l col valore vero k. Sostituendo $p(l|k)$ nell'ultima equazione ritroviamo ovviamente la (3.3).

Capitolo 4

Teoria della maggiorizzazione

Il confronto tra due quantità vettoriali porta spesso a interessanti disuguaglianze che possono essere espresse come relazioni di *maggiorizzazione*. Questo capitolo offre solo gli aspetti elementari di tale teoria (per una trattazione completa si faccia riferimento al Cap. 2 di [10]), enfatizzando il fondamentale legame col concetto di entropia e quindi di disordine. Nei teoremi che seguono viene poi sottolineata la relazione tra maggiorizzazione e matrici unitarie-stocastiche, con particolare attenzione alle relazioni di maggiorizzazione tra i vettori di autovalori di due matrici.

4.1 Definizione

Il motivo basilare della maggiorizzazione riguarda il problema di confrontare due distribuzioni di probabilità e determinare quale delle due è più disordinata. Sia $x = (x_1, \ldots, x_n)$ un vettore $\in \mathbb{R}^n$; introduciamo la notazione $\downarrow$ per indicare le componenti del vettore poste in ordine decrescente, *i.e.* $x^\downarrow = (x_1^\downarrow, \ldots, x_n^\downarrow)$, dove $x_1^\downarrow \geq \ldots \geq x_n^\downarrow$. Consideriamo $x, y \in \mathbb{R}^n$, diciamo che x è maggiorizzato da y, in simboli $x \prec y$, se

$$\sum_{j=1}^{k} x_j^\downarrow \leq \sum_{j=1}^{k} y_j^\downarrow, \qquad 1 \leq k \leq n \tag{4.1}$$

con

$$\sum_{j=1}^{n} x_j^{\downarrow} = \sum_{j=1}^{n} y_j^{\downarrow}. \tag{4.2}$$

Nota. In tutte le relazioni di maggiorizzazione, nel caso in cui si debbano confrontare due vettori di dimensione diversa, è sempre possibile aggiungere degli zeri quali entrate del vettore con dimensione minore fino a raggiungere la stessa per entrambi. Quindi si adotta la convenzione che quando x e y sono di dimensione diversa, $x \prec y$ significa $\tilde{x} \prec \tilde{y}$, dove $\tilde{x}$ e $\tilde{y}$ contengono componenti nulle aggiunte. È evidente che questa nozione estesa di maggiorizzazione è ben definita, e applicabile anche ad x e y aventi componenti non-negative.

Esempio. Se $x_i \geq 0$ e $\sum x_i = 1$, allora

$$(\frac{1}{n}, \ldots, \frac{1}{n}) \prec (x_1, \ldots, x_n) \prec (1, 0, \ldots, 0).$$

4.2 Teoremi sulla maggiorizzazione

Riportiamo ora, senza dimostrazione, un teorema [10] che offre una prima naturale nozione di disordine nel senso di mescolamento:

Teorema 4.1 (Birkhoff) *Siano x e y due distribuzioni di probabilità, si ha che*

$$x \prec y \quad \textit{se e solo se} \quad x = \sum_i p_i P_i y,$$

dove p_i è la componente di una distribuzione di probabilità, e le P_i sono matrici di permutazione. □

Quando $x \prec y$, possiamo immaginare che y sia la distribuzione di probabilità in entrata in un canale rumoroso che permuta random i simboli mandati attraverso di esso, inducendo una distribuzione di probabilità in uscita x [11]. Il concetto di disordine può essere a questo punto facilmente legato a quello di *entropia.* Definiamo *Schur convessa* una funzione $f(\cdot)$, a valori reali, che preserva la relazione di maggiorizzazione, nel senso che se $x \prec y$ allora

$f(x) \leq f(y)$. Molte interessanti funzioni sono Schur convesse; ad esempio la funzione $x \mapsto f(x) = \sum_{j=1}^{d} x_j^k$, $\forall k \geq 1$. Allo stesso modo, una funzione $f(\cdot)$ è *Schur concava* se per $x \prec y$ allora $f(x) \geq f(y)$. Equivalentemente, $f(\cdot)$ è Schur concava se $-f(\cdot)$ è Schur convessa. L' esempio canonico di una funzione Schur concava è proprio l'entropia di Shannon $H(x) = -\sum_j x_j \log_2(x_j)$, tale che se $x \prec y$ allora $H(x) \geq H(y)$. Questa relazione giustifica l'intuitivo significato attribuito a $x \prec y$, esprime realmente il fatto che x è più disordinato di y.
La connessione tra teoria della maggiorizzazione e meccanica quantistica si presenta principalmente come conseguenza del *lemma di Horn* [12]. Definiamo *stocastica-unitaria* ogni matrice D le cui componenti possono essere scritte nella forma $D_{ij} = |u_{ij}|^2$ per qualche matrice unitaria $u = (u_{ij})_{ij}$. Il legame tra queste matrici e la maggiorizzazione è fornito dal seguente

Teorema 4.2 (lemma di Horn) *Siano x e y due vettori d-dimensionali. Allora $x \prec y$ se e solo se esiste una matrice unitaria- stocastica D tale che $x = Dy$.* □

Per dare un'idea intuitiva della dimostrazione, diciamo che è possibile, dati $x \prec y$, costruire esplicitamente una matrice unitaria $u = (u_{ij})_{ij}$ tale che $x = Dy$, dove $D_{ij} = |u_{ij}|^2$. In realtà, per questa implicazione diretta, sarebbe sufficiente considerare solo matrici ortogonali u, *i.e.* matrici reali tali che $uu^T = u^T u = \mathbb{I}$, dove $(\cdot)^T$ indica la matrice trasposta. La matrice corrispondente $D_{ij} = u_{ij}^2$ è detta *ortostocastica.* Per l'implicazione inversa bisogna usare la decomposizione $x = T_1 T_2 \ldots T_n y$, dopo aver dimostrato che $x \prec y$ se e solo se esiste un insieme finito $(T_1, T_2, ..., T_n)$ di T-trasformazioni[1]. Questa fondamentale relazione tra maggiorizzazione e unitarietà assicura molte connessioni tra maggiorizzazione e meccanica quantistica.

[1]Una trasformazione T è una matrice che agisce come l'identità ovunque tranne che in un sottospazio bidimensionale, dove ha la forma

$$T = \begin{pmatrix} t & 1-t \\ 1-t & t \end{pmatrix}$$

per qualche parametro t, $0 \leq t \leq 1$

Conseguenza elementare del lemma di Horn è il *Ky Fan's maximum principle* [11], secondo il quale per ogni matrice hermitiana A, la somma dei k autovalori più grandi di A [2] è il valore massimo di $\mathrm{Tr}(AP)$, dove il massimo è preso su tutti i proiettori k-dimensionali P,

$$\sum_{j=1}^{k} \lambda_j(A) = \max_P \mathrm{Tr}(AP). \tag{4.3}$$

Infatti, scegliendo P come il proiettore sullo spazio spannato dai k autovettori di A con i k autovalori più grandi, risulta $\mathrm{Tr}(AP) = \sum_{j=1}^{k} \lambda_j(A)$. La dimostrazione del Ky Fan's maximum principle è a questo punto completata se dimostriamo che $\mathrm{Tr}(AP) \leq \sum_{j=1}^{k} \lambda_j(A)$ per ogni proiettore k-dimensionale P. Siano $(|e_1\rangle, \ldots, |e_d\rangle)$ una base ortonormale tale che $P = \sum_{j-1}^{k} |e_j\rangle\langle e_j|$ e $(|f_1\rangle, \ldots, |f_d\rangle)$ un insieme ortonormale di autovettori di A, ordinati in modo che i corrispondenti autovalori siano in ordine non- crescente. Allora

$$\langle e_j|A|e_i\rangle = \sum_{k=1}^{d} |u_{jk}|^2 \lambda_k(A), \tag{4.4}$$

dove $u_{jk} \equiv \langle e_j|f_k\rangle$ è unitario. Dal lemma di Horn segue che $(\langle e_j|A|e_i\rangle) \prec \lambda(A)$, e quindi

$$\mathrm{Tr}(AP) = \langle e_j|A|e_i\rangle \leq \sum_{j=1}^{k} \lambda_j(A), \tag{4.5}$$

come richiesto.

Dal Ky Fan's maximum principle deriva un'utile condizione sugli autovalori della somma di due matrici hermitiane, *i.e.* $\lambda(A+B) \leq \lambda(A)+\lambda(B)$. Infatti, scegliamo un proiettore P k-dimensionale tale che

$$\begin{aligned}
\sum_{j=1}^{k} \lambda_j(A+B) &= \mathrm{Tr}\left((A+B)P\right. \\
&= \mathrm{Tr}(AP) + \mathrm{Tr}(BP) \\
&\leq \sum_{j=1}^{k} \lambda_j(A) + \sum_{j=1}^{k} \lambda_j(B),
\end{aligned} \tag{4.6}$$

[2] $\lambda(X)$ denota il vettore degli autovalori della matrice X posti in ordine non-crescente

dove l'ultimo passaggio segue dal Ky Fan's maximum principle.
Un'altra conseguenza [12] del lemma di Horn è che, date una matrice densità ρ e una distribuzione di probabilità p_i, allora esistono stati puri $|\psi_i\rangle$ tali che $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ se e solo se $(p_i) \prec \lambda(\rho)$.
L'ultimo risultato che proponiamo è che se $(P_i)_i$ è un insieme di proiettori ortogonali tali che $\sum_i P_i = \mathbb{I}$, e ρ è una matrice densità, allora

$$\lambda\Big(\sum_i P_i \rho P_i\Big) \prec \lambda(\rho). \tag{4.7}$$

Intuitivamente, se viene fatta una misura proiettiva su un sistema quantistico, ma non conosciamo il risultato della misura, allora lo stato del sistema dopo la misura è più disordinato di quello prima. Un modo di dimostrare questo teorema è con il lemma di Horn: notiamo innanzitutto che è sufficiente dimostrare che $\lambda(P\rho P + Q\rho Q) \prec \lambda(\rho)$, dove P e Q sono due proiettori ortogonali tali che $P + Q = \mathbb{I}$. Verificato ciò, la relazione (4.7) segue da un semplice calcolo. Comunque, se definiamo una matrice unitaria $U = P - Q$, allora è facile verificare che

$$P\rho P + Q\rho Q = \frac{\rho + U\rho U^\dagger}{2}.$$

Applicando il lemma di Horn si vede che se $x_1 \prec y$ e $x_2 \prec y$, allora $(x_1 + x_2)/2 \prec y$; segue con semplice algebra lineare che $\lambda(P\rho P + Q\rho Q) \prec \lambda(\rho)$.

Capitolo 5

Introduzione alla teoria dei frames

La *teoria dei frames* per uno spazio di Hilbert $\mathcal{H}$ gioca un ruolo fondamentale nei *signal processing*, *image processing*, *data compression* e *sampling theory*, oltre ad essere una ricchissima area di ricerca in matematica astratta. Nella prima parte di questa breve introduzione, forniremo definizioni e teoremi basilari per la descrizione della teoria astratta dei frames [13], con particolare attenzione alla loro interpretazione come operatori. Nelle seconda svilupperemo il legame esistente tra teoria dei frames e formalismo delle POVMs [16].

5.1 Definizioni e teoremi principali

Relativamente all'analisi delle trasformate di Fourier, nel 1946, D.Gabor formulò un fondamentale approccio alla decomposizione dei segnali tramite segnali elementari. Questo approccio diventò un paradigma per l'analisi spettrale associata a metodi tempo-frequenza e diede virtualmente il via alla teoria dei frames.
I frames per uno spazio di Hilbert furono poi formalmente definiti da Duffin e Schaeffer nel 1952, col fine di studiare le serie di Fourier non armoniche. Il la-

voro di Duffin e Schaeffer, astraendo le idee di Gabor per il *signal processing*, li portò alla seguente definizione.

Definizione 5.1 *Una sequenza* $(f_n)_{n\in\mathbb{Z}}$ *di elementi di uno spazio di Hilbert* $\mathcal{H}$ *è detta* **frame** *se esistono due costanti* $A, B > 0$ *tali che*

$$A\|f\|^2 \leq \sum_{n\in\mathbb{Z}} |\langle f, f_n\rangle|^2 \leq B\|f\|^2, \quad \forall f \in \mathcal{H}. \tag{5.1}$$

I numeri A, B della Definizione 5.1 sono rispettivamente chiamati *limite superiore* e *inferiore* del frame. Il più grande numero $A > 0$ e il più piccolo $B > 0$ che soddisfino la disuguaglianza (5.1) sono detti *limiti ottimali* del frame. Il limite inferiore A assicura che i vettori f_n spannino $\mathcal{H}$.

Nota. Nel caso in cui si consideri uno spazio di Hilbert m-dimensionale $\mathcal{H}_m$, si ha

$$A\|f\|^2 \leq \sum_{n=1}^{N} |\langle f, f_n\rangle|^2 \leq B\|f\|^2, \quad \forall f \in \mathcal{H}_m. \tag{5.2}$$

Quindi, affinchè gli f_n spaninno $\mathcal{H}_m$, dobbiamo richiedere che $N \geq m$. In questo caso abbiamo $N < \infty$: la disuguaglianza di destra risulta sempre soddisfatta con $B = \sum_{n=1}^{N}\langle f_n, f_n\rangle$. Allora ogni insieme finito di vettori che spannano $\mathcal{H}_m$ è un frame per $\mathcal{H}_m$. In particolare ogni base per $\mathcal{H}_m$ è un frame per $\mathcal{H}_m$. È fondamentale notare però, che a differenza dei vettori di base, che sono linearmente indipendenti, i vettori del frame con $N \geq m$ sono linearmente dipendenti.

Il frame è detto *tight frame* se $A = B$, e *tight frame normalizzato* se $A = B = 1$. Un frame è *esatto* se non risulta più tale quando viene rimosso uno dei suoi elementi. Come vedremo un frame è esatto se e solo se è una base di Riesz [1]. Un frame non esatto è chiamato *overcompleto* nel senso che almeno

[1]Introduciamo alcune basilari definizioni:

- Una sequenza (x_i) che spanna $\mathcal{H}$ è una *base di Schauder* (o *base*) per $\mathcal{H}$ se ogni elemento $x \in \mathcal{H}$ ha un'unica rappresentazione $x = \sum_i a_i x_i$, dove (a_i) è una sequenza di scalari.
- La base (x_i) è *limitata* se $\exists M > 0$ tale che $M^{-1} \leq \|x_i\| \leq M \quad \forall\, i$.

un vettore può essere tolto dal frame e il rimanente insieme di vettori è ancora un frame, magari con limiti diversi.

Risulta evidente come ogni base ortonormale (e_n) di $\mathcal{H}$ sia un tight frame normalizzato per $\mathcal{H}$. Anche le seguenti sequenze di vettori sono tight frames normalizzati per $\mathcal{H}$:

$$\{e_1, 0, e_2, 0, e_3, 0, \ldots\},$$

$$\{\frac{e_1}{\sqrt{2}}, \frac{e_1}{\sqrt{2}}, \frac{e_2}{\sqrt{2}}, \frac{e_2}{\sqrt{2}}, \ldots\},$$

$$\{e_1, \frac{e_2}{\sqrt{2}}, \frac{e_2}{\sqrt{2}}, \frac{e_3}{\sqrt{3}}, \frac{e_3}{\sqrt{3}}, \frac{e_3}{\sqrt{3}}, \ldots\}.$$

Se (f_n) è una qualsiasi sequenza con un limite superiore di frame finito, allora (e_n, f_n) è un frame per $\mathcal{H}$. Ovviamente (e_n/n) non ha un limite inferiore di frame, mentre (ne_n) non ha quello superiore.

Un utile approccio della teoria dei frames per spazi di Hilbert infinito dimensionali, è quello di vedere i frames come operatori [14]. Prendiamo una base ortonormale (e_n) di $\mathcal{H}$ infinito dimensionale e una sequenza (f_n) di vettori $\in \mathcal{H}$, $\forall n \in \mathbb{Z}$. Chiamiamo *operatore preframe* associato ad (f_n) l'operatore $T : \mathcal{H} \to \mathcal{H}$, tale che $Te_n = f_n$. Per ogni $f \in \mathcal{H}$ e $n \in \mathbb{Z}$, abbiamo $\langle T^\dagger f, e_n \rangle = \langle f, Te_n \rangle = \langle f, f_n \rangle$. Allora

$$T^\dagger f = \sum_n \langle f, f_n \rangle e_n, \quad \forall\, f \in \mathcal{H}. \tag{5.3}$$

Segue che l'operatore preframe è limitato[2] se e solo se (f_n) ha un limite superiore di frame B finito. Dalla (5.3) segue

$$\|T^\dagger f\|^2 = \sum_n |\langle f, f_n \rangle|^2, \quad \forall\, f \in \mathcal{H}.$$

La definizione di frame, in questa nuova ottica, ci porta al seguente teorema.

- Una *base di Riesz* per $\mathcal{H}$ è una base limitata e incondizionata (*i.e.* nella serie $\sum_i a_i x_i$, ogni riarrangiamento di $a_i x_i$ converge ad x, $\forall x \in \mathcal{H}$) per $\mathcal{H}$.

[2] T è limitato se $\|T\| = \sup_{0 \neq x \in \mathcal{H}} \frac{\|Tx\|}{\|x\|} < \infty$

Teorema 5.1 *Sia $\mathcal{H}$ uno spazio di Hilbert con una base ortonormale (e_n). Siano poi (f_n) una sequenza di elementi di $\mathcal{H}$ e T, tale che $Te_n = f_n$, l'operatore preframe. Le seguenti affermazioni sono equivalenti:*

(1) (f_n) è un frame per $\mathcal{H}$.

(2) L'operatore T è limitato, lineare e suriettivo (i.e. $\operatorname{Rng} T = \mathcal{H}$)

(3) L'operatore $T^\dagger$ è un isomorfismo (i.e. iniettivo, continuo e con un inverso T^{-1}, definito sul $\operatorname{Rng} T$, continuo), chiamato trasformazione di frame.

Inoltre, (f_n) è un tight frame normalizato se e solo se l'operatore preframe è un'isometria parziale[3]. □

Dalle condizioni (1) e (2) segue che l'operatore $S = TT^\dagger$ è invertibile (isomorfismo suriettivo) in $\mathcal{H}$, ed è chiamato *operatore di frame*. Si ha inoltre che:

$$Sf = TT^\dagger f = T\left(\sum_n \langle f, f_n\rangle e_n\right) = \sum_n \langle f, f_n\rangle Te_n = \sum_n \langle f, f_n\rangle f_n.$$

Con un semplice calcolo si ottiene:

$$\langle Sf, f\rangle = \sum_n |\langle f, f_n\rangle|^2.$$

Quindi l'operatore di frame risulta positivo, hermitiano e invertibile in $\mathcal{H}$. La disuguaglianza (5.1) comporta che (f_n) è un frame con limiti $A, B > 0$ se e solo se $A \cdot \mathbb{I} \le S \le B \cdot \mathbb{I}$. Quindi (f_n) è un tight frame normalizzato se e solo se $S = \mathbb{I}$. Si verifica che:

$$f = SS^{-1}f = \sum_n \langle S^{-1}f, f_n\rangle f_n = \sum_n \langle f, S^{-1}f_n\rangle f_n = \sum_n \langle f, S^{-1/2}f_n\rangle S^{-1/2} f_n. \tag{5.4}$$

Chiamiamo i $(\langle S^{-1}f, f_n\rangle)$ *coefficienti di frame* per f. Segue che

[3] T è un'isometria se $\|Tx\|_{\mathcal{H}} = \|x\|_{\mathcal{H}}$. T è un'isometria parziale se è un'isometria nel complemento ortogonale del suo kernel ($\operatorname{Ker} T = \{x : Tx = 0\}$)

Teorema 5.2 *Ogni frame* (f_n)*, con operatore di frame* S*, è equivalente al tight frame normalizzato* $(S^{-1/2}f_n)$. $\square$

Notiamo che l'equazione (5.4) è una formula di ricostruzione per un elemento $\in \mathcal{H}$. Questo metto alla luce uno dei maggiori problemi nell'applicazione della teoria dei frame. Per ricostruire un vettore bisogna conoscere i suoi coefficienti di frame, *i.e.* trovare $S^{-1}f$: ciò equivale ad invertire una matrice di dimensione infinita, compito molto arduo.
Visto che S è un isomorfismo in $\mathcal{H}$, $(S^{-1}f_n)$ è un frame equivalente al frame (f_n) e viene chiamato *frame duale (canonico)*.

Nota. Questo approccio alla teoria dei frames per spazi infinito dimensionali, vale anche, con piccole variazioni, per dimensione finita. Una sequenza (f_n) in uno spazio di Hilbert m-dimensionale $\mathcal{H}_m$ è un frame se e solo se l'operatore $T : l_2 \to \mathcal{H}_m$, dato da $Te_n = f_n$, dove (e_n) è una base ortonormale di l_2, è lineare, limitato e suriettivo.

La proposizione seguente mostra il legame esistente tra gli elementi e i limiti del frame.

Proposizione 5.1 *Sia* (f_n) *un frame per* $\mathcal{H}$ *con limiti di frame* A, B*. Si ha che* $\forall\, n \in \mathbb{Z}$*,* $\|f_n\|^2 \leq B$*.* $\|f_n\|^2 = B$ *implica che* $f_n \perp \operatorname{span}_{j\neq n}(f_j)$*. Se* $\|f_n\|^2 \leq A$ *allora* $f_n \in \overline{\operatorname{span}}_{j\neq n}(f_j)$. $\square$

Come caso particolare della Proposizione 5.1, abbiamo che per un tight frame normalizzato (f_n), $\|f_n\|^2 \leq 1$ e che $\|f_n\| = 1$ se e solo se $f_n \perp \operatorname{span}_{j\neq n}(f_j)$. Se (f_n) è un frame esatto, allora $\langle S^{-1}f_n, f_m\rangle = \langle S^{-1/2}f_n, S^{-1/2}f_m\rangle = \delta_{nm}$, poichè $(S^{-1/2}f_n)$ è una base ortonormale per $\mathcal{H}$. Cioè $(S^{-1/2}f_n)$ e (f_n) formano un sistema biortogonale.
Segue che (e_n) è una base ortonormale per $\mathcal{H}$ se e solo se è un tight frame esatto e normalizzato.

Proposizione 5.2 *Sia* (f_n) *un frame per* $\mathcal{H}$ *con limiti di frame* A, B*, e sia* P *un proiettore ortogonale su* $\mathcal{H}$*. Allora* (Pf_n) *è un frame per* $P(\mathcal{H})$ *con limiti* A, B. $\square$

Dimostrazione. Per ogni $f \in P(\mathcal{H})$ abbiamo

$$\sum_n |\langle f, Pf_n\rangle|^2 = \sum_n |\langle Pf, f_n\rangle|^2 = \sum_n |\langle f, f_n\rangle|^2.$$

Il risultato è a questo punto immediato dalla Definizione 5.1. ■

Segue che un proiettore ortogonale P fatto agire su una base ortonormale (e_n) (o su un tight frame normalizzato) genera un tight frame normalizzato (Pe_n) per $P(\mathcal{H})$. Ma è vero anche il contrario [14].

Teorema 5.3 *Una sequenza (f_n) è un tight frame normalizzato per uno spazio di Hilbert $\mathcal{H}$ se e solo se $\exists$ uno spazio di Hilbert $\mathcal{K} \supset \mathcal{H}$ e una base ortonormale (e_n) per $\mathcal{K}$ tali che il proiettore ortogonale $P_{\mathcal{H}}$ di $\mathcal{K}$ in $\mathcal{H}$ soddisfi $Pe_n = f_n \quad \forall n = 1, 2, \ldots$.* □

Dimostrazione. Per la Proposizione 5.2, la condizione è necessaria. Perchè sia sufficiente, consideriamo un tight frame normalizzato (f_n) per $\mathcal{H}$, quindi l'operatore preframe $T : l_2 \to \mathcal{H}_m$ è un'isometria parziale. Sia (e_n) una base ortonormale per l_2, $Te_n = f_n$ risulta allora il nostro frame. Poichè $T^\dagger$ è un'isometria iniettiva, possiamo associare $\mathcal{H}$ a $T^\dagger(\mathcal{H})$. Siano ora $\mathcal{K} = l_2$ e P il proiettore ortogonale di $\mathcal{K}$ in $T^\dagger(\mathcal{H})$. Allora $\forall n = 1, 2, \ldots$ e $\forall g = T^\dagger f \in T^\dagger(\mathcal{H})$, si ha:

$$\langle T^\dagger f, Pe_n\rangle = \langle T^\dagger f, e_n\rangle = \langle f, Te_n\rangle = \langle f, f_n\rangle = \langle T^\dagger f, T^\dagger f_n\rangle.$$

Quindi $Pe_n = T^\dagger f_n$, e data l'associazione di $\mathcal{H}$ a $T^\dagger(\mathcal{H})$, $(T^\dagger f_n)$ è un frame. ■

Esiste una generalizzazione del Teorema 5.3 secondo la quale è sufficiente prendere un proiettore $P : \mathcal{K} \to \mathcal{H}$, e non necessariamente uno ortogonale.

Un'altra interessante conseguenza del considerare i frames come operatori, nel caso finito dimensionale, è la seguente proposizione.

Proposizione 5.3 *Se (f_n) è un tight frame normalizzato per uno spazio di Hilbert m-dimensionale $\mathcal{H}_m$, allora*

$$\sum_n \|f_n\|^2 = m.$$

Quindi se (f_n) *è un tight frame normalizzato per un* $\mathcal{H}$ *infinito dimensionale, per tutti i proiettori ortogonali* P *di rango finito in* $\mathcal{H}$*, si ha che:*

$$\sum_n \|Pf_n\|^2 = i \in \mathbb{N}$$

$\square$

Dimostrazione. Per il Teorema 5.3, $\exists\, \mathcal{K} \supset \mathcal{H}$ e un proiettore ortogonale P che porta una base ortonormale (e_n) di $\mathcal{H}$ in $Pe_n = f_n$. Quindi

$$\sum_n \|f_n\|^2 = \sum_n \|Pe_n\|^2 = \|P\|_{HS}^2 = \dim \mathcal{H}_m = m,$$

dove $\|\cdot\|_{HS}$ è la norma di Hilbert-Schmidt. $\blacksquare$

Ancora nel caso infinito dimensionale, trattare i frames come operatori permette di decomporli in "oggetti migliori", ad esempio in [15] si dimostra che ogni frame può essere scritto come somma di tre basi ortonormali. Questa è una conseguenza del seguente teorema nella teoria degli operatori.

Teorema 5.4 *Ogni operatore limitato* T *in uno spazio di Hilbert complesso* $\mathcal{H}$ *infinito dimensionale può essere scritto come* $T = a(U_1 + U_2 + U_3)$*, dove ogni* U_j *è un operatore unitario e* a *è un numero reale e positivo.* $\square$

Dimostrazione. Fissiamo $0 < \epsilon < 1$ e consideriamo

$$S = \frac{1}{2}\mathbb{I} + \frac{1-\epsilon}{2}\frac{T}{\|T\|}.$$

Si dimostra che $\|\mathbb{I} - S\| < 1$, quindi S è un operatore invertibile. Se scriviamo la decomposizione polare di S come $S = VP$, visto che S è invertibile, V è un operatore unitario. Possiamo anche scrivere [18] $P = \frac{1}{2}(W + W^\dagger)$, dove W, $W^\dagger$ sono unitari. Quindi $S = \frac{1}{2}(VW + VW^\dagger)$, dove VW, $VW^\dagger$ sono unitari. Infine

$$T = \frac{\|T\|}{1-\epsilon}(VW + VW^\dagger - \mathbb{I}),$$

somma di tre unitari. $\blacksquare$

È stato osservato [15] che un operatore lineare, limitato e suriettivo in $\mathcal{H}$ può essere scritto come combinazione lineare di due operatori unitari se e solo se è invertibile. Il Teorema 5.4 e l'osservazione precedente diventano per i frames:

Teorema 5.5 *Ogni frame (in uno spazio di Hilbert complesso $\mathcal{H}$ infinito dimensionale) è (un multiplo del) la somma di tre basi ortonormali. Inoltre, un frame è la combinazione lineare di due basi ortonormali se e solo se è una base di Riesz.* □

Se indeboliamo la richiesta sugli oggetti in cui decomporre un frame, si dimostra [15] che ogni frame è la somma di due tight frames normalizzati, o di una base ortonormale e una di Riesz.

Come abbiamo visto, se (f_n) è un frame con operatore di frame S, allora $(S^{-1}f_n)$ è un frame chiamato *frame duale*. Se poi $g_n = S^{-1}f_n$, allora per la (5.4) si ha:

$$f = \sum_n \langle f, g_n \rangle f_n, \quad \forall f \in \mathcal{H}. \tag{5.5}$$

Sfruttando la (5.5) definiamo:

Definizione 5.2 *Se (f_n) è un frame per $\mathcal{H}$, un frame (h_n) per $\mathcal{H}$ è detto* frame pseudo-duale *per f_n se*

$$f = \sum_n \langle f, h_n \rangle f_n, \quad \forall f \in \mathcal{H}. \tag{5.6}$$

$(S^{-1}f_n)$ diventa allora *frame duale canonico* di f_n. Se (f_n) è un tight frame normalizzato, $S = \mathbb{I}$ e quindi il frame è uguale al suo duale canonico. Vale ovviamente anche l'inverso. In generale comunque, un frame può avere molti frames duali associati.

Esempio. Consideriamo il frame $\{e_1, e_1, e_2, e_2, \ldots\}$ dove (e_n) è una base ortonormale per $\mathcal{H}$. I seguenti sono entrambi pseudo-duali per questo frame:

$$\{e_1, 0, e_2, 0, e_3, 0, \ldots\},$$

$$\{0, e_1, 0, e_2, 0, e_3, \ldots\}.$$

Il frame duale canonico risulta

$$\{e_1/2, e_1/2, e_2/2, e_2/2, \ldots\}.$$

Nella Definizione 5.2 assumiamo che la sequenza (h_n) sia un frame per $\mathcal{H}$. Il motivo è che esistono sequenze che soddisfano la (5.6) ma non sono frames. Ad esempio

$$\left\{e_1, \frac{e_2}{\sqrt{2}}, \frac{e_2}{\sqrt{2}}, \frac{e_3}{\sqrt{3}}, \frac{e_3}{\sqrt{3}}, \frac{e_3}{\sqrt{3}}, \ldots\right\}$$

è un tight frame normalizzato per $\mathcal{H}$ e la sequenza non-frame

$$\{e_1, \sqrt{2}e_2, 0, \sqrt{3}e_3, 0, 0, \sqrt{4}e_4, 0, \ldots\}$$

soddisfa la (5.6).

5.2 Frames e POVMs

I tight frames e le misurazioni quantistiche di rango 1 sono intimamente correlate: la famiglia dei tight frames normalizzati per lo spazio in cui giace un sistema quantistico coincide, infatti, con quella delle POVMs i cui elementi di rango 1 siano definiti su tale spazio. Nella prima parte definiamo le matrici di misurazione associate alle POVM e riprendiamo il teorema di Neumark in questa nuova rappresentazione. Passiamo quindi al problema dell'ottimizzazione delle misurazioni nel caso di stati puri non ortogonali. Nella seconda parte, la sequenza precedente viene affrontata per i tight frames: associamo ad ognuno di essi una matrice di frame, derivando poi un analogo del teorema di Neumark per i tight frames. Forniamo, infine, le direttive principali per la costruzione di tight frames ottimali per un sottospazio $\mathcal{U}$ dato un insieme di vettori che spannano $\mathcal{U}$. Faremo riferimento, per questa parte, all'articolo [16]

5.2.1 Matrici di misurazione e ottimizzazione

Abbiamo già caratterizzato le POVMs nel Capitolo 1; associamo ora ad ogni POVM $\mathbf{\Pi}$ costituita da elementi Π_i, con $\mathrm{Rng}(\Pi_i) = 1 \ \forall i$, una *matrice di misurazione*. Consideriamo la POVM $\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_n)$, con $\mathrm{Rng}(\Pi_i) = 1 \ \forall i$, agente nel sottospazio r-dimensionale $\mathcal{U} \subseteq \mathcal{H}$ dove si trova il sistema che deve essere misurato. La POVM è definita da un insieme di n vettori di misurazione $\{|u_i\rangle, 1 \leq i \leq n\}$ che soddisfano la relazione di completezza

$$\sum_{i=1}^{n} |u_i\rangle\langle u_i| = P_{\mathcal{U}} \tag{5.7}$$

i.e., gli operatori $\Pi_i = |u_i\rangle\langle u_i|$ devono essere una risoluzione dell'identità in $\mathcal{U}$. La *matrice di misurazione* M corrispondente ad un insieme di vettori di misurazione $|u_i\rangle \in \mathcal{U}$ è definita come la matrice ottenuta accostando gli n vettori colonna $|u_i\rangle$ [17]. Si ha dunque

$$MM^\dagger = P_{\mathcal{U}}. \tag{5.8}$$

Quindi una matrice M con n colonne in $\mathcal{H}$ è una matrice di misurazione per gli stati nel sottospazio $\mathcal{U} \subseteq \mathcal{H}$ se e solo se M soddisfa la (5.8). Riassumiamo le propietà delle matrici di misurazione nel seguente teorema

Teorema 5.6 *Le seguenti proposizioni sono equivalenti per una matrice M le cui colonne siano n vettori in uno spazio di Hilbert complesso $\mathcal{H}$:*

1. *M è una matrice di misurazione corrispondente ad una POVM con elementi di rango 1 in un sottospazio $\mathcal{U} \subseteq \mathcal{H}$;*
2. *M è una isometria parziale*[4] *tra i sottospazi r-dimensionali $\mathcal{U} \subseteq \mathcal{H}$ e $\mathcal{V} \subseteq \mathbb{C}^n$;*
3. *$MM^\dagger = P_{\mathcal{U}}$ per un sottospazio r-dimensionale $\mathcal{U} \subseteq \mathcal{H}$;*

[4] Equivalentemente alla definizione precedentemente data, possiamo dire che una matrice M di rango r è un'isometria parziale se i suoi valori singolari diversi da zero sono tutti uguali a 1

4. $M^\dagger M = P_{\mathcal{V}}$ *per un sottospazio* r*-dimensionale* $\mathcal{V} \subseteq \mathbb{C}^n$.

Una matrice di misurazione M*, corrispondente ad una POVM con elementi di rango 1 agenti in un sottospazio* r*-dimensionale* $\mathcal{U} \subseteq \mathcal{H}$*, può essere espressa come* $M = UZ_rV^\dagger$*, dove* U *è una matrice unitaria le cui prime* r *colonne* $\{|u_i\rangle\, 1 \leq i \leq r\}$ *sono una base ortonormale per* $\mathcal{U}$*,* V *è una matrice* $n \times n$ *unitaria le cui prime* r *colonne* $\{|v_i\rangle\, 1 \leq i \leq r\}$ *sono una base ortonormale per* $\mathcal{V}$*, e* Z_r *è la matrice con tutti i valori singolari diversi da zero uguali a 1. Equivalentemente,* $M = \sum_{i=1}^{r} |u_i\rangle\langle v_i|$.

Una matrice di misurazione M *è un'isometria se ristretta a* $\mathcal{V}$.

Una matrice di misurazione M*, le cui colonne sono* n *vettori in* $\mathcal{H}$*, rappresenta una misurazione di Von-Neumann (proiettiva) se e solo se ha rango* n*. In questo caso* $M = UZ_nV^\dagger$*, con* $M^\dagger M = \mathbb{I}_n$. □

Abbiamo già discusso del teorema di Neumark [3], sempre nel Capitolo 1. Ne diamo qui di seguito una versione adattata alle matrici di misurazione: lo useremo poi per estendere un tight frame ad una base ortonormale in uno spazio più grande.

Teorema 5.7 (Neumark) *Sia* M *una matrice di misurazione di rango* r*, corrispondente ad una generica POVM, con* n *colonne in uno spazio di Hilbert complesso* $\mathcal{H}$*. In altre parole,* M *è un'isometria parziale tra i sottospazi* r*-dimensionali* $\mathcal{U} \subseteq \mathcal{H}$ *e* $\mathcal{V} \subseteq \mathbb{C}^n$*. Allora esiste una misura proiettiva (di Von Neumann) con matrice di misurazione* $\widetilde{M}$ *che è un'isometria parziale tra un sottospazio allargato* $\widetilde{\mathcal{U}} \supseteq \mathcal{U}$*, in uno spazio di Hilbert complesso allargato* $\widetilde{\mathcal{H}} \supseteq \mathcal{H}$*, e* $\mathbb{C}^n$*, tale che* $M = P_{\mathcal{U}}\widetilde{M}$. □

Descriviamo ora alcuni risultati relativi all'ottimizzazione delle misurazioni quantistiche, secondo diversi criteri. Sia $\{|\psi_i\rangle\,, 1 \leq i \leq n\}$ un insieme di $n \leq k$ vettori normalizzati $|\psi_i\rangle$ in uno spazio di Hilbert complesso k-dimensionale $\mathcal{H}$ e rappresentino le differenti preparazioni di un sistema quantistico. In generale questi vettori non sono ortogonali e spannano uno spazio r-dimensionale $\mathcal{U} \subset \mathcal{H}$. Supponiamo che per distinguere tra le diverse preparazioni si usino POVMs $\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_n)$ con $\operatorname{Rng}\Pi_i = 1$ e

$\Pi_i = |u_i\rangle\langle u_i|$, dove i vettori di misurazione $|u_i\rangle \in \mathcal{U}$ e soddisfano la condizione di completezza $\sum_i |u_i\rangle\langle u_i| = P_{\mathcal{U}}$. Se gli stati sono preparati con uguale probabilità a priori, allora la probabilità di commettere un errore usando i vettori di misurazione $|u_i\rangle$ è data da

$$P_e = 1 - \frac{1}{n}\sum_{i=1}^{n} |\langle u_i|\psi_i\rangle|^2.$$

Se i vettori u_i sono ortonormali, allora scegliendo $|u_i\rangle = |\psi_i\rangle$, risulterebbe $P_e = 0$. Se però tali vettori non sono ortonormali, allora nessuna misurazione può discriminare con certezza tra di essi. Ed è proprio questo il problema: costruire misurazioni ottimizzate per distinguere tra un insieme di stati puri non ortogonali (*quantum detection problem*). Il criterio di ottimizzazione che poi useremo anche per i frames, è quello dello *squared-error* che consiste nel realizzare il $(\min_{|u_i\rangle} \sum_i \||\psi_i\rangle - |u_i\rangle\|^2)$ [17]. La misurazione in questo senso ottimale è detta *least-squares measurement* (LSM).

5.2.2 Matrici di frame e tight frames ottimizzati

Utilizzeremo la notazione di Dirac anche per i vettori di un frame. Dalla Definizione 5.2, sappiamo che i vettori $\{|\varphi_i\rangle, 1 \leq i \leq n\}$ in un sottospazio r-dimensionale $\mathcal{U} \subseteq \mathcal{H}$ formano un tight frame se $\exists\, B > 0$ tale che

$$\sum_{i=1}^{n} |\langle x|\varphi_i\rangle|^2 = B^2\||x\rangle\|^2, \quad \forall |x\rangle \in \mathcal{U}. \tag{5.9}$$

Se poi $B = 1$, il tight frame è detto normalizzato, altrimenti $B-$*scaled*. Visto che

$$\sum_{i=1}^{n} |\langle x|\varphi_i\rangle|^2 = \sum_{i=1}^{n}\langle x|\varphi_i\rangle\langle\varphi_i|x\rangle = \langle x|\Big(\sum_i |\varphi_i\rangle\langle\varphi_i|\Big)x\rangle, \tag{5.10}$$

il fatto che la (5.9) valga $\forall\,|x\rangle \in \mathcal{U}$ implica che

$$\sum_i |\varphi_i\rangle\langle\varphi_i| = B^2 P_{\mathcal{U}} \tag{5.11}$$

Vale anche l'implicazione inversa, cioè se i vettori $|\varphi_i\rangle \in \mathcal{U}$ soddisfano la (5.11), allora (5.10) implica che (5.9) valga $\forall\,|x\rangle \in \mathcal{U}$. Possiamo dunque concludere che un insieme di n vettori $|\varphi_i\rangle \in \mathcal{U}$ formano un tight frame per $\mathcal{U}$ se e solo se soddisfano la (5.11) per qualche $B > 0$.
Confrontando la (5.11) con la (5.7), concludiamo che:

Teorema 5.8 *Un insieme di vettori $|\varphi_i\rangle \in \mathcal{U}$ forma un tight frame B-scaled per $\mathcal{U}$ se e solo se i vettori riscalati $B^{-1}|\varphi_i\rangle$ sono i vettori di misurazione di un POVM $\mathbf{\Pi}$ con elementi di rango 1 su $\mathcal{U}$. In particolare, i vettori $|\varphi_i\rangle$ formano un tight frame normalizzato per $\mathcal{U}$ se e solo se risultano essere i vettori di misurazione della POVM $\mathbf{\Pi}$.* □

Questa fondamentale relazione tra misurazioni quantistiche e tight frames ci permette di definire ora le matrici di frame in analogia alle matrici di misurazione precedentemente introdotte. Useremo poi il teorema di Neumark per estendere i tight frames alle basi ortogonali. Affronteremo infine il problema della costruzione di tight frames ottimali.

Definiamo le matrici F di frame come le matrici ottenute accostando le colonne $|\varphi_i\rangle$, dove i vettori $|\varphi_i\rangle$ formano un tight frame per $\mathcal{U}$. Dalla (5.11) segue che

$$FF^\dagger = B^2 P_{\mathcal{U}} \tag{5.12}$$

Le proprietà delle matrici di frame seguono dal Teorema 5.8 e dal Teorema 5.6 :

Teorema 5.9 *Per una matrice F le cui colonne siano n vettori in uno spazio di Hilbert complesso $\mathcal{H}$ e per una costante $B > 0$, le seguenti proposizioni sono equivalenti:*

1. *F è una matrice di frame di un B-scaled tight frame in un sottospazio r-dimensionale $\mathcal{U} \subseteq \mathcal{H}$;*

2. *$B^{-1}F$ è una isometria parziale tra i sottospazi r-dimensionali $\mathcal{U} \subseteq \mathcal{H}$ e $\mathcal{V} \subseteq \mathbb{C}^n$;*

3. $FF^\dagger = B^2 P_{\mathcal{U}}$ *per un sottospazio r-dimensionale* $\mathcal{U} \subseteq \mathcal{H}$*;*

4. $F^\dagger F = B^2 P_{\mathcal{V}}$ *per un sottospazio r-dimensionale* $\mathcal{V} \subseteq \mathbb{C}^n$*.*

Una matrice di misurazione F di un B-scaled tight frame per un sottospazio r-dimensionale $\mathcal{U} \subseteq \mathcal{H}$*, può essere espressa come* $F = BUZ_rV^\dagger$*, dove U è una matrice unitaria le cui prime r colonne* $\{|u_i\rangle\, 1 \leq i \leq r\}$ *sono una base ortonormale per* $\mathcal{U}$*, V è una matrice* $n \times n$ *unitaria le cui prime r colonne* $\{|v_i\rangle\, 1 \leq i \leq r\}$ *sono una base ortonormale per* $\mathcal{V}$*, e* Z_r *è la matrice con tutti i valori singolari diversi da zero uguali a 1. Equivalentemente,* $F = B\sum_{i=1}^{r} |u_i\rangle\langle v_i|$*.*

Una matrice di misurazione F di un B-scaled tight frame è un'isometria se ristretta a $\mathcal{V}$*.*

Una matrice di misurazione F di un B-scaled tight frame, le cui colonne sono n vettori in $\mathcal{H}$*, rappresenta una base ortogonale per* $\mathcal{U}$ *(i.e. è un tight frame ortogonale) se e solo se ha rango n. In questo caso* $F = BUZ_nV^\dagger$*, con* $F^\dagger F = B^2\mathbb{I}_n$*; i.e., tutti i vettori di frame hanno norma quadra uguale a* B^2*.*

□

Se i vettori $\{|\varphi_i\rangle, 1 \leq i \leq n\}$ formano un tight frame per $\mathcal{U}$, allora ogni $|x\rangle \in \mathcal{U}$ può essere espresso come combinazione lineare di questi vettori: $|x\rangle = \sum_i a_i|\varphi_i\rangle$. Quando $n > r = \dim(\mathcal{U})$, i coefficienti in questa espansione non sono unici. Una possibile scelta è $a_i = B^2\langle\varphi_i|x\rangle$, visto che

$$B^2\sum_{i=1}^{n}\langle\varphi_i|x\rangle|\varphi_i\rangle = B^2FF^\dagger|x\rangle = P_{\mathcal{U}}|x\rangle = |x\rangle.$$

Questa espansione ricorda l'espansione di $|x\rangle$ in funzione di una base ortonormale per $\mathcal{U}$. Bisogna però fare attenzione: mentre i vettori in una espansione ortonormale sono linearmente indipendenti, i vettori $|\varphi_i\rangle$ nell'equazione precedente sono linearmente dipendenti se $n > r$.

Dal Teorema 5.8, le matrici di frame dei tight frames hanno le stesse proprietà delle matrici di misurazione delle POVMs con elementi rango 1; proponiamo quindi l'equivalente del teorema di Neumark per i tight frames.

Teorema 5.10 (Neumark per i tight frames) *Sia F una matrice di frame, con n colonne in $\mathcal{H}$ che spannano un sottospazio r-dimensionale $\mathcal{U} \subseteq \mathcal{H}$. Allora $\exists$ una matrice ortogonale di frame $\widetilde{F}$ con colonne ortogonali, aventi norma uguale, che spannano un sottospazio n-dimensionale allargato $\widetilde{\mathcal{U}} \supseteq \mathcal{U}$ in uno spazio di Hilbert $\widetilde{\mathcal{H}} \supseteq \mathcal{H}$, tale che $F = P_{\mathcal{U}}\widetilde{F}$.* □

Ricordiamo che, dato un insieme vettori ortogonali di norma uguale in $\widetilde{\mathcal{U}} \supseteq \mathcal{U}$, allora i proiettori su $\mathcal{U}$ formano un tight frames per $\mathcal{U}$. Combinando questa osservazione col Teorema 5.10, concludiamo che un insieme di vettori forma un tight frame per $\mathcal{U}$ se e solo se i vettori possono essere espressi come proiezioni su $\mathcal{U}$ di un insieme di vettori ortogonali, con norma uguale, in uno spazio $\widetilde{\mathcal{U}} \supseteq \mathcal{U}$.

Per il Teorema 5.8, usiamo adesso la *least-squares measurement* (LSM), sviluppata nel contesto della quantum detection [17], per costruire il tight frame ottimale $\{|\varphi_i\rangle, 1 \leq i \leq n\}$, dato insieme di vettori $\{|\psi_i\rangle, 1 \leq i \leq n\}$ che spanna lo spazio r-dimensionale $\mathcal{U} \subseteq \mathcal{H}$. Vogliamo ovvero trovare i vettori $|\varphi_i\rangle \in \mathcal{H}$ che minimizzano l'errore E definito da

$$E = \sum_{i=1}^{n} \langle e_i | e_i \rangle, \tag{5.13}$$

dove $|e_i\rangle$ è l'i-esimo vettore d'errore

$$|e_i\rangle = |\psi_i\rangle - |\varphi_i\rangle,$$

e vale la condizione (5.11). In [16] vengono esplicitamente ricavati i frames ottimali riferiti sia al *constrained least-squares frame* (CLSF), cioè per $B = 1$, sia al al *unconstrained least-squares frame* (ULSF), quando si scelgono i vettori $\{\varphi_i\}$ e B tali che soddisfino (5.11) e minimizzino (5.13).

Conclusioni

Dopo aver esposto la teoria generale della misurazione quantistica nel primo capitolo, abbiamo focalizzato la nostra attenzione sulle POVMs.
Tutti i risultati del secondo capitolo sono stati punto cruciale del nostro lavoro di tesi, sia concettualmente che per il tempo ad essi dedicato; la presentazione dei teoremi rispetta l'ordine cronologico della loro scoperta.
Le due iniziali condizioni necessarie per l'estremalità delle POVMs sono supportate da due semplici esempi che negano la validità delle implicazioni inverse.
Una effettiva caratterizzazione delle POVMs affette dal solo rumore intrinseco della misurazione quantistica è stigmatizzata nella condizione necessaria e sufficiente proposta. Abbiamo trovato, in un primo momento, una condizione che valeva solamente per POVMs con elementi di rango 1; in questo caso infatti una dimostrazione costruttiva riesce a sondare tutte le possibilità in cui gli elementi di due POVMs possono combinarsi.
La generalizzazione a POVMs con elementi di rango generico è stata particolarmente laboriosa ma alla fine abbiamo trovato anche due diverse dimostrazioni per la condizione stessa: nella prima abbiamo sfruttato solamente la definizione di POVM non estremale e quindi la dimostrazione è risultata semplice e lineare. La seconda, invece, ci è stata indirettamente suggerita dal teorema di Choi: abbiamo definito delle mappe che verificassero ipotesi diverse da quelle di Choi, dimostrato due teoremi preliminari, tra cui la condizione necessaria e sufficiente per la loro estremalità, verificato che ci fosse una corrispondenza biunivoca tra queste e le POVMs, e infine applicato

la condizione suddetta alle POVMs. Questa seconda versione risulta quindi meno intuitiva della prima, ma ugualmente efficace. Alla fine del nostro lavoro, si è trovata in letteratura una terza dimostrazione della stessa condizione necessaria e sufficiente. Questa versione di Parthasarathy risulta però particolarmente complicata e non è stata riportata nella tesi; è basata sul teorema di Stinespring e la corrispondenza biunivoca tra POVMs e mappe lineari positive e unitali definite su una C^*-algebra abeliana.
Lavoro di ricerca è stato poi eseguito relativamente al problema della generalizzazione del concetto di osservabile dal formalismo dei proiettori a quello delle POVMs: abbiamo trovato la decomposizione a valori singolari di una misura generalizzata corrispondente ad una POVM commutante (generalizzazione della risoluzione ortonormale) e verificato che proprio tale POVM risulta essere un'osservabile. Era nostro obiettivo, all'inizio del lavoro, trovare una relazione di maggiorizzazione tra le osservabili, sfruttando questa prevista generalizzazione: tale relazione si è rivelata però non descrivibile a causa dell'arbitrarietà dei parametri che una relazione di maggiorizzazione tra due POVMs necessita.

Per la continuazione di questo lavoro si intende studiare classi particolari di POVMs con proprietà interessanti, quali le POVMs covarianti, e trovare all'interno di esse le POVMs estremali. Allo stesso modo si intende studiare i lavori di Winter [19] sulla separazione dell'informazione ottenibile da una misurazione quantistica in una parte intrinseca (meaningful) ed una estrinseca (not meaningful).
Infine, per quanto riguarda i frames, merita ulteriore approfondimento il legame tra frames e POVMs, esteso a POVMs con elementi di rango generico.

Bibliografia

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

[2] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publisher, Dordrecht, 1995).

[3] M. A. Neumark, Iza. Akad. Nauk USSR, Ser. Mat. **4**, 277 (1940).

[4] M. Ozawa, J. Math. Phys. **25**, 79 (1984).

[5] G. M. D'Ariano, *Quantum estimation theory and opticaldetection*, in *Quantum Optics and the Spectroscopy of Solids* (Kluwer Academic Publishers, Dordrecht, 1997).

[6] M. D. Choi, Linear Alg. Appl. **10**, 285-290 (1975).

[7] K. R. Parthasarathy, Inf. Dim. Anal. Quant. Prob. Rel. Top. **2**, 557-568 (1999).

[8] A. Messiah, *Quantum Mechanics* (Dover Publication, Inc., Mineola, New York, 1999).

[9] S. Boffi, *Da Laplace a Heisenberg, un'introduzione alla meccanica quantistica e alle sue applicazioni* (La Goliardica Pavese, Pavia, 1996).

[10] R. Bhatia, *Matrix analysis* (Springer-Verlag, New York, 1997).

[11] M. A. Nielsen, Phys. Rev. A **63**, 022114 (2001).

[12] M. A. Nielsen, Phys. Rev. A **62**, 052308 (2000).

[13] P. G. Casazza, Taiwanese J. Math. **4**, 129-201 (2000).

[14] D. Han, D. Larson, Mem. Amer. Math. Soc. **147**, 697 (2000).

[15] P. G. Casazza, J. Fourier Anal. Appl. **4**, 727-732 (1998).

[16] Y. C. Eldar, G. D. Forney, Jr., quant-ph/0106070 (2001).

[17] Y. C. Eldar, G. D. Forney, Jr., quant-ph/0005132 (2000).

[18] P. R. Halmos, *A Hilbert Space Problem Book* (Van Nostrand, Princeton, New York, 1967).

[19] A. Winter, quant-ph/0109050 (2001).

Ringraziamenti