# Indice

# Introduzione

Negli ultimi anni si sta delineando sempre più nettamente un nuovo settore della ricerca scientifica che viene definito Fisica dell'Informazione Quantistica. Ogni processo in cui si vogliano codificare, trasmettere o manipolare delle informazioni consiste in un'interazione col sistema fisico che costituisce il supporto dell'informazione stessa. L'idea di codificare l'informazione su un sistema quantistico (i.e. un sistema le cui proprietà siano descrivibili solo attraverso la meccanica quantistica) ha rapidamente portato ad un superamento delle esistenti teorie classiche del Calcolo, della Crittografia e della Comunicazione. La Fisica dell'Informazione Quantistica comprende i nuovi campi di ricerca detti *Quantum Cryptography* (Crittografia Quantistica), *Quantum Communication* (Comunicazione Quantistica) e *Quantum Computation* (Calcolo Quantistico), nati appunto dall'esigenza di rivedere le corrispondenti teorie classiche alla luce delle proprietà peculiari dei sistemi quantistici.

In questo lavoro si analizzerà il problema del cloning che è direttamente collegato ad una delle proprietà che distinguono l'informazione quantistica da quella classica: la sua non completa riproducibilità. Si tratta di un problema di carattere fondamentale, comune ai campi di ricerca appena evidenziati.
Intuitivamente si può pensare ad un cloner come ad una macchina che riceve in ingresso uno stato quantistico e produce come output M copie dello stesso. Il *Teorema del No-Cloning* afferma che non è possibile copiare esattamente uno stato quantistico a priori non noto (diremo che il cloning "ideale" non è realizzabile).
A questa impossibilità è collegata un'altra caratteristica che distingue la meccanica quantistica (e quindi l'informazione quantistica) da quella classica: l'impossibilità di determinare uno stato quantistico a priori non noto effettuando su di esso una sola misura.

Poiché sia il cloning ideale che la determinazione di uno stato quantistico a priori non noto non si possono fare esattamente, è interessante studiare il massimo della precisione con cui si possono realizzare queste operazioni. Il problema della stima ottima di uno stato quantistico rientra nell'ambito della *Quantum Estimation Theory* (Teoria Quantistica della Stima) che è stata studiata da diversi autori tra cui Holevo [9] e Helstrom [1].
Qui si vuole analizzare il problema di trovare il cloner quantistico ottimale, i.e quello che produce cloni "migliori" rispetto a qualsiasi altro. Imposteremo questo problema in maniera rigorosa, definendo un generico cloner attraverso una mappa T caratterizzata da diverse proprietà, una delle quali è la *covarianza*, che garantisce l'universalità di T, ovvero che il nostro cloner agisca "allo stesso modo" su tutti gli stati in ingresso (in pratica se T è covariante, T clona tutti gli stati in ingresso con la stessa "precisione"). Dopo aver introdotto un criterio quantitativo con cui esprimere la bontà del cloning (la Fidelity), presenteremo due diversi approcci con cui risolvere il problema impostato.
Nel primo, tratto da un lavoro di Werner [7], si ricava la forma esplicita della mappa di cloning ottima. Nel secondo, ispirato da un lavoro di Bruß, DiVincenzo et al.[12], utilizzando risultati già noti di Teoria Quantistica della Stima si ricava un limite per l'efficienza del cloning, senza avere a disposizione la forma esplicita della mappa T che lo descrive. Questi calcoli verranno presentati per il caso d=2 (cloning di qubits).

Il secondo approccio ci servirà come punto di partenza per procedere nella parte originale di questo lavoro, in cui analizziamo il problema del cloning ottimale di qubits "equatoriali". Indebolendo l'originaria condizione di covarianza (covarianza "in fase"), si ottiene un cloner che non lavora più "allo stesso modo" su qualunque stato $|\psi\rangle \in \mathcal{H}$ in ingresso. Vedremo che è comunque possibile individuare una classe $\mathcal{C} \subset \mathcal{H}$ di stati su cui T agisce ancora in modo universale. La classe così individuata è proprio quella dei *qubits equatoriali*, caratterizzati da un vettore di Bloch con componente Z nulla. L'importanza dello studio del cloning ottimale di questi stati risiede nel fatto che i qubits equatoriali vengono utilizzati nel più famoso schema crittografico proposto da Bennett e Brassard nel 1984, per questo chiamato schema BB84. Dopo avere calcolato la precisione massima con cui è possibile stimare lo stato di un generico qubit equatoriale (che verrà espressa tramite una quantità detta "Fidelity media ottima"), ricaveremo l'estremo superiore per la Fidelity ottima per il

cloning di qubits equatoriali. Vedremo poi che questa quantità è maggiore di quella relativa al cloning di un generico qubit. Intuitivamente questo è dovuto al fatto che considerare una classe di stati di input che costituisce un sottoinsieme proprio di $\mathcal{H}$ significa avere a disposizione una conoscenza a priori su tali stati, che permette di effettuare il cloning con una precisione maggiore. Avendo a disposizione la Fidelity massima sarà possibile interrogarsi sulla migliore strategia possibile che un ladro di informazioni può attuare inserendosi nel canale di comunicazione quantistico tra due soggetti che si stiano inviando un crittogramma seguendo la procedura prevista dallo schema BB84.
Come si potrà notare nel corso della trattazione, i problemi da risolvere quando si indebolisce la condizione di covarianza diventano più complicati, e soprattutto diventa estremamente difficile trovare la forma esplicita per la mappa di cloning covariante in fase ottima.
Il lavoro è strutturato come segue:

Nel **Capitolo 1** si presenta una breve trattazione della Teoria Quantistica della Stima, in cui sono fornite le basi per affrontare il calcolo (che rientra nella parte originale di questo lavoro) della Fidelity media ottima per la stima dello stato di un qubit equatoriale.

Nel **Capitolo 2**, dopo aver dato la dimostrazione del Teorema del No-Cloning, si presentano i due approcci al problema del cloning ottimale universale di qubits già discussi.

Nel **Capitolo 3** si analizza il problema del cloning ottimale di qubits *equatoriali* e si ricava il limite superiore per la Fidelity ottima. Viene anche ricavata la forma esplicita del cloner ottimale di qubits equatoriali, che ricevendo uno stato in ingresso ne produce due copie in uscita, e si mostra che la Fidelity relativa a tale cloner è uguale al limite superiore precedentemente ricavato. Questo costituisce una importante conferma dei risultati ottenuti e permette inoltre di affermare che, nel caso particolare analizzato, il limite superiore per la Fidelity ottima viene raggiunto.

# Capitolo 1

# STIMA DELLO STATO DI N QUBITS EQUATORIALI

## 1.1 Introduzione

In questo capitolo ci proponiamo di risolvere il problema di valutare quantitativamente la precisione massima con cui è possibile stimare lo stato quantistico di N quantum-bits (qubits) equatoriali. In letteratura il termine "qubit" è utilizzato per indicare un sistema il cui stato quantistico sia descrivibile in uno spazio di Hilbert bidimensionale. In questo lavoro, introduciamo il termine "equatoriale" per caratterizzare un qubit il cui vettore di Bloch giace nel piano equatoriale della sfera di Bloch.

La stima dello stato di un qubit equatoriale verrà ricondotta ad un problema di stima di fase. Tale problema si inserisce nel contesto generale della Teoria Quantistica della Stima, che a sua volta utilizza in modo cruciale il concetto di POVM. La parte originale di questo capitolo sarà quindi preceduta da una breve presentazione di questi argomenti, ispirata principalmente dai lavori [1], [2], [3].

## 1.2 Il concetto di POVM

Per estrarre informazioni da un generico sistema quantistico è necessario farlo interagire con un apparato di misura $\mathcal{M}$ ed analizzare i risultati ottenuti dalla

lettura di $\mathcal{M}$ attraverso una teoria che tenga conto di come sia avvenuta l'interazione.

Se facciamo interagire con $\mathcal{M}$ un certo numero di sistemi quantistici S indipendenti l'uno dall'altro, ma dello stesso tipo e nello stesso stato quantistico, i risultati numerici delle varie osservazioni non sono in generale gli stessi per ogni sistema, ma variano da un'osservazione all'altra. È necessario trattare questi risultati come variabili casuali, non solo a causa degli errori sperimentali e dell'incertezza sul vero stato del sistema S, ma anche a causa del fatto che la meccanica quantistica rinuncia alla predizione esatta dei risultati sperimentali, limitandosi a determinare le loro distribuzioni di probabilità.

I risultati numerici $u_1$,$u_2$,...,$u_n$ che si ottengono osservando il sistema S con $\mathcal{M}$ si possono rappresentare come un punto $\mathbf{u} = (u_1, u_2, ..., u_n)$ in uno spazio R su cui è definita una misura che assegna probabilità Pr($\Delta$) a regioni arbitrarie $\Delta$ di R. Pr($\Delta$) dà la probabilità che il punto $\mathbf{u}$ appartenga alla regione $\Delta$ di R. Le probabilità Pr($\Delta$) dipendono dalla matrice densità $\varrho$ relativa allo stato del sistema S appena prima dell'interazione con $\mathcal{M}$. Tale dipendenza, dovendo rispettare le combinazioni lineari convesse, deve essere data da un funzionale lineare positivo di $\varrho$ e sarà pertanto esprimibile mediante un set di operatori lineari $\hat{\Pi}(\Delta)$, il cui dominio è lo spazio di Hilbert $\mathcal{H}_{\mathrm{S}}$ del sistema S, attraverso l'equazione:

$$Pr(\Delta) = Tr[\varrho\,\hat{\Pi}(\Delta)] \tag{1.1}$$

Utilizzando il fatto che le Pr($\Delta$) possiedono le proprietà richieste dalla teoria standard della probabilità [1], abbiamo che gli operatori $\hat{\Pi}(\Delta)$ devono essere definiti non negativi ed ermitiani. Inoltre ad un insieme vuoto $\emptyset$ di punti in R deve essere associato l'operatore nullo $\hat{O}$ in $\mathcal{H}_{\mathrm{S}}$:

$$\emptyset \longmapsto \hat{\Pi}(\emptyset) = \hat{O} \tag{1.2}$$

mentre all'intero spazio R va associato l'operatore identità $\hat{I}$ su $\mathcal{H}_{\mathrm{S}}$:

$$R \longmapsto \hat{\Pi}(R) = \hat{I} \tag{1.3}$$

Infine ad una unione disgiunta di regioni $\Delta_\imath$ ($\imath$=1,2,..,k,...) tali che $\Delta_1 \cap ... \cap \Delta k \cap ... = \emptyset$, si associa un operatore che viene determinato per addizione:

$$\Delta_1 + ... + \Delta_k + ... \longmapsto \hat{\Pi}(\Delta_1 + ... + \Delta_k ...) = \hat{\Pi}(\Delta_1) + ... + \hat{\Pi}(\Delta_k) + ... \tag{1.4}$$

[1] Per un trattato completo di teoria della probabilità si veda Ref.[4]

L'associazione tra regioni $\Delta$ e operatori $\hat{\Pi}(\Delta)$ è una mappa che definisce un insieme di operatori detto "Positive Operator-Valued Measure" (POVM) in R. Quando R è un insieme denso è conveniente vedere la POVM come generata da operatori ermitiani infinitesimi e definiti non negativi $d\hat{\Pi}(\mathbf{u})$ associati a ciascun punto $\mathbf{u}$ di R in modo tale che per ogni regione finita $\Delta$ si abbia:

$$\hat{\Pi}(\Delta) = \int_{\Delta} d\hat{\Pi}(\mathbf{u}) \tag{1.5}$$

Le (1.2),(1.3),(1.4) sono in accordo con questa definizione se

$$\int_{R} d\hat{\Pi}(\mathbf{u}) = \hat{I} \tag{1.6}$$

Possiamo a questo punto definire la funzione densità di probabilità $p(\mathbf{u})$ tramite la:

$$dP(\mathbf{u}) \equiv p(\mathbf{u}) d^n\mathbf{u} = Tr[\varrho\, d\hat{\Pi}(\mathbf{u})] \tag{1.7}$$

dove $d^n\mathbf{u} = du_1\, du_2 ... du_n$ è l'elemento di volume di R. Nel caso particolare in cui $d\hat{\Pi}(\mathbf{u})\, d\hat{\Pi}(\mathbf{u}') = \delta(\mathbf{u} - \mathbf{u}')\, d\hat{\Pi}(\mathbf{u})$ la POVM si dice ortogonale.

Consideriamo un set di osservabili compatibili, ovvero di operatori commutanti $\hat{X}_\imath$ ($\imath$=1,...,n) che condividono una decomposizione spettrale

$$d\hat{E}(\mathbf{x}) = |\mathbf{x}\rangle\langle\mathbf{x}|\, d\mathbf{x} \tag{1.8}$$

tale che

$$\hat{X}_\imath = \int x_\imath\, d\hat{E}(\mathbf{x}) \tag{1.9}$$

dove $\mathbf{x}$=($x_1$,...,$x_n$) denota il vettore degli autovalori simultanei $x_\imath$ di $\hat{X}_\imath$ con autovettore comune $|\mathbf{x}\rangle$. Nel caso di POVM ortogonale la (1.7) dà la regola di Born che fornisce la probabilità che, facendo sullo stato S specificato da $\varrho$ una misura del set di operatori commutanti $X_\imath$, il risultato sia compreso nella regione $[\mathbf{x}, \mathbf{x} + d\mathbf{x}]$. La (1.7) è quindi una generalizzazione della regola di Born con una POVM genericamente non ortogonale.

Consideriamo infatti una misura indiretta di secondo tipo [2] di una osservabile $\hat{X}$ con risoluzione spettrale $\mathrm{d}\hat{E}_{SP}(\mathrm{x})$ che agisce sullo spazio di Hilbert

[2]Secondo la nomenclatura utilizzata da M.Ozawa in [8], indichiamo con misura di secondo tipo una misura che distrugge lo stato del sistema (ovvero di cui sia assegnata solo la distribuzione di probabilità e non la riduzione dello stato).

$\mathcal{H}_{\mathrm{S}} \otimes \mathcal{H}_{\mathrm{P}}$ ( $\mathcal{H}_{\mathrm{P}}$ indica lo spazio di Hilbert di una parte opportuna dell'apparato di misura, il Probe, che è necessario tenere in considerazione per una descrizione quantistica del processo di misurazione). Sia inoltre $\varrho_S \otimes \varrho_P$ la matrice densità che descrive il sistema composto S+P prima dell'interazione. La (1.7) si scrive ora:

$$dP(x) = Tr_{SP}[\varrho_S \otimes \varrho_P \, d\hat{E}_{SP}(x)] \tag{1.10}$$

Valutando la traccia che compare in (1.10) in due passaggi successivi abbiamo:

$$dP(x) = Tr_S\{\varrho_S Tr_P[\varrho_P \, d\hat{E}_{SP}(x)]\} \tag{1.11}$$

Dal punto di vista di un osservatore che ignori (deliberatamente o no) il probe P, la (1.11) deve contenere soltanto operatori sullo spazio di Hilbert $\mathcal{H}_{\mathrm{S}}$ e si può scrivere nella forma (1.7) come segue:

$$dP(x) = Tr_S[\varrho_S \, d\hat{\Pi}(x)] \tag{1.12}$$

con POVM data da

$$d\hat{\Pi}(x) = Tr_P[\varrho_P \, d\hat{E}_{SP}(x)] \tag{1.13}$$

È chiaro dalla (1.13) che per una generica $\varrho_P$ la POVM $\mathrm{d}\hat{\Pi}(\mathrm{x})$ non è ortogonale.

Il vantaggio di una descrizione della procedura di misurazione tramite POVM è che $\mathrm{d}\hat{\Pi}(\mathrm{x})$ dipende dall'apparato di misurazione considerato: per uno stato fissato $\varrho_S$ si possono avere diverse distribuzioni di probabilità $\mathrm{dP(x)}$ cambiando l'apparato stesso e/o la sua preparazione $\varrho_P$.

Il concetto di osservabile fisica che deriva dall'utilizzo delle POVM è quindi basato sulla definizione della procedura con cui si attua la misurazione. In tal modo è possibile, in linea di principio, descrivere i risultati della misura di una grandezza fisica a cui non sia necessariamente associabile un operatore autoaggiunto.

## 1.3 Teoria Quantistica della Stima

La corrispondenza tra apparati di misura e POVM non è biunivoca, ma ci sono in generale più apparati di misura descritti dalla stessa POVM.

Nella Teoria Quantistica della Stima si analizzano le POVM ad un livello puramente astratto. Con lo scopo di trovare la migliore strategia per la misura di uno o più parametri di un sistema in uno stato fissato, si individua

la classe di POVM più adeguata, e al suo interno si sceglie la POVM ottima secondo un pre-definito criterio di ottimalità. In questo modo la teoria permette di trovare la classe di apparati che realizzano una determinata misura in maniera ottimale (i.e. quelli corrispondenti alla POVM ottima) e di dare una valutazione quantitativa della bontà della misura stessa.

In generale è possibile esprimere lo stato del sistema in esame tramite una matrice densità $\varrho = \varrho(\boldsymbol{\theta})$ che dipende dai parametri $\theta_1$,...,$\theta_m$ che si vogliono stimare e che si possono rappresentare tramite un punto $\boldsymbol{\theta}$=($\theta_1$,...,$\theta_m$) in uno "spazio dei parametri" $\Theta$ di dimensione m.

Denotiamo con $\mathrm{d}\hat{\Pi}(\boldsymbol{\theta})$ la generica POVM che sintetizza la "strategia" utilizzata per la misura di $\boldsymbol{\theta}$, ovvero la struttura dell'apparato di misura ed in generale l'insieme di operazioni che è necessario eseguire per tradurre i dati forniti da $\mathcal{M}$ nel set ($\theta_{1*}$,...,$\theta_{m*}$) che costituisce la stima $\boldsymbol{\theta}_*$ di $\boldsymbol{\theta}$. La densità di probabilità condizionata $p(\boldsymbol{\theta}_*|\boldsymbol{\theta})$ di misurare $\boldsymbol{\theta}_*$ invece del "valore vero" $\boldsymbol{\theta}$ sarà data da:

$$p(\boldsymbol{\theta}_*|\boldsymbol{\theta})\, d^m\, \boldsymbol{\theta}_* = Tr[\varrho(\boldsymbol{\theta})\, d\hat{\Pi}(\boldsymbol{\theta}_*)] \tag{1.14}$$

con $d^m\boldsymbol{\theta}_*$=d$\theta_{1*}$...d$\theta_{m*}$volume infinitesimo nello spazio dei parametri $\Theta$.

Se introduciamo una funzione costo C($\boldsymbol{\theta}_*$,$\boldsymbol{\theta}$) che esprima il costo degli errori nella stima di $\boldsymbol{\theta}$, la POVM migliore per la stima dei parametri $\boldsymbol{\theta}$ sarà quella che minimizza il costo medio $\overline{C}$ in cui si incorre quando si utilizza la strategia di misurazione sintetizzata da $\mathrm{d}\hat{\Pi}(\boldsymbol{\theta})$, che definiamo come:

$$\overline{C} = \int_\Theta d^m\boldsymbol{\theta}_* \int_\Theta d^m\boldsymbol{\theta}\; z(\boldsymbol{\theta})\, C(\boldsymbol{\theta}_*, \boldsymbol{\theta})\, p(\boldsymbol{\theta}_*|\boldsymbol{\theta}) \tag{1.15}$$

dove abbiamo indicato con z($\boldsymbol{\theta}$) la probabilità a priori del punto $\boldsymbol{\theta} \in \Theta$. Nel prossimo paragrafo verrà analizzata la procedura di minimizzazione del costo medio $\overline{C}$ nel caso della stima canonica della fase.

## 1.4 POVM ottima per una stima di fase

Analizziamo in questo paragrafo il problema della stima dello shift di fase $\phi \in [0,2\pi]$ indotto tramite la trasformazione unitaria

$$\varrho(\phi) = e^{-i\phi\hat{H}}\, \varrho_o\, e^{i\phi\hat{H}} \tag{1.16}$$

dove $\hat{H}$ è un operatore autoaggiunto degenere sullo spazio di Hilbert $\mathcal{H}_\mathrm{S}$ con spettro discreto illimitato Spec($\hat{H}$)=$\mathbb{Z}$, limitato inferiormente Spec($\hat{H}$)=$\mathbb{N}$, op-

pure limitato Spec($\hat{H}$)=$\mathbb{Z}_q$ ($q > 0$), mentre $\varrho_o$ è una matrice densità su $\mathcal{H}_S$ corrispondente ad un generico stato iniziale. Per impostare il problema nel contesto generale della teoria quantistica della stima cominciamo con l'osservare che lo spazio dei parametri $\Theta$ in questo caso ha dimensione 1 i.e:

$$\Theta = \{\phi | \phi \in [0, 2\pi]\} \tag{1.17}$$

Consideriamo la situazione generale in cui $\phi$ è a priori distribuito uniformemente nell'intervallo $[0, 2\pi]$ (i.e $z(\phi) = \frac{1}{2\pi}$) e in cui la funzione costo $C(\phi, \phi_*)$ è una funzione pari della variabile $\phi_* - \phi$, $C(\phi, \phi_*) = C(\phi_* - \phi)$. Questa ultima assunzione corrisponde all' idea di voler pesare gli errori commessi nella stima di $\phi$ indipendentemente dal valore di $\phi$, ma solo in base al valore assoluto della differenza tra il valore "vero" $\phi$ e quello stimato $\phi_*$. Dalle proprietà richieste per la funzione costo, segue che anche la densità di probabilità condizionata ottima dipenderà solo da $\phi_* - \phi$: $p(\phi_*|\phi) = p(\phi_* - \phi)$. Inoltre, se indichiamo con d$\hat{\mu}(\phi_*)$ la POVM relativa al processo di misurazione da ottimizzare, dall'uguaglianza

$$p(\phi_*|\phi)\, d\phi_* = Tr[d\mu(\phi_*)\, e^{-i\phi\hat{H}}\, \varrho_0\, e^{i\phi\hat{H}}] \tag{1.18}$$

e utilizzando l'invarianza della traccia per permutazioni cicliche, segue che $p(\phi_*|\phi) = p(\phi_* - \phi)$ se e solo se

$$d\hat{\mu}(\phi_*) = e^{-i\hat{H}\phi_*}\, \xi\, e^{i\hat{H}\phi_*}\, \frac{d\phi_*}{2\pi} \tag{1.19}$$

con $\hat{\xi}$ operatore positivo e tale che:

$$\int_0^{2\pi} d\mu(\phi) = \hat{I} \tag{1.20}$$

Una POVM della forma (1.19) si dice covariante in fase. Il problema di ottimizzazione della nostra POVM covariante in fase si riduce quindi a quello di trovare il migliore operatore $\hat{\xi}$ per una data funzione costo $C(\phi - \phi_*)$ ed un generico stato $\varrho_o$. La funzione costo medio (1.15) assume in questo caso particolare la forma:

$$\overline{C} = \int_0^{2\pi} d\phi \int_0^{2\pi} d\phi_* z(\theta) C(\phi_*, \phi) p(\phi_*|\phi) = \tag{1.21}$$

$$= \int_0^{2\pi} d\phi \int_0^{2\pi} d\phi_* z(\phi) C(\phi_* - \phi) p(\phi_* - \phi) = \tag{1.22}$$

$$= \frac{1}{2\pi}\int_0^{2\pi} d\phi \int_0^{2\pi} d\phi_* C(\phi_* - \phi) Tr[\hat{\xi} e^{i\hat{H}(\phi_* - \phi)} \varrho_o e^{-i\hat{H}(\phi_* - \phi)}] = \tag{1.23}$$

$$= Tr[\hat{C}\, \varrho_o] \tag{1.24}$$

con $\hat{C} = \int d\mu(\tilde{\phi}) C(\tilde{\phi})$ e $\tilde{\phi} = \phi_* - \phi$ variabile indipendente. Minimizzando $\overline{C}$ si ottiene la POVM ottima per la classe di equivalenza di stati individuati dalla matrice densità $\varrho(\phi)$ con $\phi$ che varia nell'intervallo $[0, 2\pi]$.

Per risolvere questi problemi è conveniente introdurre la rappresentazione in cui l'operatore $\hat{H}$ è diagonale. $\hat{H}$ è in generale degenere: indicheremo con $|n\rangle_\nu$ un insieme di autovettori (normalizzati) corrispondenti all'autovalore $n$, con $\nu$ indice di degenerazione, e con $\Pi_n$ il proiettore sul sottospazio di $\mathcal{H}_\mathrm{S}$ da essi generato. Analizziamo il caso in cui lo stato iniziale sia uno stato puro, $\varrho_0 = |\psi_o\rangle\langle\psi_o|$. Sia $\mathcal{H}_\parallel \subseteq \mathcal{H}_\mathrm{S}$ lo spazio di Hilbert generato dai vettori (anch'essi normalizzati)

$$|n\rangle \propto \Pi_n |\psi_o\rangle \neq 0 \tag{1.25}$$

con le fasi arbitrarie scelte in modo che $\langle n|\psi_o\rangle > 0$. Osservando le (1.24) e la (1.18), ci accorgiamo che possiamo scegliere la POVM da ottimizzare diagonale a blocchi su $\mathcal{H}_\mathrm{S} = \mathcal{H}_\parallel \oplus \mathcal{H}_\perp$, i.e $d\mu(\phi) = d\mu_\parallel(\phi) \oplus d\mu_\perp(\phi)$ con $d\mu_\perp(\phi)$ arbitraria POVM su $\mathcal{H}_\perp$. Se ottimizziamo la POVM nel caso in cui $\Pi_n|\psi_o\rangle \neq 0\ \forall n \in Spec(\hat{H}) \equiv S$, avremo chiaramente risolto il problema anche per il caso in cui $\Pi_n|\psi_o\rangle = 0$ per qualche $n \in S$. Seguendo questa impostazione ci siamo ridotti al problema di trovare l'operatore positivo $\hat{\xi}_\parallel$ che minimizza $\overline{C}$ in equazione (1.24) nello spazio di Hilbert ristretto $\mathcal{H}_\parallel$. Invece di $\hat{H}$ consideriamo perciò la sua restrizione $\hat{H}_\parallel = \sum_{n\in S} n|n\rangle\langle n|$ e scriviamo l'operatore $\hat{\xi}_\parallel$ come:

$$\hat{\xi}_\parallel = \sum_{n,m\in S} \xi_{n\,m} |n\rangle\langle m| \tag{1.26}$$

Per una generica funzione costo pari e periodica di $2\pi$ si ha

$$C(\tilde{\phi}) = -\sum_{l=0}^{\infty} c_l \cos l\tilde{\phi}$$

ed il costo medio diventa:

$$\overline{C} = -c_o - \frac{1}{2}\sum_{l=1}^{\infty} c_l \sum_{|m-n|=l} \xi_{n\,m} \langle\psi_o|n\rangle\langle m|\psi_o\rangle \tag{1.27}$$

La positività di $\hat{\xi}$ implica la disuguaglianza di Schwartz generalizzata:

$$|\xi_{n\,m}| \leq \sqrt{\xi_{n\,n}\xi_{m\,m}} = 1 \tag{1.28}$$

dove l'ultima uguaglianza viene dalla $\int d\hat{\mu}_{\|}(\phi) = \hat{I}_{\|}$. Dal fatto che la disuguaglianza seguente:

$$sign(c_l) \sum_{|n-m|=l} \xi_{n\,m}\langle\psi_o|n\rangle\langle m|\psi_o\rangle \leq \sum_{|n-m|=l} |\langle\psi_o|n\rangle||\langle m|\psi_o\rangle| \tag{1.29}$$

diventa un'uguaglianza per $\xi_{n\,m} = sign(c_{|n-m|})$, deduciamo che il costo medio minimo è:

$$\overline{C} = -c_o - \frac{1}{2}\sum_{l=1}^{\infty} |c_l| \sum_{|n-m|=l} |\langle\psi_o|n\rangle||\langle m|\psi_o\rangle| \tag{1.30}$$

dove abbiamo posto $sign(0)$=1 poiché $\overline{C}$ è indipendente da $\xi_{nm}$ per $c_{|n-m|} = 0$. Se scegliamo $c_l \geq 0\ \forall l \geq 1$ in modo che la positività di $\xi_{\|}$ sia garantita, abbiamo che la POVM ottima diventa:

$$d\mu_{\|}(\phi) = \frac{d\phi}{2\pi}|e(\phi)\rangle\langle e(\phi)| \tag{1.31}$$

con i vettori $|e(\phi)\rangle$ dati da:

$$|e(\phi)\rangle = \sum_{n\in S} e^{\,in\phi}|n\rangle \tag{1.32}$$

La scelta particolare $c_l \geq 0\ \forall l \geq 1$ (il parametro $c_o$ è irrilevante) è stata considerata da Holevo[3] e include una vasta classe di funzioni costo tra cui la Fidelity $C(\phi) = 1 - |\langle\psi_o|e^{\,i\hat{H}\phi}|\psi_o\rangle|^2$ che utilizzeremo in seguito.

## 1.5 Stima di uno stato quantistico

Fino ad ora abbiamo spiegato come sia possibile stimare alcuni parametri della matrice densità relativa ad uno stato quantistico, ma non è ancora chiaro come (e se) sia possibile stimare la funzione d'onda $|\Psi\rangle$ che descrive lo stato stesso.

Consideriamo il caso in cui $|\Psi\rangle$ appartenga ad uno spazio di Hilbert $\mathcal{H}$ di dimensione $d$ finita e introduciamo la base $\{|\varphi_k\rangle\}_{k=1,\ldots,d}$ costituita da $d$ vettori

[3] Si veda a questo proposito Ref.[9]

ortonormali. Il vettore $|\Psi\rangle$ è individuato dal vettore $\mathbf{c} = (c_1, ..., c_d) \in \mathbb{C}^d$, dove $c_k = \langle\varphi_k|\Psi\rangle$. Possiamo scrivere

$$|\Psi\rangle = |\Psi(\mathbf{c})\rangle = \sum_{k=1}^{d} c_k|\varphi_k\rangle \tag{1.33}$$

I $d$ numeri complessi $c_k = c_{k_x} + i\, c_{k_y}$ sono i parametri dell'operatore densità

$$\varrho(\mathbf{c}) = |\Psi(\mathbf{c})\rangle\langle\Psi(\mathbf{c})| \tag{1.34}$$

Quindi il problema della stima dello stato $|\Psi\rangle$ è stato ricondotto al problema (già analizzato) della stima dei d parametri complessi $c_k$ della matrice densità $\varrho(\mathbf{c})$. Notiamo che siccome $|\Psi(\mathbf{c})\rangle$ è normalizzato

$$\sum_{k=1}^{d} |c_k|^2 = \sum_{k=1}^{d} (c_{k_x}^2 + c_{k_y}^2) = 1$$

Il punto $\mathbf{c}$ appartiene quindi alla ipersfera $2d$-dimensionale di raggio 1 $S_{2d}$. Lo spazio dei parametri $\Theta$ coincide in questo caso con $S_{2d}$. Se lo stato $|\Psi\rangle$ è completamente non noto il punto $\mathbf{c}$ ha a priori la stessa probabilità di trovarsi ovunque sulla sfera $S_{2d}$, da cui

$$z(\mathbf{c}) = A_{2d}^{-1}$$

dove $= A_{2d}^{-1}$ è l'area dell'ipersfera $S_{2d}$. La stima di $\mathbf{c}$ fornirà un punto $\mathbf{c}^* \in S_{2d}$

$$\mathbf{c}^* = (c_1^*, ..., c_d^*)$$

tramite il quale è possibile costruire un nuovo vettore $|\Psi^*\rangle \in \mathcal{H}$

$$|\Psi^*\rangle = \sum_{k=1}^{d} c_k^*|\varphi_k\rangle$$

che costituisce la stima del vettore $|\Psi\rangle$. Attraverso il "nuovo" stato $|\Psi^*\rangle$ è possibile definire la funzione costo

$$C(\mathbf{c}, \mathbf{c}^*) = 1 - |\langle\Psi|\Psi^*\rangle|^2 \tag{1.35}$$

dove

$$|\langle\Psi|\Psi^*\rangle|^2 \equiv F(\mathbf{c}, \mathbf{c}^*)$$

è detta Fidelity relativa al processo di stima. La Fidelity può assumere valori nell'intervallo $[0,1]$ ed esprime quanto lo stato stimato $|\Psi^*\rangle$ è vicino a quello da stimare $|\Psi\rangle$. In particolare se $|\Psi^*\rangle = |\Psi\rangle$ abbiamo $F(\mathbf{c},\mathbf{c}^*) = 1$ e quindi $C(\mathbf{c},\mathbf{c}^*) = 0$, altrimenti pioché $|\Psi^*\rangle$ e $|\Psi\rangle$ sono stati normalizzati si ha che $0 \leq F(\mathbf{c},\mathbf{c}^*) \leq 1$.

## 1.6 Stima dello stato di un sistema di N qubits

Introduciamo nello spazio di Hilbert $\mathcal{H} \simeq \mathbb{C}^2$ la base ortonormale $\{|0\rangle, |1\rangle\}$.

Sappiamo da [5] che dato un sistema di N qubits, ciascuno dei quali si trovi nel medesimo stato sconosciuto a priori e descritto dal vettore $|\psi\rangle \in \mathcal{H}$, esiste una POVM che fornisce la stima ottima di $|\psi\rangle$ con Fidelity media

$$\overline{F}^{opt}_{gen}(N) = \frac{N+1}{N+2} \tag{1.36}$$

Consideriamo ora in maggior dettaglio il seguente problema. Dato un qubit equatoriale, descritto da un vettore di stato della forma[4]:

$$|\psi_\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\,i\phi}|1\rangle) \tag{1.37}$$

con $\phi \in [0, 2\pi]$, consideriamo il sistema composto da N qubits preparati identicamente e non interagenti tra loro, descritto dal vettore di stato

$$|\Psi_\phi\rangle = \otimes_{l=1}^{N} \frac{1}{\sqrt{2}}(|0\rangle_l + e^{\,i\phi}|1\rangle_l) = \tag{1.38}$$

$$= [\frac{1}{\sqrt{2}}(|0\rangle + e^{\,i\phi}|1\rangle)]^{\otimes N} \tag{1.39}$$

$|\Psi_\phi\rangle$ appartiene al sottospazio di $\mathcal{H}^{\otimes \mathrm{N}}$ generato dai vettori della forma $\varphi^{\otimes N} = \varphi \otimes \varphi \otimes ... \otimes \varphi$ (i.e invarianti per ogni permutazione), cioè al sottospazio simmetrico $\mathcal{H}_+^{\otimes \mathrm{N}}$ di $\mathcal{H}^{\otimes \mathrm{N}}$. Il problema della stima dello stato $|\Psi_\phi\rangle$ è immediatamente riconducibile al problema della stima del parametro $\phi$ della matrice densità $\varrho(\phi) = |\Psi_\phi\rangle\langle\Psi_\phi|$. Come abbiamo visto in (1.4), misurare $\phi$ è equivalente a stimare lo shift di fase a cui viene sottoposto lo stato iniziale

[4] Come vedremo nei prossimi capitoli, gli stati della forma $|\psi_\phi\rangle$ sono caratterizzati da un vettore di Bloch di norma unitaria e componente Z nulla, giacente perciò nel piano equatoriale della sfera di Bloch.

$|\Psi_o\rangle = [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]^{\otimes N}$ se gli applichiamo l'operatore (detto appunto di shift di fase):

$$\hat{U}_\phi = \otimes_{l=1}^{N} \exp[-\frac{i}{2}(\sigma_z^l - 1)\phi] \tag{1.40}$$

Infatti, se consideriamo l'operatore $\hat{u}_\phi$ agente su $\mathcal{H}$, così definito:

$$\hat{u}_\phi = \exp(-i\hat{h}\phi) \tag{1.41}$$

con $\hat{h} = \frac{1}{2}(\sigma_z - 1)$, e lo applichiamo allo stato $|\psi_o\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \in \mathcal{H}$ abbiamo:

$$\begin{aligned}
\hat{u}_\phi|\psi_o\rangle &= \exp[-\frac{i}{2}(\sigma_z - 1)\phi][\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)] = \\
&= \frac{1}{\sqrt{2}}\{\exp[-\frac{i}{2}(\sigma_z - 1)\phi]|0\rangle + \exp[-\frac{i}{2}(\sigma_z - 1)\phi]|1\rangle\} = \\
&= \frac{1}{\sqrt{2}}[|1\rangle + e^{i\phi}|1\rangle]
\end{aligned}$$

Se scriviamo l'operatore $U_\phi$ nella forma $U_\phi = \exp(-i\hat{H}\phi)$, con

$$\hat{H} = \sum_{l=1}^{N} \frac{1}{2}(\sigma_z^l - 1)$$

dove l'operatore $\frac{1}{2}(\sigma_z^l - 1)$ è l'operatore su $\mathcal{H}^{\otimes N}$ che agisce sulla particella l-sima come $\hat{h}$ e sulle restanti N-1 come l'operatore identità, vediamo subito che:

$$\begin{aligned}
\hat{U}_\phi : \quad \mathcal{H}_+^{\otimes N} &\longrightarrow \mathcal{H}_+^{\otimes N} \\
|\Psi_o\rangle &\longmapsto |\Psi_\phi\rangle
\end{aligned}$$

Per ottimizzare la POVM relativa alla stima di $\phi$ non ci resta a questo punto che introdurre la rappresentazione di H. Siccome $Spec(\hat{h}) = \{0, 1\}$, avremo che $Spec(\hat{H}) = \{0, 1, ..., N\} \simeq \mathbb{Z}_q$ $(q = N + 1)$, ovvero $\hat{H}$ ha $q$ autovalori. Inoltre il generico autovalore $k$ ha degenerazione

$$deg(k) = \binom{N}{k} \tag{1.42}$$

Definiamo a questo punto $q$ vettori (opportunamente normalizzati) tramite la relazione (1.25): $|k\rangle \propto \Pi_k|\Psi\rangle_o$[5]. Dalla (1.31) abbiamo immediatamente la

[5]Ricordiamo che $\Pi_k$ è il proiettore sul sottospazio generato dagli autovettori relativi all'autovalore $k \in \mathrm{Spec}(\hat{H})$.

POVM ottima per la classe di Holevo di funzioni costo:

$$d\mu_{opt}(\phi) = \frac{d\phi}{2\pi}|e(\phi)\rangle\langle e(\phi)| \tag{1.43}$$

con

$$|e(\phi)\rangle = \sum_{k=0}^{N} e^{\,ik\phi}|k\rangle \tag{1.44}$$

Per trovare il set di vettori $\{|k\rangle\}$, esplicitiamo nella tabella 1.1 gli autovettori relativi ai diversi autovalori di $\hat{H}$, utilizzando la notazione

$$|0..010..0\rangle = |0\rangle \otimes .. \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle .. \otimes |0\rangle$$

per i vettori appartenenti allo spazio di Hilbert $\mathcal{H}^{\otimes N}$.

| Autovalore $k$ | $\nu = deg(k)$ | Autovettori |
|---|---|---|
| 0 | $\binom{N}{0} = 1$ | $\|000...0\rangle$ |
| 1 | $\binom{N}{1} = N$ | $\|100...0\rangle, \|010...0\rangle, ..., \|000...1\rangle$ |
| 2 | $\binom{N}{2} = \frac{N!}{2!(N-2)!}$ | $\|110...0\rangle, \|101...0\rangle, ...$ |
| ... | ... | ... |
| ... | ... | ... |
| N | $\binom{N}{N} = 1$ | $\|111...1\rangle$ |

Tabella 1.1: Autovalori di $\hat{H}$, relativo grado di degenerazione e autovettori corrispondenti.

Il vettore $|\Psi\rangle_o$ nella nuova notazione si scrive:

$$\begin{aligned} |\Psi_o\rangle &= [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]^{\otimes N} = \\ &= \frac{1}{2^{\frac{N}{2}}}[|000...0\rangle + |100...0\rangle + ... + |000...1\rangle + |110...0\rangle + ...] \end{aligned}$$

Applicando a $|\Psi_o\rangle$ gli N proiettori $\Pi_k$ e normalizzando opportunamente gli N vettori ottenuti abbiamo:

$$|k\rangle = \binom{N}{k}^{-\frac{1}{2}} \sum_{\{s_i=0,1\}} \delta(\sum_i s_i - k) \otimes_{i=1}^{N} |s_i\rangle \tag{1.45}$$

da cui anche:

$$|\Psi_o\rangle = \frac{1}{2^{\frac{N}{2}}} \sum_{k=0}^{N} \binom{N}{k}^{\frac{1}{2}} |k\rangle \tag{1.46}$$

Consideriamo a questo punto la particolare funzione costo, appartenente alla classe di Holevo (ovvero con $c_l \geq 0 \ \forall l \geq 1$):

$$C(\tilde{\phi}) = 1 - F(\tilde{\phi}) \tag{1.47}$$

dove la funzione $F(\tilde{\phi}) = F(\phi - \phi_*)$ è la Fidelity definita nel §1.5, che riscriviamo in questo caso particolare:

$$F(\tilde{\phi}) = |\langle_\phi \psi | \psi_{\phi *}\rangle|^2 = |\langle_o \psi | U_\phi | \psi_o \rangle|^2 \tag{1.48}$$

Svolgendo i calcoli abbiamo:

$$\begin{aligned} F(\tilde{\phi}) &= |\frac{1}{2}(\langle 0| + \langle 1|) \exp[-\frac{i}{2}(\sigma_z - 1)\tilde{\phi}](|0\rangle + |1\rangle)|^2 = & (1.49)\\ &= |\frac{1}{2}(1 + e^{\,i\tilde{\phi}})|^2 = & (1.50)\\ &= \frac{1}{4}(2 + e^{\,i\tilde{\phi}} + e^{-i\tilde{\phi}}) & (1.51) \end{aligned}$$

Possiamo ora calcolare il costo medio $\overline{C}^{opt}$ relativo alla misura ottima della classe di stati $\varrho(\phi)$:

$$\begin{aligned} \overline{C}^{opt} &= 1 - \overline{F}^{opt} = \\ &= Tr[\int d\mu_{opt}(\tilde{\phi})(1 - F(\tilde{\phi}))\varrho_o] = \\ &= Tr[\int d\mu_{opt}(\tilde{\phi})\varrho_o] - Tr[\int d\mu_{opt}(\tilde{\phi})F(\tilde{\phi})\varrho_o] = \\ &= 1 - Tr[\int d\mu_{opt}(\tilde{\phi})F(\tilde{\phi})\varrho_o] \end{aligned}$$

da cui deduciamo immediatamente la Fidelity media ottima:

$$\overline{F}^{opt} = Tr[\int d\mu_{opt}(\tilde{\phi})F(\tilde{\phi})\varrho_o] \tag{1.52}$$

Inserendo nella (1.52) $\varrho_o = |\psi_o\rangle\langle_o\psi|$ con $|\psi_o\rangle = \sum_k x_k|k\rangle$ ($x_k = \langle k|\psi_o\rangle = 2^{-\frac{N}{2}}\binom{N}{k}^{\frac{1}{2}}$) otteniamo:

$$\overline{F}^{opt} = Tr\left[\int_0^{2\pi} \frac{d\tilde{\phi}}{2\pi} \sum_{k\,k'} e^{\,i(k-k')\vec{\phi}} |k\rangle\langle k'| (\frac{e^{\,i\vec{\phi}} + e^{-i\vec{\phi}} + 2}{4}) \cdot \right.$$

$$\cdot \sum_{l\,m} \frac{1}{2^N} \binom{N}{l}^{\frac{1}{2}} \binom{N}{m}^{\frac{1}{2}} |l\rangle\langle m| \Bigg] =$$

$$= \frac{1}{2^N}\frac{1}{4}\left[\int_0^{2\pi} \frac{d\tilde{\phi}}{2\pi} \sum_{j,k,l} \langle j|k\rangle e^{i(k-l)\vec{\phi}} (e^{i\vec{\phi}} + e^{-i\vec{\phi}} + 2)\cdot \right.$$

$$\left. \cdot \sum_{m} \binom{N}{l}^{\frac{1}{2}} \binom{N}{m}^{\frac{1}{2}} \langle m|j\rangle \right] =$$

$$= \frac{1}{2^N}\frac{1}{4}\left[\sum_{l=1}^{N} \binom{N}{l}^{\frac{1}{2}} \binom{N}{l-1}^{\frac{1}{2}} + \sum_{l=0}^{N-1} \binom{N}{l}^{\frac{1}{2}} \binom{N}{l+1}^{\frac{1}{2}} + \right.$$

$$\left. +2\sum_{l=0}^{N-1} \binom{N}{l} \right] =$$

$$= \frac{1}{2^N}\frac{1}{4}\left[2\sum_{l=0}^{N-1} \binom{N}{l+1}^{\frac{1}{2}} \binom{N}{l}^{\frac{1}{2}} + 2^{N+1}\right]$$

Da cui:

$$\overline{F}^{opt} = \overline{F}^{opt}(N) = \frac{1}{2} + \frac{1}{2^{N+1}} \sum_{l=0}^{N-1} \sqrt{\binom{N}{l}\binom{N}{l+1}} \tag{1.53}$$

In Appendice A dimostreremo che la funzione $\overline{F}^{opt}(N)$ gode delle seguenti proprietà:

- $$\overline{F}^{opt}(N) \leq 1 \ \forall N \tag{1.54}$$

- $$\lim_{N\to\infty} \overline{F}^{opt}(N) = 1 \tag{1.55}$$

Uno stato quantistico (in accordo all'interpretazione statistica) non è altro che un' entità matematica che racchiude in sè tutti i dati che si possono raccogliere tramite una serie di esperimenti statistici. Una perfetta determinazione di tale stato (corrispondente ad una stima di stato con $\overline{F}^{opt} = 1$) necessiterebbe perciò di un ensemble infinito di particelle identicamente preparate su cui fare delle misure. Nella pratica, si dispone di un ensemble finito di N particelle e pertanto lo stato di ciascuna può essere determinato solo approssimativamente, con un' accuratezza (che nel nostro caso è espressa dalla Fidelity media ottima) tanto maggiore quanto più grande è N.

Nella figura 1.1 riportiamo il grafico della quantità $\overline{F}^{opt}(N)$ a confronto con quello di $\overline{F}^{opt}_{gen}$ di equazione (1.36). Come atteso, entrambe le quantità sono funzioni crescenti di N e tendono ad 1 per $N \longrightarrow \infty$.
Sempre dalla figura 1.1 si vede che

$$\overline{F}^{opt}_{gen}(N) \leq \overline{F}^{opt}(N)$$

pre tutti gli N presi in considerazione. In realtà ci aspettiamo che questa disuguaglianza valga per ogni N. Infatti $\overline{F}^{opt}_{gen}$ è la Fidelity relativa alla stima dello stato, a priori ignoto, di un sistema di N qubits, mentre nel caso di $\overline{F}^{opt}$ abbiamo a disposizione delle informazioni a priori sullo stato da stimare: sappiamo che questo è della forma $|\psi_\phi\rangle$.

Chiariremo questo punto nei paragrafi successivi, dopo aver intrdotto la nozione di cloning ed avere stabilito un collegamento tra cloning e stima di stato.

Figura 1.1: Grafici di $F1(N) = \overline{F}^{opt}(N)$ e $F2(N) = \overline{F}^{opt}_{gen}(N)$, con scala logaritmica sull'asse N

# Capitolo 2

# CLONING DI STATI QUANTISTICI

## 2.1 Introduzione

In questo capitolo introduciamo il concetto di cloning di uno stato quantistico. Intuitivamente un clone di uno stato è una copia del medesimo identica all'originale. Il "teorema del no cloning" pone severe limitazioni sulle classi di stati che è possibile clonare esattamente utilizzando uno stesso cloner. In particolare, se predisponiamo un cloner T per lavorare su una classe di stati che ne contiene almeno due non ortogonali, esiste una limitazione di principio alla "qualità" dei cloni prodotti da T. Si pone quindi il problema di trovare, se esiste, il cloner ottimo, i.e. quello che produce cloni migliori. Questo sarà possibile solo dopo aver individuato la classe di cloners all'interno della quale cercare quello ottimo e dopo aver dato un criterio quantitativo di ottimalità.

Presentiamo qui due diversi approcci al problema della ricerca del cloner ottimo. Il primo, ispirato da [7] utilizza in maniera cruciale la forma esplicita della mappa T che definisce il cloning. Il secondo, ispirato da [15], utilizza una relazione tra la stima dello stato di N qubits ed il loro cloning ottimale per ricavare un limite superiore alla precisione con cui è possibile effettuare tale cloning. Quest'ultimo approccio ci servirà come riferimento per il lavoro originale che presenteremo nel prossimo capitolo.

## 2.2 Il cloning ideale

In questo paragrafo ci chiediamo se sia possibile in linea di principio costruire un apparato che, agendo opportunamente su un sistema quantistico in un certo stato $|\Psi\rangle \in \mathcal{C} \subseteq \mathcal{H}$, produca in uscita $M > 1$ cloni di tale sistema, ovvero M sistemi ciascuno descritto dalla matrice densità $\varrho = |\Psi\rangle\langle\Psi|$. La risposta a questa domanda dipende dalle caratteristiche dell'insieme $\mathcal{C} \subseteq \mathcal{H}$ che individua la classe di stati che vogliamo duplicare con il nostro apparato (che chiameremo "cloner" o "cloning machine" ideale). Infatti, se $\mathcal{C}$ contiene un solo stato, questo significa che lo stato da clonare è noto a priori e quindi sarà possibile produrne un numero arbitrario di copie. La situazione opposta si presenta invece se $\mathcal{C} \simeq \mathcal{H}$, ovvero se lo stato $|\Psi\rangle$ è completamente arbitrario. Supponiamo per assurdo che sia possibile produrre un clone di $|\Psi\rangle$: tramite una serie di procedure di clonazione identiche alla prima sarebbe possibile, in linea di principio, produrre infinite copie dello stato di partenza. Avremmo a disposizione a questo punto un ensemble di infiniti sistemi tutti nel medesimo stato $|\Psi\rangle$, utilizzabile per determinare completamente tale stato. Questo ci porta immediatamente ad una incongruenza: l'utilizzo della macchina per il cloning ideale ci ha permesso di determinare esattamente uno stato quantistico di cui avevamo a disposizione una sola copia, in contrasto con l'interpretazione statistica della funzione d'onda.

Dimostreremo ora[1] che si può attuare una procedura di clonazione ideale per qualsiasi classe $\mathcal{C}$ di stati mutuamente ortogonali, mentre questo non è possibile se in $\mathcal{C}$ sono presenti anche solo due stati non ortogonali fra loro. Possiamo rappresentare l'effetto della cloning machine ideale attraverso l'applicazione di un operatore unitario U che agisce sullo spazio di Hilbert:

$$\begin{aligned} \mathcal{H}' &= \mathcal{H} \otimes ... \otimes \mathcal{H} \otimes \mathcal{H}_{\mathrm{P}} = \\ &= \mathcal{H}^{\otimes \mathrm{M}} \otimes \mathcal{H}_{\mathrm{P}} \end{aligned}$$

dove $\mathcal{H}_{\mathrm{P}}$ è lo spazio di Hilbert del Probe (ovvero di parte della cloning machine stessa ed eventualmente di una parte dell'ambiente circostante), scelto in modo che il sistema complessivo risulti chiuso e quindi sia possibile descrive-

[1] In questo paragrafo seguiremo la trattazione di Ref.[16], [17]. Sempre a proposito del No Cloning Theorem si veda Ref.[19] in cui si dimostra che la cloning machine viola il principio di sovrapposizione, che si applica ad un numero minimo di *tre* stati, e quindi non esclude la possibilità di clonare *due* stati non ortogonali.

re la sua evoluzione attraverso un operatore unitario $U = \exp(-i\hat{H}t)$ con $\hat{H}$ Hamiltoniana del sistema complessivo. Abbiamo quindi:

$$U : \qquad \mathcal{H}' \longrightarrow \mathcal{H}' \tag{2.1}$$

$$|X\rangle \otimes |\Psi\rangle \otimes |\omega_1\rangle \otimes ... \otimes |\omega_{M-1}\rangle \longmapsto |X'(\Psi)\rangle \otimes |\Psi\rangle \otimes ... \otimes |\Psi\rangle \tag{2.2}$$

dove abbiamo denotato con $|\omega_1\rangle \otimes ... \otimes |\omega_{M-1}\rangle$ la preparazione (nota a priori) degli M-1 sistemi che supportano la procedura di cloning, mentre $|X\rangle$ è lo stato del Probe.

**Teorema del NO CLONING** *Consideriamo il caso in cui $\mathcal{C}$ contenga due stati $|\Psi\rangle, |\Phi\rangle$ con*

$$0 \leq |\langle\Psi|\Phi\rangle| \leq 1 \tag{2.3}$$

*La trasformazione (2.1) essendo unitaria, dovrà mantenere il prodotto scalare. Se facciamo il prodotto scalare al primo e al secondo membro della (2.2) per gli stati $|\Psi\rangle$ e $|\Phi\rangle$, otteniamo l'identità:*

$$\langle\Psi|\Phi\rangle = (\langle\Psi|\Phi\rangle)^M \langle X'(\Psi)|X'(\Phi)\rangle \tag{2.4}$$

*Dalla (2.4) segue che o i due stati in $\mathcal{C}$ sono ortogonali, i.e:*

$$\langle\Psi|\Phi\rangle = 0 \tag{2.5}$$

*oppure:*

$$(\langle\Psi|\Phi\rangle)^{M-1} \langle X'(\Psi)|X'(\Phi)\rangle = 1 \tag{2.6}$$

*Dalla (2.6), tenendo presente la (2.3), deduciamo la seguente disuguaglianza valida per $M > 1$:*

$$|\langle X(\Psi)|X(\Phi)\rangle| > 1 \tag{2.7}$$

*che non è verificata da nessuna coppia di vettori $|X(\Phi)\rangle$ e $|X(\Psi)\rangle$ con $0 < |\langle X(\Psi)|X(\Phi)\rangle| < 1$. La soluzione della (2.4) è data quindi da $\langle\Psi|\Phi\rangle = 0$ con $\langle X(\Psi)|X(\Phi)\rangle$ arbitrario, oppure da $\langle\Psi|\Phi\rangle = \langle X(\Psi)|X(\Phi)\rangle = e^{i\theta}$ con $\theta$ reale; nel secondo caso $|\Psi\rangle$ e $|\Phi\rangle$ rappresentano lo stesso stato.*

*In conclusione, abbiamo dimostrato che due differenti stati possono essere clonati dalla stessa cloning machine ideale* **se e solo se** *sono ortogonali. Se consideriamo un generico insieme $\mathcal{C} = \{|\Phi_i\rangle\}$, applicando i ragionamenti appena presentati arriviamo alla conclusione che gli stati $|\Phi_i\rangle$ devono essere mutuamente ortogonali tra loro se vogliamo che vengano clonati dalla medesima cloning machine ideale. Si giunge alle medesime conclusioni anche se U è anti-unitario.*

È quindi possibile realizzare un cloner ideale solo per stati ortogonali. Ma, a parte questo caso particolare in cui è noto a priori che gli stati all'ingresso del cloner costituiscono un insieme di stati mutuamente ortogonali, in generale il cloning ideale non è realizzabile. Esisteranno comunque delle macchine per la clonazione che realizzano il cloning in maniera imperfetta. Definendo opportunamente la "bontà" dei cloni prodotti da tali apparati, sarà possibile confrontare tra loro diverse macchine e determinare il cloner ottimale. Prima di affrontare questo problema, cominciamo con qualche osservazione di carattere generale.

Pensiamo di costruire un cloner, che chiameremo cloner classico, che realizzi sul sistema in ingresso la misura di un set di parametri $\boldsymbol{\theta}$, tramite i quali sia possibile ricostruire lo stato quantistico del sistema in ingresso con un certo grado di precisione. Come abbiamo visto i risultati di tale misura si possono vedere come un punto $\boldsymbol{\theta}_*$ nello spazio dei parametri $\Theta$ di dimensione m opportuna. Dopo aver copiato M volte i risultati $\boldsymbol{\theta}_*$ della stima di $\boldsymbol{\theta}$, il nostro cloner classico utilizza gli M punti $\boldsymbol{\theta}_*$ per produrre M copie dello stato in ingresso. Siccome l'accuratezza nella stima di un generico stato aumenta se si hanno a disposizione un numero maggiore di copie[2], avremo che il nostro cloner funzionerà tanto "meglio" quante più copie dello stato da clonare gli daremo in ingresso. Inoltre, non ci saranno limiti al numero di cloni ottenibili in questo modo poiché la m-pla $(\theta_{*1}, ..., \theta_{*m})$ costituisce un'informazione di tipo classico, ovvero è riproducibile e utilizzabile un numero arbitrario di volte (anche infinite). È naturale chiedersi a questo punto se sia possibile ottenere dei cloni "migliori" nel caso in cui si abbia bisogno solamente di un numero finito di copie.

Nei prossimi paragrafi affronteremo proprio il problema di trovare la cloning machine ottima fissati il numero di copie in ingresso e quelle in uscita. Vedremo che in generale c'è una relazione tra il numero di cloni e la loro qualità.

[2]Nel §1.6, abbiamo visto che nel caso particolare dei qubits $\overline{F}^{opt}(N)$ è una funzione non decrescente di N e che $\lim_{N\to\infty} \overline{F}^{opt}(N) = 1$.

## 2.3 Cloning ottimale universale

### 2.3.1 Impostazione del problema

Consideriamo due individui, Alice ($\mathcal{A}$) che controlla gli stati in ingresso ad una cloning machine e Bob ($\mathcal{B}$) che possiede la cloning machine e osserva gli stati da essa prodotti in uscita. $\mathcal{A}$ sceglie la preparazione per un sistema quantistico, descrivibile attraverso un'opportuna matrice densità $\varrho$:

$$\varrho : \mathcal{H} \longrightarrow \mathcal{H}$$

dove $\mathcal{H}$ è lo spazio di Hilbert di tale sistema. $\mathcal{A}$ ripete poi la procedura di preparazione N volte, producendo un sistema composto nello spazio di Hilbert $\mathcal{H}^{\otimes \mathrm{N}} \equiv \mathcal{H} \otimes ... \otimes \mathcal{H}$, descrivibile tramite la matrice densità $\varrho^{\otimes N}$. Quindi $\mathcal{A}$ spedisce il suo sistema a $\mathcal{B}$, il quale ha a disposizione una cloning machine T (da lui scelta) che, dati gli N sistemi come input, produce M sistemi ($M > N$) come output. Parametri fissati in questo schema sono $d = dim(\mathcal{H})$, N e M. Se vogliamo risolvere il problema di trovare la cloning machine che realizzi la procedura di cloning (con parametri d, N e M fissati) in maniera ottimale, dobbiamo prima definire le proprietà di un generico cloner T. Questo si può fare in due modi equivalenti, nei quali si caratterizza T tramite la sua azione sui sistemi quantistici in ingresso.

**I.Approccio assiomatico** *Definiamo T come una mappa:*

$$\begin{aligned} T: \quad End(\mathcal{H}^{\otimes N}) &\longrightarrow End(\mathcal{H}^{\otimes M}) \\ \nu_N &\longmapsto T(\nu_N) \end{aligned}$$

*dove $End(\mathcal{H}^{\otimes N})$ e $End(\mathcal{H}^{\otimes M})$ sono gli spazi in cui sono definite rispettivamente le matrici densità di input (abbiamo indicato con $\nu_N$ la generica matrice densità con supporto su $\mathcal{H}^{\otimes N}$) e quelle di output. Richiediamo inoltre che T abbia le seguenti proprietà*

- *LINEARITÀ: in modo che rispetti le combinazioni convesse di stati in ingresso.*
- *COVARIANZA: $T(U^{\otimes N} \nu_N U^{*\otimes N}) = U^{\otimes M} T(\nu_N) U^{*\otimes M} \ \forall\, U \in SU(d)$. Come vedremo questa proprietà è necessaria se si vuole che il cloner tratti indistintamente ogni stato in ingresso.*

- *CONSERVAZIONE DELLA TRACCIA: in modo che T conservi la normalizzazione.*

- *COMPLETA POSITIVITÀ: T deve mandare elementi positivi in elementi positivi (positività) e inoltre se facciamo una generica estensione di $\mathcal{H}^{\otimes N}$:*

$$\mathcal{H}^{\otimes N} \longmapsto \mathcal{H}' \equiv \mathcal{H}^{\otimes N} \otimes \mathcal{H}$$

*ed estendiamo per linearità T su $\mathcal{H}'$, l'estensione T' di T applicata alla generica matrice densità $\nu' \in End(\mathcal{H}')$ deve essere ancora una mappa positiva.*

**II.Definizione costruttiva** *La generica cloning machine può eseguire solo operazioni che facciano interagire in modo unitario il sistema in input con un sistema ausiliario (Probe). Sarà poi possibile descrivere l'evoluzione di un sottinsieme opportuno del sistema complessivo tracciando parzialmente sulla restante parte del sistema.*

Osserviamo che ciascuno degli step definiti in (II) si realizza tramite una mappa completamente positiva (CP map) che conservi la traccia. Quindi se una macchina quantistica è ammissibile secondo (II) lo è anche secondo (I). Si può dimostrare[3] che ogni operatore lineare completamente positivo e che conservi la traccia si può costruire seguendo le "istruzioni" date in (II). Le due definizioni (I) e (II) sono perciò equivalenti. Nel seguito di questo lavoro utilizzeremo principalmente la (I).

La descrizione dell'evoluzione di un sistema quantistico attraverso una CP map risulta necessaria ogniqualvota il sistema stesso sia aperto. L'idea fondamentale è che considerando un'opportuna estensione $\mathcal{H}' = \mathcal{H} \otimes \mathcal{H}_P$ dello spazio di Hilbert $\mathcal{H}$ del sistema, è possibile ricondursi ad un sistema esteso di tipo Hamiltoniano, i.e. la cui evoluzione sia data da un operatore unitario $U_t = \exp(-i\hat{H}t)$ dove $\hat{H}$ è l'operatore hamiltoniano del sistema complessivo. Se ci interessa solo l'evoluzione del sistema originario, è sufficiente tracciare parzialmente su $\mathcal{H}_{\mathrm{P}}$. L'applicazione

$$\begin{aligned} End(\mathcal{H}) &\longrightarrow End(\mathcal{H}) \\ Tr_P(|\psi\rangle\langle\psi|) &\longmapsto Tr_P(U|\psi\rangle\langle\psi|U^*) \end{aligned}$$

è una CP map[4].

[3] Si veda Ref.[22].

[4] Una breve trattazione delle CP map e delle loro proprietà si può trovare in Ref.[21].

### 2.3.2 La "bontà" del cloning

A questo punto si pone il problema di esprimere la "bontà" del cloning. A tal fine cominciamo a fare le due scelte fondamentali:

- $\mathcal{A}$ prepara uno stato puro[5] $\omega^{\otimes N} = [\,|\phi\rangle\langle\phi|\,]^{\otimes N}$, $|\phi\rangle \in \mathcal{H}$
- Versione "Many-Particles-Test" (MPT)[6] del problema del cloning: esprimeremo la bontà del cloning confrontando lo stato del sistema completo di M particelle di output $T(\omega^{\otimes N})$ con lo stato $\omega^{\otimes M}$ che $\mathcal{A}$ può ottenere facilmente ripetendo la procedura di preparazione M volte invece di N.

Quindi definiamo la seguente quantità che chiameremo Fidelity:

$$F(T,\omega) = Tr[\omega^{\otimes M}\, T(\omega^{\otimes N})] \tag{2.8}$$

Osserviamo che la Fidelity di una cloning machine ideale vale 1. Un buon cloner sarà quindi descritto da una mappa T per la quale la Fidelity sia più possibile vicino ad 1 per ogni scelta di $\omega$ iniziale. Se indichiamo con F(T) il risultato peggiore ottenibile con il cloner T, i.e:

$$F(T) = \inf_{\omega\, puro} Tr[\omega^{\otimes M}\, T(\omega^{\otimes N})] \tag{2.9}$$

il problema di trovare la cloning machine ottima si riduce a massimizzare F(T) al variare di T con fissati d, N e M.

### 2.3.3 Descrizione della cloning machine ottima

Diamo qui la descrizione della cloning machine ottima, lasciando la dimostrazione di ottimalità al sottoparagrafo seguente. Utilizzando l'approccio **I** di §2.3.1, descriviamo una generica cloning machine come una mappa T:

$$T : End(\mathcal{H}^{\otimes \mathrm{N}}) \longrightarrow End(\mathcal{H}^{\otimes \mathrm{M}})$$

[5] Da questo punto in poi indicheremo con $\omega$ la generica matrice densità relativa ad uno stato *puro*.

[6] Questa nomenclatura viene introdotta in Ref.[7] per distinguere questa impostazione del problema dalla versione "One-Particle-Test" utilizzata, ad esempio, in Ref.[15], di cui parleremo più avanti.

con le proprietà già citate. Osserviamo che è possibile restringere il dominio di T, poiché gli stati in ingresso sono della forma $\omega^{\otimes N}$. Il sottospazio di $\mathcal{H}^{\otimes \mathrm{N}}$ che supporta tali stati è generato dai vettori della forma:

$$\phi^{\otimes N} = \phi \otimes ... \otimes \phi$$

e non è altro che lo spazio dei vettori invarianti per tutte le permutazioni, che indicheremo con $\mathcal{H}_+^{\otimes \mathrm{N}}$. Scelta una base $\{|e_i\rangle\}_{i=1,...,d}$ nello spazio di Hilbert $\mathcal{H}$ di una particella, il generico vettore $|\phi\rangle \in \mathcal{H}$ sarà individuato dai coefficienti $(\phi_1, ..., \phi_d)$ del suo sviluppo sulla base data:

$$|\phi\rangle \simeq (\phi_1, ..., \phi_d)$$

Canonicamente associata alla base $\{|e_i\rangle\}$ per $\mathcal{H}$ è la base per $\mathcal{H}_+^{\otimes \mathrm{N}}$ (detta del numero di occupazione) $\{|n_1...n_d\rangle\}$ con $\sum_i n_i = N$, dove il generico $n_i$ indica il numero di particelle del sistema complessivo che si trovano nello stato $|e_i\rangle$ di particella singola. Si può esprimere $\phi^{\otimes N}$ nella base appena introdotta come segue:

$$\phi^{\otimes N} = \sqrt{N!} \sum_{n_1,...,n_d} \delta(\sum_i n_i - N) \prod_{k=1}^{d} \frac{\phi_k^{n_k}}{\sqrt{n_k!}} |n_1...n_d\rangle \tag{2.10}$$

Il numero di vettori del tipo $|n_1...n_d\rangle$ con la condizione $\sum_i n_i = N$ è pari al numero di partizioni di N in d interi. La dimensione di $\mathcal{H}_+^{\otimes \mathrm{N}}$ è quindi:

$$d[N] = (-1)^N \binom{-d}{N} = \binom{d+N-1}{N} \tag{2.11}$$

Una delle proprietà cruciali del sottospazio simmetrico è che gli operatori unitari $U^{\otimes N}$ ($U \in SU(d)$) trasformano $\mathcal{H}_+^{\otimes \mathrm{N}}$ in se stesso e agiscono irriducibilmente su questo sottospazio[7]. Se indichiamo con $S_N$ il proiettore ortogonale di $\mathcal{H}^{\otimes \mathrm{N}}$ su $\mathcal{H}_+^{\otimes \mathrm{N}}$, un generico operatore $\hat{A}$ supportato da $\mathcal{H}_+^{\otimes \mathrm{N}}$ è caratterizzato dalla proprietà $\hat{A} = \hat{A}S_N = S_N\hat{A}$. Inoltre se $\hat{A}$ commuta con tutti gli $U^{\otimes N}$, il primo lemma di Schur ci dice che $\hat{A}$ è un multiplo dell'operatore identità

[7]Come sappiamo, uno spazio di Hilbert di dimensione finita d supporta la rappresentazione irriducibile fondamentale [d] di SU(d). Sullo spazio di Hilbert $\mathcal{H}^{\otimes \mathrm{N}}$ sono definiti i tensori a N indici (bassi); possiamo dividere tali tensori nelle loro componenti irriducibili con processi di simmetrizzazione e antisimmetrizzazione. In SU(d) non c'è altro modo per ridurre la dimensione, per cui tensori con una definita simmetria sono irriducibili (si veda a questo proposito Ref.[10]). $\mathcal{H}_+^{\otimes \mathrm{N}}$ è il sottospazio di $\mathcal{H}^{\otimes \mathrm{N}}$ che contiene i tensori con gli indici *completamente* simmetrizzati.

su $\mathcal{H}_+^{\otimes \mathrm{N}}$, cioè di $S_N$. Siccome la cloning machine ideale $\overline{T}$ ha come stato di arrivo $\omega^{\otimes M}$, che è supportato da $\mathcal{H}_+^{\otimes \mathrm{M}}$, possiamo ragionevolmente supporre che la mappa $\hat{T}$ associata alla cloning machine[8] ottimale abbia come codominio $End(\mathcal{H}_+^{\otimes \mathrm{M}})$. Questo significa che gli M cloni in uscita sono tutti descritti dalla medesima matrice densità. Otterremo la cloning map ottimale $\hat{T}$ in due passaggi successivi. Il primo consiste nel definire l'applicazione triviale:

$$\begin{aligned} End(\mathcal{H}_+^{\otimes \mathrm{N}}) &\longrightarrow End(\mathcal{H}^{\otimes \mathrm{M}}) \\ \varrho_N &\longmapsto \varrho_N \otimes \hat{I}^{\otimes (M-N)} \end{aligned}$$

dove $\varrho_N$ è la generica matrice densità supportata da $\mathcal{H}_+^{\otimes \mathrm{N}}$, mentre $\hat{I}^{\otimes (M-N)}$ è l'operatore identità su $\mathcal{H}^{\otimes (M-N)}$. Per fare in modo che il codominio dell'applicazione appena definita sia $End(\mathcal{H}_+^{\otimes \mathrm{M}})$ proiettiamo l'operatore $\varrho_N \otimes \hat{I}^{\otimes (M-N)}$ su tale sottospazio tramite $S_M$. La cloning map così ottenuta e correttamente normalizzata è:

$$\hat{T}(\varrho_N) = \frac{d[N]}{d[M]} S_M (\varrho_N \otimes \hat{I}^{\otimes (M-N)}) S_M \tag{2.12}$$

Dimostreremo successivamente che $\hat{T}$ è ottima. Per ora cominciamo a verificare che essa soddisfa le proprietà che avevamo richiesto per una generica mappa di cloning.

- La linearità segue immediatamente dalla distributività della somma rispetto al prodotto tensoriale e dalla linearità di $S_M$.

- Per dimostrare che la mappa $\hat{T}$ è covariante, cominciamo con l'osservare che ogni matrice densità $\varrho_N$ con supporto su $\mathcal{H}_+^{\otimes \mathrm{N}}$ si può scrivere[9] come combinazione lineare del prodotto tensoriale di stati puri identici tra loro

  $$\varrho_N = \sum_i \alpha_i \left[ |\psi_i\rangle\langle\psi_i| \right]^{\otimes N} \tag{2.13}$$

  con $\sum_i \alpha_i = 1$ e $|\psi_i\rangle \in \mathcal{H}$. Utilizzando questa proprietà ed indicando $|\psi_i\rangle\langle\psi_i|$ con $\omega_i$, abbiamo:

  $$U^{\otimes M} \hat{T}(\varrho_N) U^{*\otimes M} = \frac{d[N]}{d[M]} U^{\otimes M} S_M (\varrho_N \otimes \hat{I}^{\otimes (M-N)}) S_M U^{*\otimes M} =$$

[8] Tale mappa sarà chiamata d'ora in poi *cloning map*.

[9] Si veda a questo proposito Ref.[7].

$$
\begin{aligned}
&= \frac{d[N]}{d[M]} S_M U^{\otimes M} (\varrho_N \otimes \hat{I}^{\otimes (M-N)}) U^{*\otimes M} S_M = \\
&= \frac{d[N]}{d[M]} \sum_i \alpha_i S_M \left[ (U \omega_i U^*)^{\otimes N} \otimes (U \hat{I} U^*)^{\otimes (M-N)} \right] S_M = \\
&= \frac{d[N]}{d[M]} \sum_i \alpha_i S_M \left[ (U \omega_i U^*)^{\otimes N} \otimes \hat{I}^{\otimes (M-N)} \right] S_M = \\
&= \frac{d[N]}{d[M]} S_M \left[ U^{\otimes N} \varrho_N \, U^{*\otimes N} \otimes \hat{I}^{\otimes (M-N)} \right] S_M = \\
&= \hat{T}(U^{\otimes N} \varrho_N \, U^{*\otimes N})
\end{aligned}
$$

che è la proprietà di covarianza. Si noti che ci siamo serviti dell'uguaglianza $S_M U^{\otimes M} = U^{\otimes M} S_M$, che segue dal fatto che gli operatori unitari $U^{\otimes M}$ agiscono irriducibilmente su $\mathcal{H}_+^{\otimes \mathrm{M}}$ e che $S_M$ è l'identità in tale sottospazio.

- Conservazione della traccia. Poiché $Tr[\hat{T}(\varrho_N)]$ è un funzionale lineare di $\varrho_N$ si può scrivere come $Tr(\varrho_N \hat{X})$ con $\hat{X}$ opportuno operatore su $\mathcal{H}_+^{\otimes \mathrm{N}}$ positivo. Utilizzando la proprietà di covarianza appena dimostrata abbiamo che:

$$
\begin{aligned}
Tr[\hat{T}(U^{\otimes N} \varrho_N \; U^{*\otimes N})] &= Tr[U^{\otimes M} T(\varrho_N) U^{*\otimes M}] = Tr[T(\varrho_N)] = Tr[\varrho_N \hat{X}] = \\
&= Tr[U^{\otimes N} \varrho_N \; U^{*\otimes N} \hat{X}] \;\; \forall \varrho_N
\end{aligned}
$$

da cui segue, utilizzando come nel primo passaggio l'invarianza della traccia per permutazioni cicliche, $\hat{X} U^{\otimes N} = U^{\otimes N} \hat{X}$. Quindi per il primo lemma di Schur $\hat{X}$ è della forma $\hat{X} = \lambda S_N$, cioè un multiplo dell'identità su $\mathcal{H}_+^{\otimes \mathrm{N}}$. Ci rimane da dimostrare che $\lambda = 1$, da cui segue immediatamente:

$$
Tr[\hat{T}(\varrho_N)] = Tr[\varrho_N \hat{X}] = Tr[\varrho_N S_N] = Tr[\varrho_N] = 1
$$

per ogni $\varrho_N$ supportata da $\mathcal{H}_+^{\otimes \mathrm{N}}$. Per dimostrare che $\lambda = 1$ è sufficiente trovare una particolare $\varrho_N$ la cui traccia sia preservata da $\hat{T}$. Scegliendo $\varrho_N = \tau_N = d[N]^{-1} S_N$ ($\tau_N$ è il proiettore su $\mathcal{H}_+^{\otimes \mathrm{N}}$ con la corretta normalizzazione) abbiamo:

$$
\begin{aligned}
\hat{T}(\tau_N) &= d[M]^{-1} S_M (S_N \otimes \hat{I}^{\otimes (M-N)}) S_M = \\
&= d[M]^{-1} S_M = \tau_M
\end{aligned}
$$

da cui:

$$Tr[\hat{T}(\tau_N)] = Tr[\tau_M] = 1$$

che è quello che ci rimaneva da dimostrare.

- La positività segue osservando che $\varrho_N$, $\hat{I}^{\otimes(M-N)}$ e $S_M$ sono operatori positivi. Osserviamo inoltre che l'applicazione di $S_M$ è una CP map, poiché l'estensione di un proiettore è un proiettore, che è un operatore positivo. Siccome anche l'estensione

$$\varrho_N \longmapsto \varrho_N \otimes \hat{I}^{\otimes(M-N)}$$

è una CP map e la composizione di CP maps è ancora una mappa CP, T è a sua volta CP.

Per determinare il valore di $F(\hat{T})$ cominciamo col definire la media $\underline{T}$ di una generica mappa di cloning T rispetto al gruppo SU(d) degli operatori unitari U su $\mathcal{H}$:

$$\underline{T}(\varrho_N) = \int dU\, U^{*\otimes M} T(U^{\otimes N} \varrho_N U^{*\otimes N}) U^{\otimes M} \tag{2.14}$$

dove $dU$ denota l'integrazione rispetto alla misura di Haar normalizzata del gruppo SU(d). La linearità di $\underline{T}$ segue da quella di T, mentre la sua covarianza e la completa positività sono evidenti. Dalla covarianza segue immediatamente che $Tr[\underline{T}(\varrho_N)] = 1$, infatti:

$$\begin{aligned} Tr[\underline{T}(\varrho_N)] &= \int dU\, Tr[U^{*\otimes M} T(U^{\otimes N} \varrho_N U^{*\otimes N}) U^{\otimes M}] = \\ &= \int dU\, Tr[T(\varrho_N)] = \int dU = 1 \end{aligned}$$

Qiundi $\underline{T}$ è una mappa di cloning ammissibile. Dimostriamo ora il seguente

**Teorema 2.3.1** *La generica mappa di cloning $T$ è covariante se e solo se $T = \underline{T}$*

**Dimostrazione** *Se $T$ è covariante l'uguaglianza $T = \underline{T}$ segue immediatamente dalla definizione di covarianza. Viceversa se $T = \underline{T}$ abbiamo che*

$$T(\varrho_N) = \int dU\, U^{*\otimes M} T(U^{\otimes N} \varrho_N U^{*\otimes N}) U^{\otimes M}$$

*che possiamo riscrivere nel seguente modo:*

$$\int dU\, T(\varrho_N) = \int dU\, U^{*\otimes M} T(U^{\otimes N} \varrho_N U^{*\otimes N}) U^{\otimes M}$$

*da cui*

$$T(\varrho_N) = U^{*\otimes M} T(U^{\otimes N} \varrho_N U^{*\otimes N}) U^{\otimes M}$$

*cioè*

$$T(U^{\otimes N} \varrho_N U^{*\otimes N}) = U^{\otimes M} T(\varrho_N) U^{*\otimes M}$$

*che è la proprietà di covarianza per la mappa T.*

Ora, siccome $\hat{T}$ è una mappa covariante, utilizzando il teorema appena dimostrato possiamo scrivere:

$$\hat{T} = \underline{\hat{T}} = \int dU\, U^{*\otimes M} \hat{T}(U^{\otimes N} \varrho_N U^{*\otimes N}) U^{\otimes M} \tag{2.15}$$

da cui deduciamo che:

$$\begin{aligned}
F(\hat{T}) &= \inf_{\omega\, puro} Tr[\omega^{\otimes M} \hat{T}(\omega^{\otimes N})] = \\
&= \inf_{\omega\, puro} Tr[\omega^{\otimes M} \underline{\hat{T}}(\omega^{\otimes N})] = \\
&= \inf_{\omega\, puro} Tr\left[\omega^{\otimes M} \int dU\, U^{*\otimes M} \hat{T}(U^{\otimes N} \omega^{\otimes N} U^{*\otimes N}) U^{\otimes M}\right] = \\
&= \inf_{\omega\, puro} Tr\left[\int dU\, \omega^{\otimes M} U^{*\otimes M} \hat{T}(U^{\otimes N} \omega^{\otimes N} U^{*\otimes N}) U^{\otimes M}\right] = \\
&= \inf_{\omega\, puro} Tr\left[\int dU\, U^{\otimes M} \omega^{\otimes M} U^{*\otimes M} \hat{T}(U^{\otimes N} \omega^{\otimes N} U^{*\otimes N})\right]
\end{aligned}$$

Siccome ogni $\omega'^{\otimes N}$ supportata da $\mathcal{H}_+^{\otimes \mathrm{N}}$ e con $\omega'$ stato puro è un proiettore su un sottospazio di dimensione uno, si può scrivere $\omega'^{\otimes N} = U^{\otimes N} \omega^{\otimes N} U^{*\otimes N}$ con $\omega$ stato puro arbitrario e U opportunamente scelto. Da questo fatto deduciamo che la quantità

$$Tr\left[\int dU\, U^{\otimes M} \omega^{\otimes M} U^{*\otimes M} \hat{T}(U^{\otimes N} \omega^{\otimes N} U^{*\otimes N})\right]$$

non dipende da $\omega$, per cui:

$$F(\hat{T}) = Tr[\omega^{\otimes N} \hat{T}(\omega^{\otimes N})] = \tag{2.16}$$

$$= \frac{d[N]}{d[M]} Tr[\omega^{\otimes N} S_M (\omega^{\otimes N} \otimes \hat{I}^{\otimes (M-N)}) S_M] = \tag{2.17}$$

$$= \frac{d[N]}{d[M]} Tr[\omega^{\otimes N}] = \frac{d[N]}{d[M]} \tag{2.18}$$

Nel valutare la traccia in (2.17) abbiamo considerato il fatto che $\omega$ è uno stato puro su $\mathcal{H}$ e quindi $\omega^{\otimes N}$ è un proiettore uno-dimensionale che proietta su un sottospazio di $\mathcal{H}_+^{\otimes \mathrm{N}}$ di dimensione minore dei sottospazi su cui proiettano sia $S_M$ che $(\omega^{\otimes N} \otimes \hat{I}^{\otimes(M-N)})$.

### 2.3.4 Dimostrazione di ottimalità

Dimostreremo in questo sottoparagrafo che la mappa di cloning $\hat{T}$ definita in equazione (2.12) è ottima, nel senso che massimizza la funzione $F(T)$ definita in (2.9). Sia

$$\hat{F} = \sup_T F(T) \tag{2.19}$$

**Teorema 2.3.2** *Per ogni mappa $T$ che descrive un cloning con $N$ copie in ingresso e $M$ in uscita, vale la disuguaglianza:*

$$F(T) \leq \frac{d[N]}{d[M]}$$

*L'uguaglianza è verificata se e solo se $T = \hat{T}$.*

**Dimostrazione** *Sia $T$ una mappa che descrive un cloner ottimo ($F(T) = \hat{F}$). Per ogni $\omega$ puro abbiamo quindi che:*

$$Tr[\omega^{\otimes M} \underline{T}(\omega^{\otimes N})] = \int dU\, Tr[U^{\otimes M} \omega^{\otimes M} U^{*\otimes M} T(U^{\otimes N} \omega^{\otimes N} U^{*\otimes N})] \tag{2.20}$$

$$\geq \int dU\, F(T) = \hat{F} \tag{2.21}$$

*dove la (2.20) deriva direttamente dalla definizione di $\underline{T}$, mentre la disuguaglianza (2.21) segue immediatamente dalla definizione di $F(T)$ e tenendo conto che $T$ è covariante e ottima. Infatti dalla covarianza, utilizzando il Teorema 2.3.1, abbiamo*

$$F(T) = F(\underline{T}) = \inf_{\omega\ puro} \int dU\, Tr\left[U^{\otimes M} \omega^{\otimes M} U^{*\otimes M} T(U^{\otimes N} \omega^{\otimes N} U^{*\otimes N})\right]$$

*Poiché $T$ è ottima $F(T) = \hat{F}$; inoltre*

$$\begin{aligned} \inf_{\omega\ puro} \int dU\, Tr\left[U^{\otimes M} \omega^{\otimes M} U^{*\otimes M} T(U^{\otimes N} \omega^{\otimes N} U^{*\otimes N})\right] = \\ \leq \int dU\, Tr\left[U^{\otimes M} \omega^{\otimes M} U^{*\otimes M} T(U^{\otimes N} \omega^{\otimes N} U^{*\otimes N})\right] = \\ = Tr\left[\omega^{\otimes M} \underline{T}(\omega^{\otimes N})\right] \end{aligned}$$

*Come abbiamo già notato in §2.3.3 il membro di sinistra della (2.20) non dipende da $\omega$ e quindi è uguale a $F(\underline{T})$, da cui $F(\underline{T}) \geq \hat{F}$. Dalla definizione di $\hat{F}$ segue anche che $\hat{F} \geq F(\underline{T})$. Quindi se $T$ è ottima abbiamo che:*

$$F(\underline{T}) = \hat{F}$$

*Poiché sia $F(\underline{T})$ che $\hat{F}$ sono quantità positive possiamo scrivere:*

$$\int dU\, Tr[U^{\otimes M}\omega^{\otimes M}U^{*\otimes M}T(U^{\otimes N}\omega^{\otimes N}U^{*\otimes N})] - \int dU\, \hat{F} = 0$$

*da cui*

$$Tr[\omega^{\otimes M}T(\omega^{\otimes N})] = F(T) = \hat{F} \;\; \forall\omega$$

*Consideriamo a questo punto l'operatore $\tau_N = d[N]^{-1}S_N$, che essendo multiplo di $S_N$ commuta con gli operatori unitari $U^{\otimes N}$. Utilizzando questa proprietà di $\tau_N$ insieme alla covarianza di $\underline{T}$ abbiamo:*

$$\begin{aligned} \underline{T}(\tau_N) &= \underline{T}(U^{\otimes N}\tau_N U^{*\otimes N}) \\ &= U^{\otimes M}\underline{T}(\tau_N)U^{*\otimes M} \end{aligned}$$

*cioè $\underline{T}(\tau_N)$ commuta con gli operatori $U^{\otimes M}$, che ristretti a $\mathcal{H}_+^{\otimes M}$ sono una rappresentazione irriducibile. Utilizzando il primo lemma di Schur abbiamo che $\underline{T}\left(\frac{S_N}{d[N]}\right)$ è un multiplo dell'identità su $\mathcal{H}_+^{\otimes M}$. Se indichiamo con "Rest" una matrice densità sul complemento ortogonale $(\mathcal{H}_+^{\otimes M})^{\perp}$ di $\mathcal{H}_+^{\otimes M}$ in $\mathcal{H}^{\otimes M}$ (si noti che l'immagine della mappa $\underline{T}$ potrebbe essere in linea di principio uno spazio più esteso di $End(\mathcal{H}_+^{\otimes M})$) possiamo scrivere:*

$$\underline{T}\left(\frac{S_N}{d[N]}\right) = \lambda\frac{S_M}{d[M]} + (1-\lambda)Rest \tag{2.22}$$

*dove il coefficiente $(1-\lambda)$ con $0 \leq \lambda \leq 1$ assicura la conservazione della normalizzazione.*

*Calcoliamo ora la seguente quantità:*

$$\begin{aligned} Tr[\omega^{\otimes M}\underline{T}(S_N - \omega^{\otimes N})] &= Tr[\omega^{\otimes M}\underline{T}(S_N)] - Tr[\omega^{\otimes M}\underline{T}(\omega^{\otimes N})] = \\ &= \frac{d[N]}{d[M]}\,\lambda Tr[\omega^{\otimes M}S_M] + \\ &\quad +(1-\lambda)d[N]\,Tr[\omega^{\otimes M}\,Rest] - \hat{F} = \\ &= \frac{d[N]}{d[M]}\lambda\, Tr[\omega^{\otimes M}S_M] - \hat{F} \end{aligned}$$

*dove l'ultimo passaggio segue dal fatto che la traccia è stata eseguita sul sottospazio $\mathcal{H}_+^{\otimes M}$, mentre l'operatore "Rest" da risultati diversi da zero solo se lo si applica a stati in $(\mathcal{H}_+^{\otimes M})^\perp$. Siccome $Tr[\omega^{\otimes M}\underline{T}(S_N - \omega^{\otimes N})]$ deve essere un operatore positivo, abbiamo che:*

$$\frac{d[N]}{d[M]}\lambda\, Tr[\omega^{\otimes M} S_M] - \hat{F} = \lambda\frac{d[N]}{d[M]} - \hat{F} \geq 0 \tag{2.23}$$

*Perciò*

$$\hat{F} \leq \lambda\frac{d[N]}{d[M]} \leq \frac{d[N]}{d[M]}$$

*Poiché in (2.18) abbiamo mostrato che $F(\hat{T}) = \frac{d[N]}{d[M]}$ abbiamo che $\hat{F} = \frac{d[N]}{d[M]}$ e che $\hat{T}$ è ottima. In Ref.[7] si dimostra anche che $\hat{T}$ è l'unica mappa di cloning che raggiunge il valore $\hat{F}$.*

## 2.4 Cloning ottimale universale di qubits

Consideriamo un sistema costituito da N qubits ciascuno nello stato puro descritto dalla matrice densità $\omega = |\psi\rangle\langle\psi|$, con $|\psi\rangle \in \mathcal{H} \simeq \mathbb{C}^2$. Caratteristica peculiare di un qubit è il fatto che è possibile stabilire una corrispondenza tra la matrice densità che descrive il suo stato $\omega$ ed un vettore $\mathbf{S} \in \mathbb{R}^3$, detto vettore di Bloch e così definito:

$$\mathbf{S} = Tr[\omega\boldsymbol{\sigma}] \tag{2.24}$$

dove $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ e $\sigma_i$ $(i = x, y, z)$ sono le matrici di spin di Pauli:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.25}$$

Possiamo scrivere la matrice densità $\omega$ nel seguente modo:

$$\omega = \frac{1}{2}(\hat{I} + \mathbf{S}\cdot\boldsymbol{\sigma}) \tag{2.26}$$

Calcoliamoci ora $\omega^2$:

$$\begin{aligned} \omega^2 &= \frac{1}{4}(\hat{I} + \mathbf{S}\cdot\boldsymbol{\sigma})(\hat{I} + \mathbf{S}\cdot\boldsymbol{\sigma}) = \\ &= \frac{1}{4}(\hat{I} + 2\mathbf{S}\cdot\boldsymbol{\sigma} + \hat{I}(\mathbf{S}\cdot\boldsymbol{\sigma})^2) = \\ &= \frac{1}{4}(\hat{I} + 2\mathbf{S}\cdot\boldsymbol{\sigma} + \hat{I}|\mathbf{S}|^2) \end{aligned}$$

e richiediamo che $\omega$ descriva uno stato puro. Imponendo che $\omega^2 = \omega$ otteniamo la condizione $|\mathbf{S}|^2 = 1$, che è l'equazione di una sfera di raggio unitario in $\mathbb{R}^3$ che chiameremo sfera di Bloch. Quindi tutti e soli gli stati descritti da una $\omega$ il cui vettore di Bloch sia tale che $|\mathbf{S}|^2 = 1$ sono stati puri. D'altra parte, tenendo conto della positività di $\omega$, abbiamo che per stati non puri $|\mathbf{S}|^2 < 1$.

Consideriamo ora la generica cloning map T

$$\begin{aligned} T : End(\mathcal{H}_+^{\otimes \mathrm{N}}) &\longrightarrow End(\mathcal{H}_+^{\otimes \mathrm{M}}) \\ \varrho_N &\longmapsto T(\varrho_N) \end{aligned}$$

con le proprietà discusse in §2.3.1. È possibile esprimere la bontà del cloning da essa realizzato in un modo diverso da quello esposto in §2.3.2, che si basa sull'idea di confrontare lo stato di uno degli N qubits in ingresso con quello di uno degli M cloni in uscita (OPT, "One-Particle-Test version of the cloning problem") invece di considerare grandezze relative al sistema completo di M particelle (MPT). A tal fine cominciamo col definire per ogni matrice densità $\varrho_N$ supportata da $\mathcal{H}_+^{\otimes \mathrm{N}}$ la sua restrizione $R(\varrho_N)$ supportata da $\mathcal{H}$ tramite la relazione:

$$Tr[R(\varrho_N)\hat{A}] = Tr[\varrho_N(\hat{A} \otimes \hat{I}^{\otimes(N-1)})] \; \forall \hat{A} \in End(\mathcal{H}) \tag{2.27}$$

Per $\varrho_N = \omega^{\otimes N}$ il secondo membro della (2.27) diventa:

$$\begin{aligned} Tr[\varrho_N(\hat{A} \otimes \hat{I}^{\otimes(N-1)})] &= Tr[\omega\hat{A}]\, Tr[\omega^{\otimes(N-1)}\hat{I}^{\otimes(N-1)}] = \\ &= Tr[\omega\hat{A}] \end{aligned}$$

Siccome l'uguaglianza vale per ogni operatore $\hat{A}$, concludiamo che

$$R(\omega^{\otimes N}) = \omega = Tr_{N-1}(\omega^{\otimes N}) \tag{2.28}$$

dove con $Tr_{N-1}$ abbiamo indicato la traccia parziale fatta sugli spazi di Hilbert di N-1 qubits anziché N. Consideriamo ora $R(T(\omega^{\otimes N}))$. Poiché il codominio di T è $End(\mathcal{H}_+^{\otimes \mathrm{M}})$, utilizzando la (2.13) avremo che

$$R(T(\omega^{\otimes N})) = Tr_{M-1}[T(\omega^{\otimes N})]$$

Utilizzando la proprietà di covarianza di T è facile mostrare che per ogni U tale che $U\omega = \omega U$ si ha $U^{\otimes M}\, R(T(\omega^{\otimes N})) = R(T(\omega^{\otimes N}))\, U^{\otimes M}$. Infatti se $U\omega = \omega U$ abbiamo anche che $U^{\otimes N}\omega^{\otimes N}U^{*\otimes N} = \omega^{\otimes N}$, da cui:

$$R(T(U^{\otimes N}\omega^{\otimes N}U^{*\otimes N})) = R(T(\omega^{\otimes N})) \tag{2.29}$$

Inoltre, sempre utilizzando la forma data in equazione (2.13) per una generica matrice densità $\varrho_M$ supportata da $\mathcal{H}_+^{\otimes \mathrm{M}}$

$$T(\omega^{\otimes N}) = \sum_i \alpha_i \omega_i^{\otimes M}$$

abbiamo:

$$\begin{aligned} R(T(U^{\otimes N}\omega^{\otimes N}U^{*\otimes N})) &= R(U^{\otimes M}T(\omega^{\otimes N})U^{*\otimes M}) = \\ &= \sum_i \alpha_i Tr_{M-1}\left[U^{\otimes M}\omega_i^{\otimes M}U^{*\otimes M}\right] = \\ &= \sum_i \alpha_i U\omega_i U^* = UR(T(\omega^{\otimes N}))U^* \end{aligned} \tag{2.30}$$

Dalle (2.29) e (2.30) deduciamo immediatamente che $R(T(\omega^{\otimes N}))$ commuta con tutti gli U che commutano con $\omega$. Da questa proprietà di $R(T(\omega^{\otimes N}))$ segue che possiamo scrivere:

$$R(T(\omega^{\otimes N})) = \gamma(T)\omega + [1-\gamma(T)]\tau_1 \tag{2.31}$$

con $\tau_1 = d^{-1}\hat{I}$ e $\gamma(T)$ fattore dipendente dai parametri d,N e M che specificano la mappa T, ma indipendente da $\omega$.

In letteratura un cloner che agisce su uno stato $\omega^{\otimes N}$ producendo M cloni, ciascuno in uno stato descritto dalla (2.31) si dice universale. La ragione di tale nomenclatura è che la sua azione è indipendente dallo stato $\omega$ in ingresso ed è descrivibile tramite il fattore $\gamma(T)$. Si noti che per ottenere l'universalità è stato necessario utilizzare la proprietà di covarianza di T[10].

Se specializziamo la (2.31) al caso $d = 2$ e indichiamo $\gamma(2, N, M)$ con $\eta(N, M)$ abbiamo:

$$R(T(\omega^{\otimes N})) = \eta(N,M)\omega + \frac{1}{2}[1-\eta(N,M)]\hat{I} \tag{2.32}$$

dove $\hat{I}$ è la matrice identità su $\mathbb{C}^2$. Osserviamo che inserendo la (2.26) nella (2.32) otteniamo:

$$R(T(\omega^{\otimes N})) = \frac{1}{2}(\hat{I} + \eta(N,M)\mathbf{S}\cdot\boldsymbol{\sigma}) \tag{2.33}$$

[10]Abbiamo così una giustificazione di quanto asserito all'inizio del capitolo e cioè che la covarianza è necessaria se si vuole che l'azione del cloner sia indipendente dallo stato in ingresso.

Notiamo subito che per $\eta(N,M) = 1$ la (2.33) ci dice che $R(T(\omega^{\otimes N})) = \omega$ e quindi $T(\omega^{\otimes N}) = \omega^{\otimes M}$, ovvero T è un cloner ideale. Poiché questo non è possibile avremo sempre $0 < \eta(N,M) < 1$. Il parametro $\eta(N,M)$ descrive la contrazione del vettore di Bloch $\mathbf{S}' = (\eta(N,M)\mathbf{S})$ di ciascuno degli M qubits in uscita rispetto a $\mathbf{S}$, vettore di Bloch di ciascuno degli N cloni in ingresso (che ha modulo unitario). Si noti che gli M qubits in uscita si troveranno sicuramente in uno stato non puro, poiché il cloner non è ideale e quindi $\eta(N,M) < 1$.

Definiamo ora la quantità

$$\begin{aligned} F(T) &= Tr[\omega R(T(\omega^{\otimes N}))] = & (2.34)\\ &= Tr[\omega^2 \eta(N,M) + \frac{1}{2}[1-\eta(N,M)]\omega] = & (2.35)\\ &= \eta(N,M) + \frac{1}{2}(1-\eta(N,M)) = \frac{1}{2}(1+\eta(N,M)) & (2.36) \end{aligned}$$

che non è altro che l'equivalente della Fidelity definita in (2.8) o equivalentemente in (2.9), non essendoci in questo caso alcuna dipendenza esplicita dallo stato in ingresso[11]. Anche in questo caso $0 \leq F(T) \leq 1$, con $F(T) = 1$ per T cloner ideale. Il problema di trovare il cloner $\hat{T}$ che realizzi il cloning ottimale si può ricondurre anche qui a quello di massimizzare la quantità $F(T)$, ovvero a quello di trovare il limite superiore per la quantità $\eta(T) = \eta(N,M)$.

Presentiamo ora una procedura per ricavare il limite superiore per $\eta(N,M)$ (che indicheremo con $\eta_{opt}(N,M)$), che non utilizza la forma esplicita della cloning map che lo realizza. Notiamo a questo proposito che la mappa $\hat{T}$ di (2.12), non è necessariamente quella tale che

$$\eta(\hat{T}) = \eta_{opt}(N,M) \tag{2.37}$$

poiché la grandezza con cui esprimiamo ora la bontà del cloning è diversa. È quindi cruciale che la procedura che utilizzeremo nel seguito non faccia alcun uso della forma esplicita della mappa di cloning ottima, in quanto questa non è a priori nota. Una volta determinata la quantità $\eta_{opt}$ dimostreremo che vale l'uguaglianza (2.37).

Cominciamo concatenando due macchine per il cloning nel modo seguente. Il primo cloner è descritto dalla cloning map $T_{MN}$, dove i pedici M e N indicano

[11] Chiameremo F(T) Fidelity come la quantità di (2.8), anche se è importante sottolineare la differenza nei due approcci presentati. Il primo, infatti, effettua il test della bontà del cloning su stati a M particelle (MPT), mentre il secondo utilizza stati a 1 particella (OPT).

rispettivamente il numero di cloni prodotti e il numero di qubits in ingresso, a cui associamo il rispettivo "fattore di contrazione" $\eta(N, M)$ che, come appena visto, lo descrive in modo completo tramite la (2.32). Gli M cloni in uscita dal primo cloner sono utilizzati come input dal secondo ($T_{\infty M}$), il quale ne crea infinite copie con fattore di contrazione $\eta(M, \infty)$. Scriviamo ora due importanti risultati, di cui daremo dimostrazione dettagliata nel seguito:

- **I.**Il fattore di contrazione di una macchina per il cloning ottenuta concatenandone altre due è uguale al prodotto dei fattori di contrazione di queste ultime.
- **II.**Vale l'uguaglianza

$$\eta_{opt}(N, \infty) = \overline{\eta}^{mis}_{g-opt}(M) \tag{2.38}$$

  dove $\overline{\eta}^{mis}_{g-opt}(M)$ è una quantità direttamente collegata alla Fidelity media (1.36) per la stima dello stato di un sistema di M qubits[12].

Utilizzando (**I**) abbiamo immediatamente che se pensiamo ai due cloners concatenati $T_{MN}$ e $T_{\infty M}$ come ad un unico cloner $T^{conc}_{\infty N}$

$$T^{conc}_{\infty N} : N \longrightarrow \infty$$

questo sarà descritto dal fattore di contrazione prodotto dei loro rispettivi fattori di contrazione. Chiaramente il cloner $T^{conc}_{\infty N}$ non potrà lavorare meglio del cloner ottimale $T^{opt}_{\infty N}$. Dalla definizione stessa di ottimalità segue quindi immediatamente la seguente disuguaglianza

$$\eta(N, M)\eta(M, \infty) \leq \eta_{opt}(N, \infty) \tag{2.39}$$

dalla quale otteniamo:

$$\eta(N, M) \leq \frac{\eta_{opt}(N, \infty)}{\eta(M, \infty)} \tag{2.40}$$

Poiché $\eta(M, \infty)$ è una quantità compresa fra 0 e 1, otteniamo il più basso limite superiore per il fattore di contrazione di un generico cloner $N \longrightarrow M$ tramite la seguente sostituzione:

$$\eta(N, M) \leq \frac{\eta_{opt}(N, \infty)}{\eta_{opt}(M, \infty)} \tag{2.41}$$

[12]Spiegheremo più in dettaglio di cosa si tratti nei paragrafi successivi

Ora ci basta utilizzare (**II**) e la forma esplicita per $\overline{\eta}^{mis}_{g-opt}(M)$:

$$\overline{\eta}^{mis}_{g-opt}(M) = \frac{M}{M+2} \tag{2.42}$$

per concludere che per ogni $M \geq N$

$$\eta_{opt}(N, M) \leq \frac{N}{M}\frac{M+2}{N+2} \tag{2.43}$$

In particolare in [6] è mostrata una mappa di cloning che raggiunge il valore $\frac{N}{M}\frac{M+2}{N+2}$, per cui la (2.43) è effettivamente una uguaglianza. Utilizzando la (2.36) si ottiene la Fidelity ottima:

$$F^{opt}(N, M) = \frac{NM + N + M}{M(N+2)} \tag{2.44}$$

Calcoliamoci ora la quantità $\gamma(\hat{T}_{MN})$ con $\hat{T}_{MN}$ dato nell'equazione (2.12). Siccome $\hat{T}$ conserva la traccia, abbiamo che $Tr[\hat{T}(\omega^{\otimes N})] = 1$, ovvero

$$Tr\left[\frac{d[N]}{d[M]} S_M(\omega^{\otimes N} \otimes \hat{I}^{\otimes(M-N)}) S_M\right] = 1$$

da cui:

$$Tr\left[S_M(\omega^{\otimes N} \otimes \hat{I}^{\otimes(M-N)})\right] = \frac{d[M]}{d[N]}$$

per ogni $\omega$ stato puro. Utilizzeremo questo risultato nel seguente calcolo:

$$\begin{aligned}
Tr[\omega R(T(\omega^{\otimes N}))] &= Tr[(\omega \otimes \hat{I}^{\otimes(M-1)}) T(\omega^{\otimes N})] = \\
&= \frac{1}{M}\sum_k Tr[\omega^{(k)} T(\omega^{\otimes N})] = \\
&= \frac{d[N]}{M\, d[M]}\sum_k Tr[\omega^{(k)} S_M(\omega^{\otimes N} \otimes \hat{I}^{\otimes(M-N)}) S_M] = \\
&= \frac{d[N]}{M\, d[M]}\sum_k Tr[\omega^{(k)}(\omega^{\otimes N} \otimes \hat{I}^{\otimes(M-N)}) S_M] = \\
&= \frac{d[N]}{M\, d[M]} Tr\left[S_M \sum_k \omega^{(k)}(\omega^{\otimes N} \otimes \hat{I}^{\otimes(M-N)})\right] = \\
&= \frac{d[N]}{M\, d[M]}\Big[N\, Tr[S_M(\omega^{\otimes N} \otimes \hat{I}^{\otimes(M-N)})] + \\
&\quad + (M-N) Tr[S_M(\omega^{\otimes(N+1)} \otimes \hat{I}^{\otimes(M-N-1)})]\Big] =
\end{aligned}$$

$$
\begin{aligned}
&= \frac{d[N]}{M\, d[M]} \left\{ N \frac{d[M]}{d[N]} + (M-N) \frac{d[M]}{d[N+1]} \right\} = \\
&= \frac{N}{M} + \frac{M-N}{M} \frac{N+1}{d+N}
\end{aligned}
$$

Nella seconda linea abbiamo indicato con l'abbreviazione $\omega^{(k)}$ il prodotto tensoriale di M operatori che sono tutti uguali all'operatore identità tranne il k-simo che è invece uguale a $\omega$. Nella quarta linea, invece, abbiamo utilizzato la proprietà di $\sum_k \omega^{(k)}$ di essere invariante per tutte le permutazioni e quindi di commutare con $S_M$. La quantità $Tr[\omega R(T(\omega^{\otimes N}))]$ si può calcolare anche nel modo seguente:

$$
\begin{aligned}
Tr[\omega R(T(\omega^{\otimes N}))] &= Tr[\omega\gamma(T)\omega] + Tr[\omega(1-\gamma(T))\tau_1] = \\
&= \gamma(T) + (1-\gamma(T))d^{-1}
\end{aligned}
$$

Uguagliando le due espressioni ottenute e risolvendo rispetto a $\gamma(T)$ si ottiene:

$$
\gamma(\hat{T}) = \frac{N}{d+N} \frac{d+M}{M} \tag{2.45}
$$

Specializzando il risultato per d=2 troviamo

$$
\eta(\hat{T}) = \frac{N}{M} \frac{M+2}{N+2} \tag{2.46}
$$

da cui deduciamo che la cloning map $\hat{T}$ è ottima anche rispetto al criterio di ottimalità OPT esposto in questo paragrafo.

### 2.4.1 Dimostrazione della proprietà di concatenazione

Come già osservato in §2.3.3 una matrice densità $\varrho_M$ con supporto su $\mathcal{H}_+^{\otimes \mathrm{M}}$ si può scrivere come combinazione lineare del prodotto tensoriale di stati puri identici tra loro

$$
\varrho_M = \sum_i \alpha_i [|\psi_i\rangle\langle\psi_i|]^{\otimes M} \tag{2.47}
$$

con $\sum_i \alpha_i = 1$ (si noti che non si è fatta alcuna richiesta di positività sui coefficienti $\alpha_i$). Utilizzando la (2.47) è possibile estendere la (2.31) al caso in cui la mappa di cloning T non agisca su uno stato puro. Utilizzando la linearità di T e il fatto che $\gamma(T)$ non dipende dallo stato in ingresso al cloner possiamo scrivere:

$$
R(T(\varrho_M)) = \gamma(T) R(\varrho_M) + [1-\gamma(T)]\tau_1 \tag{2.48}
$$

con

$$R(\varrho_M) = Tr_{M-1}(\varrho_M) = \sum_i \alpha_i |\psi_i\rangle\langle\psi_i|$$

La (2.48) riscritta nel caso particolare d=2 diventa:

$$R(T(\varrho_M)) = \eta(T)R(\varrho_M) + \frac{1}{2}[1-\eta(T)]\hat{I} \tag{2.49}$$

Le (2.48) e (2.49) ci dicono che un generico cloner T è sempre descrivibile tramite il suo fattore $\gamma(T)$ (o il suo fattore di contrazione per qubits), indipendentemente dal fatto che lo stato a N particelle in ingresso sia puro o no, purché la matrice densità che descrive quest'ultimo abbia supporto sul sottospazio simmetrico $\mathcal{H}_+^{\otimes N}$.

Supponiamo ora di concatenare un cloner $N \longrightarrow M$, che individuiamo tramite il fattore $\gamma(T_{MN}) = \gamma_{MN}$, con un cloner $M \longrightarrow L$, a cui è associato il fattore $\gamma(T_{LM}) = \gamma_{LM}$. Il risultato della concatenazione può essere visto come un cloner $N \longrightarrow L$ a cui sarà associata la mappa di cloning $T_{LN}$ così definita:

$$T_{LN} = T_{LM} \circ T_{MN}$$

Per chiarezza diamo una rappresentazione diagrammatica della situazione in cui ci troviamo:

$$\begin{array}{ccccc} N & \xrightarrow{T_{MN}} & M & \xrightarrow{T_{LM}} & L \\ \omega^{\otimes N} & \longrightarrow & T_{MN}(\omega^{\otimes N}) & \longrightarrow & T_{LM} \circ T_{MN}(\omega^{\otimes N}) \end{array}$$

$$\begin{array}{ccc} N & \xrightarrow{T_{LN}} & L \\ \omega^{\otimes N} & \longrightarrow & T_{LN}(\omega^{\otimes N}) \end{array}$$

Utilzzando la (2.31) abbiamo[13]

$$R(T_{LN}(\omega^{\otimes N})) = \gamma_{LN}\omega + [1-\gamma_{LN}]\tau_1$$

e anche

$$R(T_{MN}(\omega^{\otimes N})) = \gamma_{MN}\omega + [1-\gamma_{MN}]\tau_1$$

[13]Ricordiamo che $\omega$ è stato puro.

da cui:

$$\begin{aligned} R(T_{LN}(\omega^{\otimes N})) &= R(T_{LM}(T_{MN}(\omega^{\otimes N}))) = \\ &= \gamma_{LM} R(T_{MN}(\omega^{\otimes N})) + [1-\gamma_{LM}]\tau_1 = \\ &= \gamma_{LM}[\gamma_{MN}\omega + (1-\gamma_{MN})\tau_1] + (1-\gamma_{LM})\tau_1 = \\ &= \gamma_{LM}\gamma_{MN}\omega + [1-\gamma_{LM}\gamma_{MN}]\tau_1 \end{aligned}$$

dove nel passaggio tra la prima e la seconda riga abbiamo utilizzato la (2.48) siccome $T_{MN}(\omega^{\otimes N})$ non è uno stato puro. Confrontando le due espressioni ottenute per $R(T_{LN}(\omega^{\otimes N})$ otteniamo l'uguaglianza

$$\gamma_{LN} = \gamma_{LM}\gamma_{MN} \tag{2.50}$$

che esprime la proprietà di concatenazione che volevamo ricavare.

### 2.4.2 Dimostrazione dell'uguaglianza $\overline{\eta}^{mis}_{g-opt}(M) = \eta_{opt}(N,\infty)$

Come già esposto nel §1.6, dati M qubits ciascuno dei quali nello stato non noto $|\psi\rangle$, esiste una POVM $\{P_\mu\}$ che fornisce la stima ottima dello stato $|\psi\rangle$ con Fidelity media

$$\overline{F}^{opt}_{gen}(M) = \frac{M+1}{M+2}$$

Il risultato di ciascuna misura sul sistema di M qubits fornisce con probabilità

$$p_\mu(\psi) = Tr[P_\mu(|\psi\rangle\langle\psi|)^{\otimes M}]$$

il "candidato" $|\psi_\mu\rangle$ per $|\psi\rangle$. Utilizzando i risultati di diverse misurazioni possiamo calcolarci la quantità

$$\begin{aligned} \overline{F}^{opt}_{g-mis}(M) &= \sum_\mu p_\mu(\psi)|\langle\psi|\psi_\mu\rangle|^2 = & (2.51) \\ &= \langle\psi|\overline{\varrho}|\psi\rangle & (2.52) \end{aligned}$$

dove

$$\overline{\varrho} = \sum_\mu p_\mu(\psi)|\psi_\mu\rangle\langle\psi_\mu|$$

costituisce lo stato "ricostruito" attraverso la serie di misurazioni effettuate. Siccome la quantità (2.52) non deve dipendere da $|\psi\rangle$, abbiamo che $\overline{\varrho}$ può essere scritto come segue:

$$\overline{\varrho} = \overline{\eta}^{mis}_{g-opt}(M)|\psi\rangle\langle\psi| + \frac{1}{2}[1-\overline{\eta}^{mis}_{g-opt}(M)]\hat{I} \tag{2.53}$$

con $\overline{\eta}^{mis}_{g-opt}(M) = 2\overline{F}^{opt}_{g-mis}(M) - 1$. È evidente dalla (2.53) che l'effetto della procedura di stima dello stato di un qubit avendone a disposizione M copie è traducibile (come nel caso del cloning) attraverso il fattore $\overline{\eta}^{mis}_{g-opt}(M)$ che dà l'accorciamento del vettore di Bloch dello stato originale. Dopo la stima dello stato $|\psi\rangle$ è possibile in linea di principio produrre un numero arbitrario di copie (anche infinite) di tale stato con una precisione esprimibile tramite la quantità $\overline{F}^{mis}_{g-opt}$. Possiamo pensare alla procedura di stima ottima descritta come ad un cloning $M \longrightarrow \infty$. Introduciamo quindi la mappa S[14]

$$S : End(\mathcal{H}_+^{\otimes \mathrm{M}}) \longrightarrow End(\mathcal{H}_+^{\otimes \infty})$$

lineare, completamente positiva e che conservi la traccia. Se rivediamo i ragionamenti utilizzati per arrivare all'equazione (2.31), vediamo che è possibile avere l'ulteriore proprietà

$$R(S(|\psi\rangle\langle\psi|^{\otimes M})) = \overline{\varrho}$$

richiedendo che S sia covariante rispetto al gruppo $SU(2)$. Dimostreremo ora che la cloning map S è quella che realizza il cloning $M \longrightarrow \infty$ in maniera ottimale. A tal fine cominciamo con l'osservare che la cloning machine descritta da S non potrà sicuramente lavorare meglio del cloner ottimale $M \longrightarrow L$ per ogni $L \geq M$ e in particolare per $L \longrightarrow \infty$. Segue quindi la seguente disuguaglianza

$$\overline{\eta}^{mis}_{g-opt}(M) \leq \eta^{opt}(M, L) \ \forall L \geq M \tag{2.54}$$

Per raggiungere il nostro obiettivo ci rimane da dimostrare che per $L \longrightarrow \infty$ la (2.54) diventa una uguaglianza. Concateniamo ora un cloner $M \longrightarrow L$ con una successiva stima di stato ottima. Lo stato degli M qubits in ingresso al cloner è descrivibile attraverso la matrice densità $(|\psi\rangle\langle\psi|)^{\otimes M}$, mentre l'output da $\varrho_L = \sum_i \alpha_i (|\psi_i\rangle\langle\psi_i|)^{\otimes L}$ con $\sum_i \alpha_i = 1$. Poiché $\varrho_L \in End(\mathcal{H}_+^{\otimes L})$, la matrice densità ridotta $\varrho$ che descrive lo stato di ciascuno degli L qubits di output sarà:

$$\begin{aligned} \varrho = Tr_{L-1}[\varrho_L] &= \sum_i \alpha_i |\psi_i\rangle\langle\psi_i| = \\ &= \eta(M, L)|\psi\rangle\langle\psi| + \frac{1}{2}[1 - \eta(M, L)]\hat{I} \end{aligned}$$

[14]La mappa S riassume la procedura attraverso la quale, dopo diverse misure, si arriva a stimare lo stato $\varrho$ attraverso lo stato "ricostruito" $\overline{\varrho}$.

Il cloner $M \longrightarrow L$ concatenato con la stima dello stato fatta sul sistema degli L qubits si può vedere come una stima di stato eseguita direttamente sul sistema di M qubits. La fidelity relativa a questa procedura si può scrivere nella maniera seguente:

$$\begin{aligned}
\overline{F}_{mis}(M) &= \langle\psi| \sum_{\mu} Tr(P_\mu \varrho_L)|\psi_\mu\rangle\langle\psi_\mu|\psi\rangle = \\
&= \sum_{\mu,i} \langle\psi|\alpha_i Tr[P_\mu(|\psi_i\rangle\langle\psi_i|)^{\otimes L}]|\psi_\mu\rangle\langle\psi_\mu|\psi\rangle = \\
&= \sum_{i} \langle\psi|\alpha_i \Big[\overline{\eta}^{mis}_{opt}(L)|\psi_i\rangle\langle\psi_i| + \frac{1}{2}[1-\overline{\eta}^{mis}_{opt}(L)]\hat{I}\Big]|\psi\rangle
\end{aligned}$$

Siccome $\lim_{L\to\infty} \overline{\eta}^{mis}_{opt}(L) = 1$ abbiamo che

$$\begin{aligned}
\overline{F}_{mis}(M) \xrightarrow{L\to\infty} \quad & \textstyle\sum_i \langle\psi|\alpha_i|\psi_i\rangle\langle\psi_i|\psi\rangle = \langle\psi|\varrho|\psi\rangle = \\
& = \tfrac{1}{2}[1+\eta(M,\infty)]
\end{aligned}$$

Il risultato della concatenazione di un cloner con una stima di stato ottimale non può dare un risultato migliore di una stima di stato ottimale; abbiamo quindi la seguente disuguaglianza:

$$\eta^{opt}(M,\infty) \leq \overline{\eta}^{mis}_{g-opt}(M) \tag{2.55}$$

Combinando le disuguaglianze (2.54) e (2.55) otteniamo infine

$$\eta^{opt}(M,\infty) = \overline{\eta}^{mis}_{g-opt}(M) \tag{2.56}$$

che prova quanto volevamo dimostrare.

## 2.5 Conclusioni

Dall'espressione per il fattore $\gamma(T)$ del cloner universale (d,N,M) ottimo $\hat{T}$

$$\gamma(\hat{T}) = \frac{N}{d+N}\frac{d+M}{M} \tag{2.57}$$

vediamo che, come anticipato nel §2.2, c'è una relazione tra il numero di cloni prodotti e la loro qualità. Infatti per (d,N) fissati, $\gamma(\hat{T})$ è una funzione decrescente di M. Questo significa che più copie si vogliono in uscita, minore è la precisione con cui queste copie si possono produrre. Se invece fissiamo (d,M)

$\gamma(\hat{T})$ è funzione crescente di N, cioè dando più copie in ingresso si ottengono cloni migliori.

Per finire, osserviamo che il cloner $T_{MN}$ ottimo, non può essere caratterizzato da una procedura intermedia di tipo classico in cui si determina lo stato del sistema in ingresso per poi produrne il numero richiesto di copie. Se così fosse, infatti, il cloner $T_{MN}$ sarebbe caratterizzato dal fattore $\gamma(d, N, \infty)$ che per d fissato è minore di $\gamma(d, N, M)$ per ogni M, in contrasto con l'ipotesi di ottimalità.

Nelle figure 2.1 e 2.2 riportiamo i grafici di $\eta(N, M)$ per ogni $M > N$ e come funzione di M per N=1,2,3.

Figura 2.1: Grafico di $e(N, M) = \eta_{opt}(N, M)$, con $(M > N)$ e scala logaritmica sull'asse N.

Figura 2.2: Grafici di $e(1, M) = \eta_{opt}(1, M)$, $e(2, M) = \eta_{opt}(2, M)$, $e(3, M) = \eta_{opt}(3, M)$ con $(M > N)$ a confronto.

# Capitolo 3

# CLONING DI QUBITS EQUATORIALI E STIMA DI FASE

## 3.1 Introduzione

Nel capitolo 2 abbiamo considerato un cloner $N \longrightarrow M$ covariante rispetto al gruppo SU(2)[1] e abbiamo visto che richiedere tale proprietà per la mappa T che lo descrive, corrisponde a richiedere che il cloner agisca allo stesso modo (i.e. tramite il fattore di contrazione $\eta(N, M)$) su un qualsiasi stato $|\psi\rangle \in \mathcal{H}$ in ingresso.

In questo capitolo indeboliremo la condizione di covarianza. Individueremo poi una classe $\mathcal{C} \subset \mathcal{H}$ di stati sui quali l'azione del cloner sarà ancora esprimibile tramite un fattore di contrazione $\eta\prime(N, M)$. Il fatto che la classe di stati $\mathcal{C}$, sui cui faremo lavorare il nostro cloner, sia un sottoinsieme proprio di $\mathcal{H}$ è sinonimo di una maggiore informazione a priori sugli stati da clonare. Ci aspettiamo quindi che sia possibile effettuare il cloning di tali stati in maniera "più precisa" (ovvero con una Fidelity maggiore) rispetto a quello che si può fare con un cloner universale (per il quale $\mathcal{C} \simeq \mathcal{H}$), i.e:

$$\eta\prime_{opt}(N, M) \geq \eta_{opt}(N, M) \quad \forall\, M \geq N$$

[1] Come già sottolineato, in letteratura tale cloner viene spesso chiamato *Cloner Universale*.

## 3.2 Cloning ottimale covariante in fase di qubits

### 3.2.1 Impostazione del problema

Prendiamo in considerazione un generico $N \longrightarrow M$ cloner di qubits, che specifichiamo tramite la cloning map T

$$\begin{array}{rcl} T : End(\mathcal{H}_+^{\otimes \mathrm{N}}) & \longrightarrow & End(\mathcal{H}_+^{\otimes \mathrm{M}}) \ \mathcal{H} \simeq \mathbb{C}^2 \\ \varrho_N & \longmapsto & T(\varrho_N) \end{array}$$

con le proprietà:

- Linearità, completa positività, conservazione della traccia[2]
- COVARIANZA rispetto al gruppo degli operatori unitari $U_\phi$:

$$\begin{array}{rcl} U_\phi & = & \exp\left[-\frac{i}{2}(\sigma_z - 1)\phi\right] = \\ & = & \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \end{array}$$

  Notiamo subito che al variare di $\phi$ in $[0, 4\pi]$ gli operatori $U_\phi$ costituiscono un sottogruppo U(1) di SU(2). In analogia alla notazione introdotta nel §1.4, se la mappa di cloning T soddisfa la

$$T(U_\phi^{\otimes N} \varrho_N U_\phi^{*\otimes N}) = U_\phi^{\otimes M} T(\varrho_N) U_\phi^{*\otimes M} \quad \forall\, \phi \tag{3.1}$$

  diremo che T è covariante in fase.

Per individuare una classe di stati $\mathcal{C}$ sulla quale la cloning map $T$ agisce attraverso un fattore di contrazione $\eta\prime(N, M)$ e ancor prima per vedere se effettivamente tale classe esista, è necessario calcolare la quantità $R(T(\varrho_N))$. Il passo successivo sarà poi quello di trovare il più basso limite superiore per il fattore $\eta\prime(N, M)$. Per eseguire tale ottimizzazione utilizzeremo una procedura simile a quella descritta in §2.4.

### 3.2.2 Calcolo di $R(T(\varrho_N))$ per $\varrho_N \in End(\mathcal{H}_+^{\otimes \mathbf{N}})$

Prima di procedere al calcolo di $R(T(\varrho_N))$ osserviamo che se scriviamo

$$\varrho_N = \sum_i \alpha_i \omega_i^{\otimes N} \tag{3.2}$$

[2]Queste proprietà sono le stesse che avevamo richiesto per un cloner universale in §2.3.1.

con $\omega_i$ stato puro, per la linearità di T e dell'operazione di traccia possiamo restringerci al calcolo di $R(T(\omega^{\otimes N}))$ con $\omega^{\otimes N}$ stato puro.
Dividiamo la seguente trattazione in punti, in ciascuno dei quali utilizziamo in maniera cruciale una delle proprietà richieste per la mappa T al fine di arrivare al calcolo esplicito di $R(T(\omega^{\otimes N}))$.

- Completa positività (I). Utilizzando la forma canonica per una CP-map data da Kraus[3], e osservando che $R(T(\omega^{\otimes N}))$ è una CP-map

$$R(T(\omega^{\otimes N})) : End(\mathcal{H}_+^{\otimes \mathrm{N}}) \longrightarrow End(\mathcal{H})$$

possiamo scrivere:

$$R(T(\omega^{\otimes N})) = \sum_k A_k \omega A_k^\dagger \tag{3.3}$$

con $A_k$ generici operatori lineari su $\mathcal{H}$ tali che:

$$\sum_k A_k^\dagger A_k = \hat{I} \tag{3.4}$$

Consideriamo la $\mathbb{C}$-algebra $\mathcal{A}$ degli operatori lineari su $\mathcal{H}$

$$\mathcal{A} = \{ A \,|\, A : \mathcal{H} \longrightarrow \mathcal{H}, \text{ lineare} \}$$

$\mathcal{A}$ è isomorfa all'algebra ML(2,$\mathbb{C}$) delle matrici 2x2 a elementi complessi con determinante diverso da zero[4]. Osserviamo che $dim(ML(2,\mathbb{C})) = 4$. Scegliamo per $ML(2,\mathbb{C})$ la base $\sigma_\alpha$ ($\alpha$=0,1,2,3) con

$$\sigma_0 \equiv \sigma_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \sigma_1 \equiv \sigma- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 \equiv \pi_+ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \sigma_3 \equiv \pi_- = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

e scriviamo:

$$A_k = \sum_{\alpha=0}^{3} c_k^\alpha \sigma_\alpha \tag{3.5}$$

[3]Si veda ref.[18].
[4]L'invertibilità segue dalla linearità.

con $c_k^\alpha \in \mathbb{C}$. Abbiamo quindi che

$$\begin{aligned} R(T(\omega^{\otimes N})) &= \sum_k \sum_{\alpha,\beta=0}^{3} c_k^\alpha c_k^{*\beta} \sigma_\alpha \omega \sigma_\beta^\dagger = \\ &= \sum_k \sum_{\alpha,\beta=0}^{3} \gamma_k^{\alpha\,\beta} \sigma_\alpha \omega \sigma_\beta^\dagger = \\ &= \sum_{\alpha,\beta=0}^{3} \Gamma^{\alpha\,\beta} \Sigma_{\alpha\,\beta}(\omega) \end{aligned} \tag{3.6}$$

con

$$\gamma_k^{\alpha\,\beta} \equiv c_k^\alpha c_k^{*\beta}, \qquad \Sigma_{\alpha\,\beta}(\omega) \equiv \sigma_\alpha \omega \sigma_\beta^\dagger \quad e \quad \Gamma^{\alpha\,\beta} \equiv \sum_k \gamma_k^{\alpha\,\beta}$$

Dalla (3.6) vediamo che $R(T(\omega^{\otimes N}))$ si può scrivere come combinazione lineare dei 16 elementi $\Sigma_{\alpha\beta}(\omega)$, che chiamiamo "generatori" della CP-map T. Osseviamo inoltre che

$$\sigma_0^\dagger = \sigma_1, \quad \sigma_1^\dagger = \sigma_0, \quad \sigma_2^\dagger = \sigma_2, \quad \sigma_3^\dagger = \sigma_3$$

- Covarianza in fase. Se T è covariante in fase abbiamo per definizione che

$$T(U_\phi^{\otimes N} \omega^{\otimes N} U_\phi^{*\otimes N}) = U_\phi^{\otimes M} T(\omega^{\otimes N}) U_\phi^{*\otimes M} \tag{3.7}$$

da cui

$$\begin{aligned} R(T(U_\phi^{\otimes N} \omega^{\otimes N} U_\phi^{*\otimes N})) &= Tr_{M-1}(T(U_\phi^{\otimes N} \omega^{\otimes N} U_\phi^{*\otimes N}) = \\ &= Tr_{M-1}(U_\phi^{\otimes M} T(\omega^{\otimes N}) U_\phi^{*\otimes M}) = \\ &= U_\phi R(T(\omega^{\otimes N})) U_\phi^* \end{aligned} \tag{3.8}$$

L'ultimo passaggio segue immediatamente se si scrive

$$T(\omega^{\otimes N}) = \sum_i \alpha_i \omega_i^{\otimes M}$$

Infatti

$$\begin{aligned} Tr_{M-1}\left[U_\phi^{\otimes M} T(\omega^{\otimes N}) U_\phi^{*\otimes N}\right] &= \sum_i \alpha_i Tr_{M-1}\Big[(U_\phi \otimes U_\phi^{\otimes(M-1)})(\omega_i \otimes \\ &\qquad \otimes \omega_i^{\otimes(M-1)})(U_\phi^* \otimes U_\phi^{*\otimes(M-1)})\Big] = \\ &= \sum_i U \alpha_i \omega_i U^* = \\ &= U Tr_{M-1} T(\omega^{\otimes N}) U^* \end{aligned}$$

Sostituendo nei due membri di (3.8) l'espressione per $R(T(\omega^{\otimes N}))$ trovata in (3.6) otteniamo:

$$\begin{aligned} R(T(U_\phi^{\otimes N}\omega^{\otimes N}U_\phi^{*\otimes N})) &= R\left[T((U_\phi\omega U_\phi^*)^{\otimes N})\right] = \\ &= \sum_{\alpha,\beta}\Gamma^{\alpha\beta}\Sigma_{\alpha\beta}(U_\phi\omega U_\phi^*) \end{aligned} \tag{3.9}$$

e anche

$$U_\phi R(T(\omega^{\otimes N}))U_\phi^* = \sum_{\alpha,\beta}\Gamma^{\alpha\beta}U_\phi\Sigma_{\alpha\beta}(\omega)U_\phi^* \tag{3.10}$$

La condizione di covarianza in fase diventa perciò:

$$\sum_k\sum_{\alpha,\beta}\gamma_k^{\alpha\beta}\Sigma_{\alpha\beta}(U_\phi\omega U_\phi^*) = \sum_k\sum_{\alpha,\beta}\gamma_k^{\alpha\beta}U_\phi\Sigma_{\alpha\beta}(\omega)U_\phi^* \tag{3.11}$$

In Appendice B mostriamo che la (3.11) dà le seguenti condizioni sui coefficienti $\Gamma^{\alpha\beta}$

$$\begin{aligned} &\Gamma^{01} = \Gamma^{02} = \Gamma^{03} = 0 \\ &\Gamma^{10} = \Gamma^{12} = \Gamma^{13} = 0 \\ &\Gamma^{20} = \Gamma^{21} = 0 \\ &\Gamma^{30} = \Gamma^{31} = 0 \end{aligned} \tag{3.12}$$

Scriviamo la generica[5] matrice densità $\omega \in End(\mathcal{H})$ relativa ad uno stato puro come in Appendice B

$$\omega = \begin{pmatrix} \alpha & \gamma \\ \gamma^* & 1-\alpha \end{pmatrix} \tag{3.13}$$

con $\alpha \in [0,1] \subset \mathbb{R}$ e $\gamma \in \mathbb{C}$, $|\gamma|^2 = \alpha(1-\alpha)$. Utilizzando le (3.12) possiamo scrivere:

$$R(T(\omega^{\otimes N})) = \Gamma^{00}\Sigma_{00}(\omega) + \Gamma^{11}\Sigma_{11}(\omega) + \Gamma^{22}\Sigma_{22}(\omega) +$$

[5]Osserviamo che $\omega$ in equazione (3.13) è la più generica matrice 2x2 che soddifa le proprietà:

- $Tr(\omega) = 1$
- $\langle\psi|\omega|\phi\rangle = \langle\phi|\omega|\psi\rangle^* \quad \forall|\phi\rangle, |\psi\rangle \in \mathcal{H}$
- $\langle\psi|\omega|\psi\rangle \geq 0 \quad \forall|\psi\rangle \in \mathcal{H}$
- $\omega^2 = \omega$

$$+\Gamma^{23}\Sigma_{23}(\omega) + \Gamma^{32}\Sigma_{32}(\omega) + \Gamma^{33}\Sigma_{33}(\omega) =$$

$$= \begin{pmatrix} \Gamma^{00}(1-\alpha) + \Gamma^{22}\alpha & \Gamma^{23}\gamma \\ \Gamma^{32}\gamma^* & \Gamma^{11}\alpha + \Gamma^{33}(1-\alpha) \end{pmatrix} \tag{3.14}$$

Ricordiamo che $\Gamma^{23} = (\Gamma^{32})^*$; notiamo inoltre che $\Gamma^{\alpha\alpha} = \sum_k |c_k^\alpha|^2 \geq 0$

- Completa positività (II). Per avere condizioni sui coefficienti $\Gamma^{\alpha\beta}$ che non sono presenti in (3.12) utilizziamo la condizione (3.4) che deriva dalla completa positività. Riscriviamo tale condizione per comodità

$$\sum_k A_k^\dagger A_k = \hat{I}$$

Inserendo $A_k = \sum_{\alpha=0}^3 c_k^\alpha \sigma_\alpha$ otteniamo:

$$\begin{aligned} \sum_k A_k^\dagger A_k &= \sum_k \sum_{\alpha,\beta=0}^3 c_k^{*\alpha} c_k^\beta \sigma_\alpha^\dagger \sigma_\beta = \\ &= \sum_k \sum_{\alpha,\beta=0}^3 \gamma_k^{\beta\alpha} \sigma_\alpha^\dagger \sigma_\beta = \\ &= \sum_{\alpha,\beta=0}^3 \Gamma^{\beta\alpha} \sigma_\alpha^\dagger \sigma_\beta = \hat{I} \end{aligned} \tag{3.15}$$

Tenendo conto della (3.12) possiamo riscrivere la (3.15) nel modo seguente:

$$\begin{aligned} &\Gamma^{00}\sigma_0^\dagger\sigma_0 + \Gamma^{11}\sigma_1^\dagger\sigma_1 + \Gamma^{22}\sigma_2^\dagger\sigma_2 + \\ &\Gamma^{23}\sigma_3^\dagger\sigma_2 + \Gamma^{32}\sigma_2^\dagger\sigma_3 + \Gamma^{33}\sigma_3^\dagger\sigma_3 = \hat{I} \end{aligned}$$

ovvero

$$\begin{aligned} &\Gamma^{00}\sigma_1\sigma_0 + \Gamma^{11}\sigma_0\sigma_1 + \Gamma^{22}\sigma_2\sigma_2 + \\ &\Gamma^{23}\sigma_3\sigma_2 + \Gamma^{32}\sigma_2\sigma_3 + \Gamma^{33}\sigma_3\sigma_3 = \hat{I} \end{aligned} \tag{3.16}$$

Calcoliamoci i prodotti di matrici seguenti:

$$\sigma_0\sigma_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \sigma_2$$

$$\sigma_1\sigma_0 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \sigma_3$$
$$\sigma_2\sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \sigma_2$$
$$\sigma_2\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\sigma_3\sigma_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\sigma_3\sigma_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \sigma_3$$

e utilizziamoli per esplicitare la (3.16), che diventa

$$\begin{pmatrix} \Gamma^{11} + \Gamma^{22} & 0 \\ 0 & \Gamma^{00} + \Gamma^{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{3.17}$$

La (3.17) dà le seguenti condizioni sui coefficienti $\Gamma^{\alpha\beta}$:

$$\Gamma^{11} + \Gamma^{22} = \Gamma^{00} + \Gamma^{33} = 1 \tag{3.18}$$

ovvero

$$\Gamma^{11} = 1 - \Gamma^{22}, \qquad \Gamma^{00} = 1 - \Gamma^{33} \tag{3.19}$$

Utilizzando queste condizioni sui coefficienti possiamo riscrivere la (3.14) come segue

$$R(T(\omega^{\otimes N})) = \begin{pmatrix} (1-\Gamma^{33})(1-\alpha) + \Gamma^{22}\alpha & \Gamma^{23}\gamma \\ \Gamma^{32}\gamma^* & (1-\Gamma^{22})\alpha + \Gamma^{33}(1-\alpha) \end{pmatrix} \tag{3.20}$$

Per finire notiamo che, siccome $\Gamma^{\alpha\alpha} \geq 0 \; \forall\, \alpha$, dalle (3.19) segue

$$0 \leq \Gamma^{22} \leq 1, \qquad 0 \leq \Gamma^{33} \leq 1 \tag{3.21}$$

da cui anche:

$$0 \leq \Gamma^{00} \leq 1 \qquad 0 \leq \Gamma^{11} \leq 1 \tag{3.22}$$

Utilizziamo le disuguaglianze (3.21) e (3.22) per ricavare la seguente maggiorazione per $|\Gamma^{32}|^2$

$$\begin{aligned} |\Gamma^{32}|^2 &= |\sum_k c_k^2 c_k^{*3}|^2 \leq \sum_k |c_k^2 c_k^{*3}|^2 = \sum_k |c_k^2|^2 |c_k^3|^2 = \\ &\leq \sum_k |c_k^2|^2 \sum_k |c_k^3|^2 \leq 1 \end{aligned} \tag{3.23}$$

Indichiamo $|\Gamma^{32}|$ con $\eta\prime$, $(0 \leq \eta\prime \leq 1)$[6] e riscriviamo la (3.20)

$$R(T(\omega^{\otimes N})) = \begin{pmatrix} (1-\Gamma^{33})(1-\alpha)+\Gamma^{22}\alpha & \gamma\eta\prime\, e^{\,i\varphi} \\ \gamma^*\eta\prime\, e^{-i\varphi} & (1-\Gamma^{22})\alpha+\Gamma^{33}(1-\alpha) \end{pmatrix} \tag{3.24}$$

con $\varphi = arg(\Gamma^{32})$.

- Conservazione della traccia. Imponiamo la condizione

$$Tr[R(T(\omega^{\otimes N}))] = 1$$

Utilizzando per $R(T(\omega^{\otimes N}))$ la forma data nell'equazione (3.24), otteniamo l'identità:

$$\begin{aligned} Tr[R(T(\omega^{\otimes N}))] &= (1-\Gamma^{33})(1-\alpha)+\Gamma^{22}\alpha+(1-\Gamma^{22})\alpha+ \\ &\quad +\Gamma^{33}(1-\alpha) = 1 \quad \forall\alpha \end{aligned}$$

che non fornisce ulteriori condizioni per i coefficienti $\Gamma^{\alpha\beta}$

### 3.2.3 La classe $\mathcal{C}_\phi$ di qubits equatoriali

La (3.24) è la forma per $R(T(\omega^{\otimes N}))$ che cercavamo. Nel §2.4 abbiamo visto che il generico cloner universale $N \longrightarrow M$ è individuato dal fattore di contrazione $\eta(N,M)$ e ciò è equivalente a richiedere che l'effetto sul vettore di Bloch in ingresso sia quello di contrarlo del fattore $\eta(N,M)$. Calcoliamo il vettore di Bloch $\mathbf{S}^{in}$ relativo a ciascuno degli N qubits in ingresso, nel generico stato $\omega$. Poiché

$$\mathbf{S}^{in} = Tr[\omega\,\boldsymbol{\sigma}]$$

abbiamo

$$\begin{aligned} S_x^{in} &= Tr[\omega\,\sigma_x] = \\ &= Tr[\begin{pmatrix} \alpha & \gamma \\ \gamma^* & 1-\alpha \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \\ &= \gamma+\gamma^* = 2|\gamma|\cos\varphi \end{aligned}$$

$$\begin{aligned} S_y^{in} &= Tr[\begin{pmatrix} \alpha & \gamma \\ \gamma^* & 1-\alpha \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}] = \\ &= i(\gamma-\gamma^*) = -2|\gamma|\sin\varphi \end{aligned}$$

[6] Si noti che $\eta\prime = \eta\prime(T) = \eta\prime(N,M)$. La dipendenza da T e quindi da (N,M) è data attraverso i coefficienti $c_k^\alpha$ di $\Gamma^{32}$.

$$\begin{aligned} S_z^{in} &= Tr[\begin{pmatrix} \alpha & \gamma \\ \gamma^* & 1-\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}] = \\ &= 2\alpha - 1 \end{aligned}$$

da cui

$$\mathbf{S}^{in} = (2|\gamma|\cos\phi, -2|\gamma|\sin\phi, 2\alpha - 1) \tag{3.25}$$

dove $\phi = arg(\gamma)$.

Calcoliamoci ora $\mathbf{S}^{out}$, ovvero il vettore di Bloch relativo a ciascuno degli M qubits in uscita, ciascuno dei quali si trova nello stato $R(T(\omega^{\otimes N}))$. Poiché

$$\mathbf{S}^{out} = Tr[R(T(\omega^{\otimes N}))\,\boldsymbol{\sigma}]$$

abbiamo

$$\begin{aligned} S_x^{out} &= Tr[\begin{pmatrix} (1-\Gamma^{33})(1-\alpha)+\Gamma^{22}\alpha & \eta\prime\, e^{i\varphi}\gamma \\ \eta\prime\, e^{-i\varphi}\gamma^* & (1-\Gamma^{22})\alpha+\Gamma^{33}(1-\alpha) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}] = \\ &= 2\eta\prime|\gamma|\cos(\phi+\varphi) \end{aligned}$$

$$\begin{aligned} S_y^{out} &= Tr[\begin{pmatrix} (1-\Gamma^{33})(1-\alpha)+\Gamma^{22}\alpha & \eta\prime\, e^{i\varphi}\gamma \\ \eta\prime\, e^{-i\varphi}\gamma^* & (1-\Gamma^{22})\alpha+\Gamma^{33}(1-\alpha) \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}] = \\ &= -2\eta\prime|\gamma|\sin(\phi+\varphi) \end{aligned}$$

$$\begin{aligned} S_z^{out} &= Tr[\begin{pmatrix} (1-\Gamma^{33})(1-\alpha)+\Gamma^{22}\alpha & \eta\prime\, e^{i\varphi}\gamma \\ \eta\prime\, e^{-i\varphi}\gamma^* & (1-\Gamma^{22})\alpha+\Gamma^{33}(1-\alpha) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}] = \\ &= (1-\Gamma^{33})(1-\alpha)+\Gamma^{22}\alpha-(1-\Gamma^{22})\alpha-\Gamma^{33}(1-\alpha) = \\ &= (2\alpha-1)(\Gamma^{33}+\Gamma^{22}-1)+(\Gamma^{22}-\Gamma^{33}) = \\ &= S_z^{in}(\Gamma^{33}+\Gamma^{22}-1)+(\Gamma^{22}-\Gamma^{33}) \end{aligned}$$

da cui

$$\mathbf{S}^{out} = (2\eta\prime|\gamma|\cos(\phi+\varphi), -2\eta\prime|\gamma|\sin(\phi+\varphi), S_z^{in}(\Gamma^{33}+\Gamma^{22}-1)+(\Gamma^{22}-\Gamma^{33})) \tag{3.26}$$

Confrontando le espressioni di $\mathbf{S}^{in}$ e $\mathbf{S}^{out}$ notiamo che la mappa T (per $\varphi = 0$) è individuata dai fattori $\eta\prime(N, M)$ e $(\Gamma^{33}+\Gamma^{22}-1)$, che danno rispettivamente la contrazione di $\mathbf{S}^{in}$ nel piano XY e lungo l'asse Z. Inoltre il fattore $(\Gamma^{22}-\Gamma^{33})$ sposta $S_z^{in}$ di una quantità fissa. Vedremo ora che scegliendo una classe di stati in ingresso al cloner T con $S_z = 0$, avremo realizzato il nostro obiettivo di avere un cloner individuabile tramite un parametro di contrazione.

Consideriamo N qubits equatoriali non interagenti, ciascuno nello stato $|\psi_\phi\rangle$ di equazione (1.37) di §1.6, descritto dalla matrice densità $\omega_\phi$[7]

$$\omega_\phi = \frac{1}{2}\begin{pmatrix} 1 & e^{-i\phi} \\ e^{i\phi} & 1 \end{pmatrix}$$

a cui è associato il vettore di Bloch $\mathbf{S}_\phi$ che determiniamo immediatamente inserendo $\gamma = \frac{1}{2}e^{-i\phi}$ e $\alpha = \frac{1}{2}$ nella (3.25):

$$\mathbf{S}_\phi = (\cos\phi, \sin\phi, 0) \tag{3.27}$$

Al variare di $\phi$ in $[0, 2\pi]$, $\omega_\phi$ descrive una classe di stati puri ($|\mathbf{S}_\phi|^2 = 1 \; \forall\, \phi$) caratterizzati da un vettore di Bloch giacente nel piano equatoriale XY della sfera di Bloch (qubits equatoriali), che forma l'angolo $\phi$ con l'asse X. Sempre ponendo $\gamma = \frac{1}{2}e^{-i\phi}$ e $\alpha = \frac{1}{2}$, questa volta nella (3.24), otteniamo:

$$R(T(\omega_\phi^{\otimes N})) = \begin{pmatrix} \frac{1}{2}(1-\Gamma^{33}) + \frac{1}{2}\Gamma^{22} & \frac{1}{2}\eta\prime e^{-i(\phi-\varphi)} \\ \frac{1}{2}\eta\prime e^{\,i(\phi-\varphi)} & \frac{1}{2}(1-\Gamma^{22}) + \frac{1}{2}\Gamma^{33} \end{pmatrix} \tag{3.28}$$

che per $\Gamma^{22} = \Gamma^{33}$ diventa

$$R(T(\omega_\phi^{\otimes N})) = \frac{1}{2}\begin{pmatrix} 1 & \eta\prime(N,M)e^{-i(\phi-\varphi)} \\ \eta\prime(N,M)e^{\,i(\phi-\varphi)} & 1 \end{pmatrix} \tag{3.29}$$

che si può scrivere:

$$R(T(\omega_\phi^{\otimes N})) = \eta\prime(N,M)\omega_{(\phi-\varphi)} + \frac{1}{2}[1-\eta\prime(N,M)]\hat{I} \tag{3.30}$$

La (3.30) ci dice che per

$$\varphi = 0, \qquad \Gamma^{22} = \Gamma^{33} \tag{3.31}$$

l'azione del cloner T sui qbits equatoriali della classe $\mathcal{C}_\phi$

$$\mathcal{C}_\phi = \{|\psi_\phi\rangle, \phi \in [0, 2\pi]\}$$

è completamente determinata dal fattore di contrazione $\eta\prime(N,M)$. Analizziamo le condizioni (3.31):

[7]Possiamo pensare che $\omega_\phi$ desciva lo stato di spin di una particella di spin $\frac{1}{2}$, il cui momento angolare di spin giace nel piano XY. L'angolo $\phi$ esprime in questo caso l'angolo tra tale vettore e l'asse X.

- $\varphi = 0$. Se $\varphi$ fosse diverso da zero il cloner T agirebbe sulle componenti XY di $\mathbf{S}^{in}$ oltre che con una contrazione, anche con una rotazione di un angolo $\varphi$ attorno all'asse Z. Scegliamo di esprimere la bontà del cloning $N \longrightarrow M$ effettuato da T sugli stati di $\mathcal{C}_\phi$ secondo il metodo OPT. Introduciamo quindi la Fidelity:

$$\begin{aligned} F(N,M) &= |\langle\psi_\phi|R(T(\omega_\phi^{\otimes N}))|\psi_\phi\rangle|^2 = \\ &= Tr\left[\omega_\phi \begin{pmatrix} \frac{1}{2}(1-\Gamma^{33}) + \frac{1}{2}\Gamma^{22} & \eta\prime e^{-i(\phi-\varphi)} \\ \eta\prime e^{\,i(\phi-\varphi)} & \frac{1}{2}(1-\Gamma^{22}) + \frac{1}{2}\Gamma^{33} \end{pmatrix}\right] = \\ &= \frac{1}{2}(1+\eta\prime(N,M)cos\varphi) \end{aligned} \tag{3.32}$$

  Il cloner ottimo $\hat{T}$ è quello che massimizza F(N,M)[8]. Dalla (3.32) vediamo che massimizzare F(N,M) è equivalente a porre $\varphi = 0$ e trovare il più basso limite superiore per $\eta\prime(N,M)$. Il problema della massimizzazione di $\eta\prime(N,M)$ sarà analizzato nel prossimo sottoparagrafo.

- $\Gamma^{22} = \Gamma^{33}$. Supponiamo di aver trovato un cloner ottimo $\hat{T}$ caratterizzato da $\eta\prime_{opt}(N,M)$ e da $\Gamma^{22} \neq \Gamma^{33}$. Se cambiamo nome ai vettori della base (i.e. scambiamo $|0\rangle$ con $|1\rangle$), poiché

$$\sigma_2 = \frac{1}{2}(1+\sigma_z), \qquad \sigma_3 = \frac{1}{2}(1-\sigma_z)$$

  questa operazione è equivalente allo scambio di 2 con 3, lasciando fissi $|0\rangle$ e $|1\rangle$. Lo scambio $2 \leftrightarrow 3$ lascia invariato il fattore di contrazione $\eta\prime(N,M)$, che è definito come

$$\eta\prime(N,M) = |\Gamma^{32}| = |\Gamma^{23}|$$

  mentre provoca lo scambio di $\Gamma^{22}$ con $\Gamma^{33}$. Il cloner $\hat{T}^*$ ottenuto rinominando la base, applicato a stati della classe $\mathcal{C}_\phi$, darà in uscita

$$\mathbf{S}^{out} = (\eta\prime_{opt}\cos\phi, \eta\prime_{opt}\sin\phi, S_z^{in}(\Gamma^{33}+\Gamma^{22}-1) + (\Gamma^{33}-\Gamma^{22}))$$

  Se $\hat{T}$ è ottimo, anche $\hat{T}^*$ deve esserlo: infatti l'ottimalità del cloner $\hat{T}$ non può dipendere da come abbiamo chiamato la base, inoltre la Fidelity di equazione (3.32) (che è il criterio con cui stabiliamo l'ottimalità) non

[8] Ricordiamo che dalla definizione di F segue immediatamente che $0 < F(N,M) < 1$ e che F(N,M)=1 per un cloner ideale.

cambia per lo scambio $2 \leftrightarrow 3$. Supponiamo ora di realizzare il cloner T, definito tramite la seguente combinazione lineare convessa di $\hat{T}$ e $\hat{T}^*$:

$$T \equiv \frac{1}{2}\left(\hat{T} + \hat{T}^*\right)$$

Per definizione abbiamo:

$$T(\varrho_N) = \frac{1}{2}\hat{T}(\varrho_N) + \frac{1}{2}\hat{T}^*(\varrho_N)$$

con $\varrho_N$ generica matrice densità su $\mathcal{H}_+^{\otimes \mathrm{N}}$. Se applichiamo T a stati di $\mathcal{C}_\phi$, $R(T(\omega_\phi^{\otimes N}))$ risulta:

$$\begin{aligned} R(T(\omega_\phi^{\otimes N})) &= \frac{1}{2}R(\hat{T}(\omega_\phi^{\otimes N})) + \frac{1}{2}R(\hat{T}^*(\omega_\phi^{\otimes N})) = \\ &= \frac{1}{2}\left[\frac{1}{2}\begin{pmatrix} \frac{1}{2}(1-\Gamma^{33}) + \frac{1}{2}\Gamma^{22} & \frac{1}{2}\eta\prime_{opt}e^{-i\phi} \\ \frac{1}{2}\eta\prime_{opt}e^{i\phi} & \frac{1}{2}(1-\Gamma^{22}) + \frac{1}{2}\Gamma^{33} \end{pmatrix} + \right. \\ &\qquad \left. + \frac{1}{2}\begin{pmatrix} \frac{1}{2}(1-\Gamma^{22}) + \frac{1}{2}\Gamma^{33} & \frac{1}{2}\eta\prime_{opt}e^{-i\phi} \\ \frac{1}{2}\eta\prime_{opt}e^{i\phi} & \frac{1}{2}(1-\Gamma^{33}) + \frac{1}{2}\Gamma^{22} \end{pmatrix}\right] = \\ &= \frac{1}{2}\begin{pmatrix} 1 & \eta\prime_{opt}(N,M)e^{-i\phi} \\ \eta\prime_{opt}(N,M)e^{i\phi} & 1 \end{pmatrix} \end{aligned} \tag{3.33}$$

che è della forma (3.29). Questo ci dice che se cerchiamo il cloner ottimo $\hat{T}$ per qubits equatoriali nella classe di cloners covarianti in fase caratterizzati da $\Gamma^{22} = \Gamma^{33}$, non può esistere un cloner $\tilde{T}$ con $\Gamma^{22} \neq \Gamma^{33}$ che realizzi il cloning meglio di $\hat{T}$. Infatti, se tale cloner esistesse e fosse caratterizzato da un fattore di contrazione $\tilde{\eta}$ nel piano XY tale che

$$\tilde{\eta} \geq \eta\prime_{opt} \tag{3.34}$$

potremmo realizzare un cloner caratterizzato da $\Gamma^{22} = \Gamma^{33}$ e $\eta\prime = \tilde{\eta}$ nel modo precedentemente descritto, in contrasto con l'ipotesi di ottimalità di $\hat{T}$.

### 3.2.4 Cloning ottimale covariante in fase per la classe di qubits equatoriali $\mathcal{C}_\phi$

Consideriamo un generico cloner T covariante in fase e caratterizzato da $\varphi = 0$ e $\Gamma \equiv \Gamma^{22} = \Gamma^{33}$. Abbiamo visto che per

$$\omega = \begin{pmatrix} \alpha & \gamma \\ \gamma^* & 1-\alpha \end{pmatrix}$$

si ha

$$R(T(\omega^{\otimes N})) = \begin{pmatrix} (1-\Gamma)(1-\alpha)+\Gamma\alpha & \gamma\eta\prime e^{i\,\varphi} \\ \gamma^{*}\eta\prime e^{-i\varphi} & (1-\Gamma)\alpha+\Gamma(1-\alpha) \end{pmatrix} \tag{3.35}$$

mentre se $\omega = \omega_\phi$

$$R(T(\omega_\phi^{\otimes N})) = \frac{1}{2}\begin{pmatrix} 1 & \eta\prime(N,M)e^{i\,\varphi} \\ \eta\prime(N,M)e^{-i\varphi} & 1 \end{pmatrix} \tag{3.36}$$

Affrontiamo qui il problema dell'ottimizzazione di $\eta\prime(N,M)$, seguendo la linea tracciata nel §2.4.
Dimostreremo nel seguito che:

- **I.**Se si realizza un cloner $T_{MN}$ covariante in fase (con N qubits in ingresso appartenenti alla classe $\mathcal{C}_\phi$) tramite la concatenazione di due opportuni cloners covarianti in fase ($T_{LN}$ e $T_{\infty L}$)

$$\begin{array}{l} N \xrightarrow{T_{LN}} L \xrightarrow{T_{ML}} M \\ \omega_\phi^{\otimes N} \longmapsto \varrho_L \equiv T_{LN}(\omega_\phi^{\otimes N}) \longmapsto T_{ML}\circ T_{LN}(\omega^{\otimes N}) \\ N \xrightarrow{T_{MN}} M \\ \omega^{\otimes N} \longmapsto T_{MN}(\omega^{\otimes N}) \end{array}$$

  si ha:

$$\eta\prime(N,M) = \eta\prime(N,L)\eta\prime(L,\infty) \tag{3.37}$$

  ovvero il fattore di contrazione $\eta\prime(N,M)$ è il prodotto dei fattori di contrazione nel piano XY dei due cloners concatenati ($T_{LN}$ e $T_{\infty L}$)

- **II.**Vale l'uguaglianza

$$\eta\prime_{opt}(N,\infty) = \overline{\eta}_{opt}^{mis}(N) \tag{3.38}$$

  dove $\eta\prime_{opt}(N,\infty)$ è il fattore di contrazione relativo al cloner $N \longrightarrow \infty$ ottimo, mentre $\overline{\eta}_{opt}^{mis}(N) = (2\overline{F}_{mis}^{opt} - 1)$ e $\overline{F}_{mis}^{opt}$ è la Fidelity relativa alla stima dello stato $|\Psi_\phi\rangle$ di N qubits data in (1.53) e calcolata utilizzando i risultati di diverse misurazioni. Riportiamo questa quantità per comodità:

$$\overline{F}_{mis}^{opt}(N) = \frac{1}{2} + \frac{1}{2^{N+1}}\sum_{l=0}^{N-1}\sqrt{\binom{N}{l}\binom{N}{l+1}} \tag{3.39}$$

Il cloner $N \longrightarrow \infty$ covariante in fase ottenuto concatenando due opportuni cloners covarianti in fase ($N \longrightarrow L$ e $L \longrightarrow \infty$) non può dare un risultato migliore del cloner $N \longrightarrow \infty$ covariante in fase ottimo. Perciò, utilizzando la proprietà di concatenazione, possiamo scrivere:

$$\eta\prime(N, L)\eta\prime(L, \infty) \leq \eta\prime^{opt}(N, \infty) \tag{3.40}$$

Da questa disuguaglianza ricaviamo immediatamente il più basso limite superiore per $\eta\prime^{opt}$:

$$\eta\prime^{opt} \leq \frac{\eta\prime^{opt}(N, \infty)}{\eta\prime^{opt}(M, \infty)} \tag{3.41}$$

Utilizzando l'uguaglianza di (**II**) la (3.41) diventa:

$$\begin{aligned} \eta\prime^{opt} &\leq \tilde{\eta}\prime = \frac{\overline{\eta}^{opt}_{mis}(N)}{\overline{\eta}^{opt}_{mis}(M)} \\ &= 2^{(M-N)} \frac{\sum_{l=0}^{N-1} \sqrt{\binom{N}{l}\binom{N}{l+1}}}{\sum_{j=0}^{M-1} \sqrt{\binom{M}{j}\binom{M}{j+1}}} \end{aligned} \tag{3.42}$$

Poiché non è nota esplicitamente nessuna mappa di cloning che realizzi il limite superiore $\tilde{\eta}\prime$ per $\eta\prime(N, M)$ dato in (3.42), non possiamo dire se tale limite venga raggiunto o meno. In figura 3.1 presentiamo il grafico di di $\tilde{\eta}\prime(N, M)$, da cui si vede che $\lim_{N\to\infty} \tilde{\eta}\prime(N, M) = 1$ ($M > N$), come atteso.
Nelle figure C.1, C.2, C.3, C.4 di Appendice C, invece, confrontiamo i grafici di $\tilde{\eta}\prime$ e $\eta$ con N=1,2,3,4 fissato e $M > N$ variabile. Si vede che per tutte le coppie $(N, M)$ prese in considerazione vale la disuguaglianza

$$\tilde{\eta}\prime(N, M) > \eta(N, M) \tag{3.43}$$

Nel paragrafo seguente troveremo la forma esplicita della cloning map che raggiunge tale limite nel caso N=1, M=2. Prima però dimostriamo le affermazioni **I** e **II**.

- Dimostrazione di **I.** Poiché $T_{MN}$ è covariante in fase, utilizzando la (3.30) con $\varphi = 0$, abbiamo

$$R(T_{MN}(\omega_\phi^{\otimes N})) = \eta\prime_{MN}\omega_\phi + \frac{1}{2}[1 - \eta\prime_{MN}]\hat{I} \tag{3.44}$$

ma

$$\begin{aligned} T_{MN}(\omega_\phi^{\otimes N}) &= T_{ML} \circ T_{LN}(\omega_\phi^{\otimes N}) = \\ &= T_{ML}(\varrho_L) \end{aligned} \tag{3.45}$$

Scriviamo

$$\varrho_L = \sum_i \beta_i \left[|\psi_i\rangle\langle\psi_i|\right]^{\otimes L}$$

e calcoliamo

$$\begin{aligned} R(T_{MN}(\omega_\phi^{\otimes N})) &= R(T_{ML}(\sum_i \beta_i \left[|\psi_i\rangle\langle\psi_i|\right]^{\otimes L}) = \\ &= \sum_i \beta_i R(T_{ML}(|\psi_i\rangle\langle\psi_i|^{\otimes L})) \end{aligned} \tag{3.46}$$

La quantità $\omega_i \equiv |\psi_i\rangle\langle\psi_i|$ è una generica matrice densità 2x2[9], che perciò scriviamo

$$\omega_i = \begin{pmatrix} \alpha_i & \gamma_i \\ \gamma_i^* & 1-\alpha_i \end{pmatrix}$$

con $0 \leq \alpha_i \leq 1$ e $\gamma_i \in C$, $|\gamma_i|^2 = \alpha_i(1-\alpha_i)$. Inserendo questa espressione in (3.46) e tenendo conto del fatto che la mappa $T_{ML}$ è covariante in fase, abbiamo:

$$R(T_{MN}(\omega_\phi^{\otimes N})) = \sum_i \beta_i \begin{pmatrix} (1-\Gamma)(1-\alpha_i) + \Gamma\alpha_i & \eta\prime_{ML}\gamma_i \\ \eta\prime_{ML}\gamma_i^* & (1-\Gamma)\alpha_i + \Gamma(1-\alpha_i) \end{pmatrix} \tag{3.47}$$

Le uguaglianze

$$\begin{aligned} R[\varrho_L] &= Tr_{L-1}[\varrho_L] = \\ &= \frac{1}{2}\begin{pmatrix} 1 & \eta\prime_{LN}e^{-i\phi} \\ \eta\prime_{LN}e^{i\phi} & 1 \end{pmatrix} = \\ &= \beta_i|\psi_i\rangle\langle\psi_i| = \\ &= \sum_i \beta_i \begin{pmatrix} \alpha_i & \gamma_i \\ \gamma_i^* & 1-\alpha_i \end{pmatrix} \end{aligned}$$

ci danno le seguenti condizioni si coefficienti $\alpha_i$ e $\gamma_i$:

$$\sum_i \alpha_i\beta_i = \frac{1}{2}$$

[9]Relativa ad uno stato puro.

$$\sum_i \beta_i \gamma_i = \frac{1}{2} \eta\prime_{LN} e^{-i\phi}$$
$$\sum_i \beta_i \gamma_i^* = \frac{1}{2} \eta\prime_{LN} e^{i\phi} \tag{3.48}$$

Inserendo le (3.48) in (3.47) otteniamo:

$$R(T_{MN}(\omega_\phi^{\otimes N})) = \frac{1}{2} \begin{pmatrix} 1 & \eta\prime_{ML}\eta\prime_{LN} e^{-i\phi} \\ \eta\prime_{ML}\eta\prime_{LN} e^{i\phi} & 1 \end{pmatrix} \tag{3.49}$$

che confrontata con la (3.44) ci dà

$$\eta\prime_{MN} = \eta\prime_{ML}\eta\prime_{LN} \tag{3.50}$$

La (3.50) è la proprietà di concatenazione che cercavamo.

- Dimostrazione di **II.** Nel §1.6 abbiamo visto che dati N qubits ciascuno nello stato ignoto $\omega_\phi = |\psi_\phi\rangle\langle\psi_\phi|$ con $|\psi_\phi\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + e^{i\phi}|1\rangle\right]$ esiste una POVM $d\mu(\phi)$ covariante in fase che dà la stima migliore di $|\psi_\phi\rangle$ con Fidelity:

$$\overline{F}^{opt}(N) = \frac{1}{2} + \frac{1}{2^{N+1}} \sum_{l=0}^{N-1} \sqrt{\binom{N}{l}\binom{N}{l+1}} \tag{3.51}$$

Il risultato di ogni misura dà con probabilità $p(\phi|\phi_*)$ il candidato $|\psi_{\phi_*}\rangle$ per $|\psi_\phi\rangle$, con

$$p(\phi|\phi_*)d\phi_* = Tr\left[d\mu(\phi_*)|\psi_\phi\rangle\langle\psi_\phi|^{\otimes N}\right]$$

La Fidelity $\overline{F}^{opt}(N)$ si può calcolare dai risultati delle misure come:

$$\begin{aligned} \overline{F}^{opt}_{mis}(N) &= \int \frac{d\phi_*}{2\pi} p(\phi|\phi_*)|\langle\psi_\phi|\psi_{\phi_*}\rangle|^2 = \\ &= \langle\psi_\phi|\overline{\varrho}_\phi|\psi_\phi\rangle \end{aligned} \tag{3.52}$$

con

$$\overline{\varrho}_\phi = \int \frac{d\phi_*}{2\pi} p(\phi|\phi_*)|\psi_{\phi_*}\rangle\langle\psi_{\phi_*}|$$

Siccome la (3.52) non deve dipendere da $|\psi_\phi\rangle$, possiamo riscrivere $\overline{\varrho}_\phi$ come segue:

$$\overline{\varrho}_\phi = \overline{\eta}^{opt}_{mis}(N)|\psi_\phi\rangle\langle\psi_\phi| + \frac{1}{2}\left[1 - \overline{\eta}^{opt}_{mis}(N)\right]\hat{I} \tag{3.53}$$

Anche in questo caso possiamo quindi pensare alla procedura di stima ottima descritta, come ad un cloning $N \longrightarrow \infty$. Inoltre sarà sufficiente richiedere che la mappa S

$$\begin{aligned} S: \quad & End(\mathcal{H}_+^{\otimes \mathrm{N}}) \longrightarrow End(\mathcal{H}_+^{\otimes \infty}) \\ & \varrho_N \longmapsto S(\varrho_N) \end{aligned}$$

(lineare,completamente positiva e che conservi la traccia) sia covariante in fase. Avremo così che $R(S(\omega_\phi^{\otimes N})) = \overline{\varrho}_\phi$. Dobbiamo ora dimostrare che S è la cloning map covariante in fase che realizza il cloning (con stati in ingresso nella classe $\mathcal{C}_\phi$) in maniera ottimale. La disuguaglianza

$$\overline{\eta}_{mis}^{opt}(N) \leq \eta\prime^{opt}(N, L) \quad \forall\, L \geq N \tag{3.54}$$

segue immediatamente, poiché la procedura appena descritta non può lavorare meglio del cloner $N \longrightarrow L$ ottimo. Infatti, se producessi infinite copie migliori delle L prodotte dal cloner ottimo, ne avrei anche L migliori, in contrasto con l'ipotesi di ottimalità.

Per dimostrare che la (3.54) è un'uguaglianza per $L \longrightarrow \infty$, concateniamo un cloner $T_{LN}$ covariante in fase con una successiva misura di stato ottima. L'input per il cloner è $\omega_\phi^{\otimes N}$ e l'output è descritto dalla matrice densità $\varrho_L \in End(\mathcal{H}_+^{\otimes L})$, la cui ridotta $\varrho$ è:

$$\begin{aligned} \varrho &= Tr_{L-1}\left[\varrho_L\right] = \\ &= \eta\prime(N, L)|\psi_\phi\rangle\langle\psi_\phi| + \frac{1}{2}\left[1 - \eta\prime(N, L)\right]\hat{I} \end{aligned}$$

Possiamo vedere l'intera procedura (cloning e successiva stima dello stato $\varrho_L$) come una stima dello stato $\omega_\phi$. Scriviamo la Fidelity relativa a tale stima di stato come

$$\overline{F}_{mis}(N) = \langle\psi_\phi| \sum_\mu Tr\left[P_\mu \varrho_L\right] |\psi_\mu\rangle\langle\psi_\mu|\psi_\phi\rangle$$

dove $P_\mu$ è la POVM per la stima ottima dello stato di ciascuno degli L qubits in uscita dal cloner $T_{LN}$. Scrivendo

$$\varrho_L = \sum_i \beta_i \omega_i^{\otimes L}$$

con $\omega_i = |\psi_i\rangle\langle\psi_i|$, abbiamo:

$$\begin{aligned}\overline{F}_{mis}(N) &= \sum_{\mu,i}\langle\psi_\phi|\beta_i Tr\left[P_\mu \varrho_i^{\otimes L}\right]|\psi_\mu\rangle\langle\psi_\mu|\psi_\phi\rangle = \\ &= \sum_i \langle\psi_\phi|\beta_i\left[\overline{\eta}^{opt}_{g-mis}(L)|\psi_i\rangle\langle\psi_i| + \frac{1}{2}\left(1-\overline{\eta}^{opt}_{g-mis}(L)\right)\hat{I}\right]|\psi_\phi\rangle\end{aligned} \tag{3.55}$$

Poiché

$$\overline{\eta}^{opt}_{g-mis}(L) = \tfrac{L+1}{L+2} \xrightarrow{L\to\infty} 1$$

abbiamo

$$\overline{F}_{mis}(N) \xrightarrow{L\to\infty} \textstyle\sum_i \langle\psi_\phi|\beta_i|\psi_i\rangle\langle\psi_i|\psi_\phi\rangle$$

ma

$$\begin{aligned}\sum_i\langle\psi_\phi|\beta_i|\psi_i\rangle\langle\psi_i|\psi_\phi\rangle &= \langle\psi_\phi|\sum_i\beta_i|\psi_i\rangle\langle\psi_i|\psi_\phi\rangle = \\ &= \langle\psi_\phi|\left[\eta\prime(N,\infty)|\psi_\phi\rangle\langle\psi_\phi| + \right. \\ &\quad \left. + \frac{1}{2}\left(1-\eta\prime(N,\infty)\right)\hat{I}\right]|\psi_\phi\rangle = \\ &= \frac{1}{2}\left[\eta\prime(N,\infty)+1\right]\end{aligned}$$

da cui

$$\overline{F}_{mis}(N) \xrightarrow{L\to\infty} \tfrac{1}{2}\left[\eta\prime(N,\infty)+1\right]$$

La stima dello stato degli N qubits effettuata in questo modo (cioè concatenando un cloner e una successiva stima di stato) non può essere effettuata con precisione maggiore di una stima di stato ottima. Perciò:

$$\eta\prime^{opt}(N,\infty) \leq \eta^{opt}_{mis}(N) \tag{3.56}$$

Combinando le disuguaglianze (3.54) e (3.56) otteniamo

$$\eta\prime^{opt}(N,\infty) = \eta^{opt}_{mis}(N) \tag{3.57}$$

come volevamo dimostrare.

## 3.3 Forma esplicita del cloner per qubits $1 \longrightarrow 2$ ottimale e covariante in fase

Nel §3.2 abbiamo trovato il limite superiore per il fattore di contrazione $\eta\prime(N, M)$ che descrive un cloner $N \longrightarrow M$ covariante in fase, ma non sappiamo se tale limite venga effettivamente raggiunto. In questo paragrafo ci proponiamo di mostrare che questo succede nel caso particolare N=1, M=2.

### 3.3.1 Descrizione di un cloner $1 \longrightarrow 2$ per qubits tramite una evoluzione unitaria

Come sottolineato nel §2.3.1, è possibile descrivere un generico cloner $N \longrightarrow M$ universale tramite un operatore unitario. Consideriamo il caso N=1, M=2 e l'operatore unitario U

$$\begin{aligned} U: \quad & \mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}_P \longrightarrow \mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}_P \\ & |\psi\rangle|0\rangle|x\rangle \longmapsto |\varphi\rangle \equiv U|\psi\rangle|0\rangle|x\rangle \end{aligned}$$

con:

- $|\psi\rangle \in \mathcal{H} = span\{|0\rangle, |1\rangle\} \simeq \mathbb{C}^2$ stato (puro e non noto) in cui si trova il qubit in ingresso.
- $|x\rangle \in \mathcal{H}_P$, stato in cui si trova il Probe (costituito da una parte opportuna del cloner e da parte dell'ambiente esterno).

Se vogliamo che il cloner descritto da U abbia le stesse proprietà di quello caratterizzato dalla mappa T lineare, completamente positiva, che conservi la traccia e covariante rispetto a SU(2)

$$T : End(\mathcal{H}) \longrightarrow End(\mathcal{H}_+^{\otimes 2})$$

dobbiamo richiedere che valgano le seguenti condizioni:

- **I.**Simmetria[10]:

$$\varrho_1 \equiv Tr_{2,P}\left[|\varphi\rangle\langle\varphi|\right] = \varrho_2 \equiv Tr_{1,P}\left[|\varphi\rangle\langle\varphi|\right]$$

[10]Utilizziamo qui e nel seguito i pedici 1 e 2 per denotare grandezze relative allo spazio di Hilbert delle particelle 1 e 2 in uscita dal cloner.

- **II.a.**Invarianza del vettore di Bloch per orientazione:

$$\mathbf{S}_1 = \eta_\psi(1,2)\mathbf{S}_\psi$$

Questa condizione ci dice che il vettore di Bloch $\mathbf{S}_\psi$ dello stato originale $|\psi\rangle$ non cambia direzione ma solo lunghezza.

- **II.b.**Isotropia:

$$F(1,2) = Tr\left[\varrho_\psi \varrho_1\right] = Tr\left[\varrho_\psi \varrho_2\right] = costante \quad (rispetto\ a\ \psi)$$

con $\varrho_\psi = |\psi\rangle\langle\psi|$. Questo significa che il cloner tratta tutti gli stati allo stesso modo. Poiché $F(1,2) = \frac{1}{2}\left[1 + \eta(1,2)\right]$ la richiesta di isotropia implica che $\eta(1,2)$ non dipende dallo stato $|\psi\rangle$.

In ref.[12] si dimostra che imporre le condizioni (**II.a**) e (**II.b**) è equivalente a richiedere che ciascuno dei due qubits di output si trovi in uno stato descritto dalla matrice densità ridotta $\varrho_{1,2}^{out}$

$$\varrho_{1,2}^{out} = \eta(1,2)|\psi\rangle\langle\psi| + \frac{1}{2}\left[1 - \eta(1,2)\right]\hat{I}$$

con $\eta(1,2)$ indipendente dallo stato $|\psi\rangle$ (universalità).

Se richiediamo che il nostro cloner lavori solo su stati $\omega_\phi$ appartenenti alla classe $\mathcal{C}_\phi$, abbiamo che

$$\varrho_{1,2}^{out} = \eta(1,2)\omega_\phi + \frac{1}{2}\left[1 - \eta(1,2)\right]\hat{I} \tag{3.58}$$

La richiesta di restrizione della classe di stati di input non è però compatibile con quella di covarianza rispetto al gruppo SU(2). Infatti preso un generico operatore $U \in SU(2)$

$$U\varrho_\phi U^* \in \mathcal{C}_\phi \quad \Leftrightarrow \quad U \in U(1)$$

e quindi per $U \notin U(1)$ il primo membro della

$$T(U\omega_\phi U^*) = U^{\otimes 2} T(\omega_\phi) U^{*\otimes 2}$$

non è definito. Questa osservazione ci permette di concludere che se ci interessa conoscere l'azione di un cloner per qubits $T : 1 \longrightarrow 2$ covariante in fase solo sugli stati della classe $\mathcal{C}_\phi$, possiamo esprimerla attraverso un operatore unitario U con le proprietà $\tilde{\mathbf{I}}$ e $\tilde{\mathbf{II}}$, che sono le **I** e **II** con $|\psi_\phi\rangle$ invece di $|\psi\rangle$.

### 3.3.2 Calcolo esplicito dell'operatore unitario relativo al cloning per qubits $1 \longrightarrow 2$ covariante in fase ottimo

Vogliamo trovare il cloner $1 \longrightarrow 2$ ottimo il cui input è costituito solo da stati puri con $S_Z = 0$[11]. Poiché la soluzione del problema non può dipendere da una particolare scelta degli assi, possiamo prendere in considerazione una qualsiasi classe di stati il cui vettore di Bloch descrive un cerchio massimo sulla sfera di Bloch. In particolare scegliamo come cerchio massimo l'equatore del piano XZ, i.e gli stati della forma

$$|\psi_{xz}\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in R, \quad \alpha^2 + \beta^2 = 1$$

il cui vettore di Bloch è:

$$\mathbf{S} = (2\alpha\beta, 0, \alpha^2 - \beta^2)$$

Per raggiungere il nostro obiettivo troveremo per prima cosa il cloner ottimale per la classe costiuita dai quattro stati seguenti

$$\begin{aligned} &|0\rangle \\ &|1\rangle \\ &|\overline{0}\rangle = \sqrt{\frac{1}{2}}\,(|0\rangle + |1\rangle) \\ &|\overline{1}\rangle = \sqrt{\frac{1}{2}}\,(|0\rangle - |1\rangle) \end{aligned} \tag{3.59}$$

che sono noti in letteratura come stati BB84[12]. Dimostreremo poi che l 'operatore unitario che descrive questa procedura di cloning dà la medesima Fidelity per ogni stato $|\psi_{xz}\rangle$ in input. A questo punto potremo concludere di aver trovato la migliore trasformazione per tutti gli stati dell'equatore XZ: infatti, se ne esistesse una migliore per tutto l'equatore, questa (per la proprietà $\tilde{\mathbf{II}}$**.b**) dovrebbe essere migliore di quella ottima per gli stati BB84, che è assurdo. Partiamo dalla seguente assunzione[13] per la forma della trasformazione

[11] In questo sottoparagrafo seguiremo Ref.[13].

[12] BB84 è il nome del più vecchio e noto schema crittografico proposto da Bennett e Brassard nel 1984 (si veda a questo proposito ref.[14]), in cui il mittente codifica ciascun bit logico, 0 o 1, nella polarizzazione lineare di un singolo fotone, lungo una delle due basi coniugate $\{|0\rangle, |1\rangle\}$, $\{|\overline{0}\rangle, |\overline{1}\rangle\}$ a sua scelta.

[13] Tale assunzione tiene conto dei calcoli già svolti in ref.[12], in cui si parte dalla forma più generale

$$U|0\rangle|0\rangle|X\rangle = a|00\rangle|A\rangle + b_1|01\rangle|B_1\rangle + b_2|10\rangle|B_2\rangle + c|11\rangle|C\rangle$$

unitaria U

$$U|0\rangle|0\rangle|X\rangle = a|00\rangle|A\rangle + b(|01\rangle + |10\rangle)|B\rangle + c|11\rangle|C\rangle$$
$$U|1\rangle|0\rangle|X\rangle = \tilde{a}|11\rangle|\tilde{A}\rangle + \tilde{b}(|10\rangle + |01\rangle)|\tilde{B}\rangle + \tilde{c}|00\rangle|\tilde{C}\rangle \qquad (3.60)$$

Per semplicità scegliamo i coefficienti a, b, c, $\tilde{a}$, $\tilde{b}$, $\tilde{c}$ reali e positivi e includiamo tutte le fasi di (3.60) negli stati del Probe. Poiché la trasformazione (3.60) non deve cambiare se si cambia nome ai vettori della base (i.e. se si scambia 0 con 1), avremo

$$a = \tilde{a}, \qquad b = \tilde{b}, \qquad c = \tilde{c} \qquad (3.61)$$

Se imponiamo che la trasformazione di cloning sia unitaria, abbiamo che i coefficienti a, b, c devono soddisfare le condizioni di normalizzazione

$$a^2 + 2b^2 + c^2 = 1 \qquad (3.62)$$

e di ortogonalità

$$ac\langle\tilde{C}|A\rangle + 2b^2\langle\tilde{B}|B\rangle + ac\langle\tilde{A}|C\rangle = 0 \qquad (3.63)$$

Ora dobbiamo determinare i parametri liberi della trasformazione (che sono i coefficienti ed i prodotti scalari tra gli stati di Probe) in modo che la Fidelity

$$F = F(1,2) = \langle\psi|\varrho_{1,2}^{out}|\psi\rangle$$

calcolata utilizzando come stati $|\psi\rangle$ i quattro stati BB84, sia costante (proprietà **$\tilde{\text{I}}\tilde{\text{I}}$.b**.) e ottima. Uguagliando le Fidelity ottenute con la matrice densità ridotta relativa ai quattro stati BB84 si ottengono le seguenti condizioni:

$$F = a^2 + b^2 \qquad (3.64)$$
$$F = \frac{1}{2}\left(1 + ab\,\Re e\left[\langle\tilde{A}|B\rangle + \langle\tilde{B}|A\rangle\right] + bc\,\Re e\left[\langle\tilde{B}|C\rangle + \langle\tilde{C}|B\rangle\right]\right) \qquad (3.65)$$
$$0 = ab\,\Re e\left[\langle\tilde{A}|\tilde{B}\rangle + \langle B|A\rangle\right] + bc\,\Re e\left[\langle\tilde{B}|\tilde{C}\rangle + \langle C|B\rangle\right] \qquad (3.66)$$

Tenendo conto del fatto che i prodotti scalari tra stati del Probe sono parametri complessi indipendenti il cui modulo può variare tra 0 e 1, possiamo massimizzare la (3.65) con

$$F = \frac{1}{2}\left(1 + 2b\,(a + c)\right) \qquad (3.67)$$

---

$$U|1\rangle|0\rangle|X\rangle = \tilde{a}|11\rangle|\tilde{A}\rangle + \tilde{b}_1|10\rangle|\tilde{B}_1\rangle + \tilde{b}_2|01\rangle|\tilde{B}_2\rangle + \tilde{c}|00\rangle|\tilde{C}\rangle$$

coi coefficienti a, $b_{1,2}$, c, $\tilde{a}$, $\tilde{b}_{1,2}$, $\tilde{c}$ complessi, e si utilizzano le proprietà **I** e **II** per ottenere le condizioni che tali coefficienti devono soddisfare.

tramite una opportuna scelta degli stati del Probe. Sempre scegliendo opportunamente tali stati è possibile fare in modo che la (3.66) sia sempre soddisfatta. Quindi ci siamo ricondotti a ricercare il massimo della funzione

$$F = a^2 + b^2 = \frac{1}{2}(1 + a^2 - c^2) \tag{3.68}$$

(la seconda uguaglianza viene dall'utilizzo della condizione di normalizzazione, che dà $b^2 = \frac{1}{2}(1 - a^2 - c^2)$) con la condizione

$$F = \frac{1}{2} + \sqrt{\frac{1}{2}(1 - a^2 - c^2)}(a + c) \tag{3.69}$$

che è la (3.67) con $b^2 = \frac{1}{2}(1 - a^2 - c^2)$.

La ricerca di tale massimo si può fare con il metodo dei moltiplicatori di Lagrange. Il risultato che si ottiene è il seguente:

$$\begin{aligned} a &= \frac{1}{2} + \sqrt{\frac{1}{8}} \\ b &= \sqrt{\frac{1}{8}} \\ c &= \frac{1}{2} - \sqrt{\frac{1}{8}} \end{aligned}$$

che dà la Fidelity ottima

$$F(1,2) = \frac{1}{2} + \sqrt{\frac{1}{8}} \tag{3.70}$$

La trasformazione di cloning ottima per gli stati BB84 si può scrivere esplicitamente come segue[14]:

$$\begin{aligned} U|0\rangle|0\rangle|X\rangle &= (\frac{1}{2} + \sqrt{\frac{1}{8}})|00\rangle|0\rangle + \sqrt{\frac{1}{8}}(|01\rangle + |10\rangle)|1\rangle + (\frac{1}{2} - \sqrt{\frac{1}{8}})|11\rangle|0\rangle \\ U|1\rangle|0\rangle|X\rangle &= (\frac{1}{2} + \sqrt{\frac{1}{8}})|11\rangle|1\rangle + \sqrt{\frac{1}{8}}(|10\rangle + |01\rangle)|0\rangle + (\frac{1}{2} - \sqrt{\frac{1}{8}})|00\rangle|1\rangle \end{aligned} \tag{3.71}$$

Ci rimane da mostrare che la (3.71) dà la stessa Fidelity per ogni stato della forma $|\psi_{xz}\rangle$. Questo segue dall'osservazione che ogni trasformazione unitaria

[14]Si trova che la dimensione minima per lo spazio di Hilbert del Probe è 2.

del tipo

$$U|0\rangle|0\rangle|X\rangle = a|00\rangle|0\rangle + b(|01\rangle + |10\rangle)|1\rangle + c|11\rangle|0\rangle$$
$$U|1\rangle|0\rangle|X\rangle = a|11\rangle|1\rangle + b(|10\rangle + |01\rangle)|0\rangle + c|00\rangle|1\rangle \qquad (3.72)$$

ha la proprietà richiesta. Infatti, se calcoliamo la Fidelity relativa al cloning del generico stato $|\psi_{xz}\rangle$ tramite il cloner specificato da (3.72) abbiamo:

$$F(\alpha) = (\alpha^4 + \beta^4)a^2 + b^2 + (\alpha^2\beta^2)2c^2 + 4\alpha^2\beta^2 b(a + c) \qquad (3.73)$$

Se inseriamo nella (3.73) le condizioni (3.62), (3.63) e (3.67), abbiamo immediatamente che la quantità $F(\alpha)$ è in realtà indipendente dal parametro $\alpha$, che è quello che ci rimaneva da dimostrare. Abbiamo perciò mostrato che oltre che per i quattro stati BB84 il nostro cloner è ottimo per tutti gli stati della forma $|\psi_{xz}\rangle$.

Se ci calcoliamo $\eta(1,2) = 2F(1,2) - 1$ attraverso la (3.70) abbiamo che

$$\eta(1,2) = \frac{1}{\sqrt{2}} \qquad (3.74)$$

che è il valore che si ottiene inserendo nella quantità $\tilde{\eta}\prime(N,M)$ di equazione (3.42)

$$\tilde{\eta}\prime = 2^{(M-N)} \frac{\sum_{l=0}^{N-1} \sqrt{\binom{N}{l}\binom{N}{l+1}}}{\sum_{j=0}^{M-1} \sqrt{\binom{M}{j}\binom{M}{j+1}}}$$

i valori N=1 e M=2. Il limite superiore per il fattore di contrazione $\eta\prime(1,2)$, in questo caso particolare, viene così raggiunto.

## 3.4 Schema crittografico BB84 e cloning ottimale di qubits equatoriali

Il BB84 è lo schema crittografico proposto da Bennett e Brassard nel 1984[15]. Scopo di questo schema è mettere a disposizione di due utenti, Alice ($\mathcal{A}$) e Bob ($\mathcal{B}$), che inizialmente non condividano un'informazione segreta, un metodo per comunicare in tutta riservatezza, con sicurezza assoluta e dimostrabile.

Il BB84 prevede l'utilizzo di due canali per la trasmissione delle informazioni tra $\mathcal{A}$ e $\mathcal{B}$: uno classico pubblico ed uno quantistico privato. Sul canale

[15]Per una breve trattazione di questo schema crittografico si veda Ref.[14].

classico pubblico (che può essere un quotidiano o un'emittente radio) si spedisce il messaggio cifrato (crittogramma); il canale quantistico è utilizzato per trasmettere la chiave. Le procedure di cifratura e decifratura sono note pubblicamente, mentre la chiave è mantenuta segreta, in modo che un avversario $\mathcal{E}$ (Eve) che abbia intercettato il crittogramma e conosca il metodo generale di cifratura, ma non la chiave, non possa dedurre niente di utile riguardo al messaggio originale. La sicurezza del canale privato in questo schema è cruciale.

In linea di principio qualunque canale privato classico può essere controllato passivamente da $\mathcal{E}$, senza che $\mathcal{A}$ e $\mathcal{B}$ si accorgano di essere spiati. Infatti, dato che tutte le informazioni (comprese le chiavi crittografiche) sono codificate tramite proprietà fisiche misurabili di qualche oggetto o segnale, la fisica classica offre la possibilità di atti di spionaggio passivi in cui la spia misura le proprietà fisiche del sistema in cui è codificata l'informazione senza conseguenze su di esso.

Nel BB84 il canale privato è di tipo quantistico: l'informazione viene codificata tramite lo stato di polarizzazione di un fotone. Se scegliamo gli stati $|0\rangle$ e $|1\rangle$ come autostati della polarizzazione orizzontale e verticale, gli stati utilizzati nel BB84 sono quelli di equazione (3.59):

$$
\begin{aligned}
&|0\rangle \\
&|1\rangle \\
&|\overline{0}\rangle = \sqrt{\frac{1}{2}}\,(|0\rangle + |1\rangle) \\
&|\overline{1}\rangle = \sqrt{\frac{1}{2}}\,(|0\rangle - |1\rangle)
\end{aligned}
$$

Poiché gli stati BB84 non sono tutti tra loro ortiogonali, il Teorema del No Cloning ci assicura che $\mathcal{E}$ non può determinare con precisione assoluta quale dei quattro stati è stato inviato sul canale quantistico, in modo da tenerne una copia per se ed inviarne una a $\mathcal{B}$ (spionaggio passivo che sarebbe possibile in un canale classico). Ogni tentativo di spiare il canale disturberà necessariamente il segnale, con conseguenze osservabili. In Ref.[20] si ricava un'espressione per l'informazione ottimale $I_{\mathcal{E}\mathcal{A}}$ che $\mathcal{E}$ può ottenere, in funzione del distubo medio D prodotto sul canale quando la sua interazione e la sua misura sul canale sono effettuate segnale per segnale.

In figura 3.2, tratta sempre da Ref.[20], è presentato il grafico della curva

$I_{\mathcal{EA}}$ come funzione del disturbo medio $D = 1 - F$ (F è la Fidelity relativa alla procedura di spionaggio, ovvero la Fidelity tra lo stato generato da Alice e quello ricevuto da Bob) insieme alla curva $I_{\mathcal{AB}}$ che dà la mutua informazione tra $\mathcal{A}$ e $\mathcal{B}$. Osserviamo innanzitutto che per d=0 $I_{\mathcal{AB}}$ è massima, mentre $I_{\mathcal{EA}}$ è nulla, come ci aspettavamo. L'intersezione tra le due curve avviene in corrispondenza del punto $\tilde{D}$ che corrisponde alla Fidelity F(1,2) per il cloning ottimale di qubits equatoriali di equazione (3.70). Questo significa che se Eve vuole attuare un "attacco simmetrico", i.e. una procedura di spionaggio in cui ottiene tanta informazione quanta ne ottiene Bob ($I_{\mathcal{AB}} = I_{\mathcal{EA}}$), non può trovare una tattica migliore che utilizzare il cloner ottimale. Ricordiamo che abbiamo dimostrato che il cloner $1 \longrightarrow 2$ ottimo è caratterizzato da $\eta\prime^{opt} = \tilde{\eta}$ e che questo cloner è quello ottimo anche se si restringe la classe dei qubits equatoriali di input da $\mathcal{C}_\phi$ alla classe BB84.

Figura 3.1: Grafico di $e'(N, M) = \tilde{\eta}\prime(N, M)$ con $(M > N)$ e scala logaritmica sull'asse N.

Figura 3.2: Grafico delle funzioni $I_{\mathcal{EA}}(D)$ e $I_{\mathcal{AB}}(D)$.

# Conclusioni

Nel lavoro presentato abbiamo ottenuto la quantità $\tilde{\eta}(N, M)$, che dà il limite superiore per la Fidelity con cui è possibile effettuare il cloning di qubits equatoriali.
Il risultato ottenuto è di particolare importanza, in quanto permette di concludere che restringere la classe di covarianza per la mappa T che descrive un generico cloner equivale ad alleggerire le condizioni che devono essere soddisfatte da tale mappa, e permette di trovare cloners che lavorano meglio di quello universale su classi ristrette di stati in ingresso.

Abbiamo verificato che il limite superiore $\tilde{\eta}$ viene effettivamente raggiunto nel caso N=1, M=2 e d=2. Sarebbe auspicabile verificare che il limite superiore viene raggiunto per ogni coppia (N,M) con $M > N$. Una possibile strada da seguire per risolvere questo problema è quella di trovare la forma esplicita della mappa di cloning ottima $\hat{T}$ covariante in fase, come viene fatto nel lavoro di Ref.[7], presentato nel capitolo 2, per il caso del cloning universale.

Un ulteriore problema aperto è la generalizzazione della procedura presentata al caso $d > 2$, ovvero la ricerca di mappe di cloning per sistemi quantistici di dimensione $d$ generica covarianti rispetto a sottogruppi del gruppo di covarianza universale $SU(d)$. Seguendo i ragionamenti esposti in questo lavoro, sarebbe in questo modo possibile evidenziare dei sottoinsiemi propri $\mathcal{C}_d$ di $\mathcal{H}$ per i quali è possibile realizzare un cloner migliore di quello universale. Questi risultati potrebbero avere importanti ripercussioni nella ricerca di nuovi metodi di comunicazione quantistica.

# Appendice A

# PROPRIETÀ DELLA FUNZIONE $\overline{F}^{opt}(N)$

## A.1 La disuguaglianza $\overline{F}^{opt}(N) \leq 1 \,\forall\, N$

Partiamo dalla (1.53) che riscriviamo per comodità:

$$\overline{F}_{opt} = \frac{1}{2} + \frac{1}{2^{N+1}} \sum_{l=0}^{N-1} \sqrt{\binom{N}{l}\binom{N}{l+1}} \tag{A.1}$$

Cominciamo con le seguenti maggiorazioni:

$$\begin{aligned}
\sum_{l=0}^{N-1} \sqrt{\binom{N}{l}\binom{N}{l+1}} &\leq \frac{1}{2} \sum_{l=0}^{N-1} [\binom{N}{l} + \binom{N}{l+1}] = \\
&= \frac{1}{2} \sum_{l=0}^{N-1} [\binom{N}{l}(1 + \frac{N-l}{l+1}) = \\
&= \frac{1}{2} \sum_{l=0}^{N-1} \binom{N}{l} \frac{N+1}{l+1} = \\
&= \frac{1}{2} \sum_{l=0}^{N-1} \binom{N+1}{l+1} \frac{1}{N-l} = \\
&\leq \frac{1}{2} \sum_{l=0}^{N-1} \binom{N+1}{l+1} =
\end{aligned}$$

$$\leq \frac{1}{2}\sum_{l=-1}^{N}\binom{N+1}{l+1} = \frac{1}{2}2^{N+1} = 2^N \ \forall N$$

dove il primo passaggio è stato ottenuto utilizzando la relazione tra media aritmetica e media geometrica, mentre i successivi tenendo conto che le somme che compaiono nei vari termini sono tutte serie a termini positivi. Possiamo così scrivere:

$$\begin{aligned}\overline{F}_{opt} &= \frac{1}{2} + \frac{1}{2^{N+1}}\sum_{l=0}^{N-1}\sqrt{\binom{N}{l}\binom{N}{l+1}} = \\ &\leq \frac{1}{2} + \frac{1}{2^{N+1}}2^N = \frac{1}{2} + \frac{1}{2} = 1 \ \forall N\end{aligned}$$

Che è quello che volevamo dimostrare.

## A.2 Calcolo del limite $\lim_{N\to\infty}\overline{F}^{opt}(N)$

Per $N \longrightarrow \infty$ si ha

$$\binom{N}{l+1} = \binom{N}{l} + o(N) \tag{A.2}$$

da cui segue immediatamente:

$$\begin{aligned}lim_{N\to\infty}\overline{F}^{opt}(N) &= lim_{N\to\infty}\left\{\frac{1}{2} + \frac{1}{2^{N+1}}\sum_{l=0}^{N-1}\sqrt{\binom{N}{l}\binom{N}{l+1}}\right\} = \\ &= \frac{1}{2} + \frac{1}{2^N}\sum_{l=0}^{N}\binom{N}{l} = 1\end{aligned} \tag{A.3}$$

# Appendice B

# LA CONDIZIONE DI COVARIANZA IN FASE

Ci proponiamo di mostrare qui l'equivalenza tra le condizioni (3.11) e (3.12) che riscriviamo per comodità:

$$\sum_k \sum_{\alpha,\beta} \gamma_k^{\alpha\beta} \Sigma_{\alpha\beta}(U_\phi \omega U_\phi^*) = \sum_k \sum_{\alpha,\beta} \gamma_k^{\alpha\beta} U_\phi \Sigma_{\alpha\beta}(\omega) U_\phi^* \tag{B.1}$$

$$\begin{aligned} &\Gamma_{01} = \Gamma_{02} = \Gamma_{03} = 0 \\ &\Gamma_{10} = \Gamma_{12} = \Gamma_{13} = 0 \\ &\Gamma_{20} = \Gamma_{21} = 0 \\ &\Gamma_{30} = \Gamma_{31} = 0 \end{aligned} \tag{B.2}$$

Per dimostrare tale equivalenza dobbiamo scrivere la (B.1) esplicitamente. A tal fine cominciamo a calcolarci le regole di commutazione tra la generica matrice $U_\phi$ e gli operatori $\sigma_\alpha$, $(\alpha = 0, 1, 2, 3)$. Ricordiamo che

$$\sigma_0 \equiv \sigma_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \sigma_1 \equiv \sigma- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 \equiv \pi_+ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \sigma_3 \equiv \pi_- = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Inoltre

$$U_\phi = \exp\left[-\frac{i}{2}(\sigma_z - 1)\phi\right] = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

da cui

$$U_\phi^* = \exp\left[\frac{i}{2}(\sigma_z - 1)\phi\right] = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix}$$

Poichè $\sigma_2$ e $\sigma_3$ contengono solo la matrice di Pauli $\sigma_z$ abbiamo immediatamente:

$$[U_\phi, \sigma_2] = 0, \quad [U_\phi^*, \sigma_2] = 0$$
$$[U_\phi, \sigma_3] = 0, \quad [U_\phi^*, \sigma_3] = 0$$

Invece di calcolare i rimanenti commutatori, calcoliamoci ora le seguenti quantità che risultano più utili per i nostri scopi:

$$\begin{aligned}
U_\phi\sigma_2 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \sigma_2 \\
U_\phi^*\sigma_2 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \sigma_2 \\
U_\phi\sigma_3 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & e^{i\phi} \end{pmatrix} = e^{i\phi}\sigma_3 \\
U_\phi^*\sigma_3 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & e^{-i\phi} \end{pmatrix} = e^{-i\phi}\sigma_3 \\
U_\phi\sigma_0 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \sigma_0 \\
\sigma_0 U_\phi &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} = \begin{pmatrix} 0 & e^{i\phi} \\ 0 & 0 \end{pmatrix} = e^{i\phi}\sigma_0 \\
U_\phi^*\sigma_0 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \sigma_0 \\
\sigma_0 U_\phi^* &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix} = \begin{pmatrix} 0 & e^{-i\phi} \\ 0 & 0 \end{pmatrix} = e^{-i\phi}\sigma_0 \\
U_\phi\sigma_1 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ e^{i\phi}0 & 0 \end{pmatrix} = e^{i\phi}\sigma_0 \\
\sigma_1 U_\phi &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \sigma_1 \\
U_\phi^*\sigma_1 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ e^{-i\phi} & 0 \end{pmatrix} = e^{-i\phi}\sigma_1 \\
\sigma_1 U_\phi^* &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \sigma_1
\end{aligned}$$

Possiamo ora passare al calcolo delle quantità:

| $\Sigma_{\alpha\beta}$ | $\Sigma_{\alpha\beta}(U_\phi \omega U_\phi^*)$ | $U_\phi \Sigma_{\alpha\beta}(\omega) U_\phi^*$ |
|---|---|---|
| $\Sigma_{00}$ | $\sigma_0\omega\sigma_1$ | $\sigma_0\omega\sigma_1$ |
| $\Sigma_{01}$ | $e^{i\phi}\sigma_0\omega\sigma_0$ | $\sigma_0\omega e^{-i\phi}\sigma_1$ |
| $\Sigma_{02}$ | $e^{i\phi}\sigma_0\omega\sigma_2$ | $\sigma_0\omega\sigma_2$ |
| $\Sigma_{03}$ | $e^{i\phi}\sigma_0\omega\sigma_3$ | $\sigma_0\omega e^{-i\phi}\sigma_3$ |
| $\Sigma_{10}$ | $\sigma_1\omega e^{-i\phi}\sigma_1$ | $e^{i\phi}\sigma_1\omega\sigma_1$ |
| $\Sigma_{11}$ | $\sigma_1\omega\sigma_0$ | $\sigma_1\omega\sigma_0$ |
| $\Sigma_{12}$ | $\sigma_1\omega\sigma_2$ | $e^{i\phi}\sigma_1\omega\sigma_2$ |
| $\Sigma_{13}$ | $\sigma_1\omega e^{-i\phi}\sigma_3$ | $e^{i\phi}\sigma_1\omega e^{-i\phi}\sigma_3$ |
| $\Sigma_{20}$ | $\sigma_2\omega e^{-i\phi}\sigma_1$ | $\sigma_2\omega\sigma_1$ |
| $\Sigma_{21}$ | $\sigma_2\omega\sigma_0$ | $\sigma_2\omega e^{-i\phi}\sigma_0$ |
| $\Sigma_{22}$ | $\sigma_2\omega\sigma_2$ | $\sigma_2\omega\sigma_2$ |
| $\Sigma_{23}$ | $\sigma_2\omega e^{-i\phi}\sigma_3$ | $\sigma_2\omega e^{-i\phi}\sigma_3$ |
| $\Sigma_{30}$ | $\sigma_3\omega\sigma_1$ | $e^{i\phi}\sigma_3\omega\sigma_1$ |
| $\Sigma_{31}$ | $e^{i\phi}\sigma_3\omega\sigma_0$ | $\sigma_3\omega\sigma_0$ |
| $\Sigma_{32}$ | $e^{i\phi}\sigma_3\omega\sigma_2$ | $e^{i\phi}\sigma_3\omega\sigma_2$ |
| $\Sigma_{33}$ | $\sigma_3\omega\sigma_3$ | $\sigma_3\omega\sigma_3$ |

Scriviamo ora il primo membro di (B.1)

$$\sum_k \quad [\gamma_k^{00}(\sigma_0\omega\sigma_1) + \gamma_k^{01}(e^{i\phi}\sigma_0\omega\sigma_0) + \gamma_k^{02}(e^{i\phi}\sigma_0\omega\sigma_2) + \gamma_k^{03}(e^{i\phi}\sigma_0\omega\sigma_3) +$$
$$+\gamma_k^{10}(\sigma_1\omega e^{-i\phi}\sigma_1) + \gamma_k^{11}(\sigma_1\omega\sigma_0) + \gamma_k^{12}(\sigma_1\omega\sigma_2) + \gamma_k^{13}(\sigma_1\omega\sigma_3) +$$
$$+\gamma_k^{20}(\sigma_2\omega e^{-i\phi}\sigma_1) + \gamma_k^{21}(\sigma_2\omega\sigma_0) + \gamma_k^{22}(\sigma_2\omega\sigma_2) + \gamma_k^{23}(e^{-i\phi}\sigma_2\omega\sigma_3) +$$
$$+\gamma_k^{30}(\sigma_3\omega\sigma_1) + \gamma_k^{31}(\sigma_3 e^{i\phi}\omega\sigma_0) + \gamma_k^{32}(\sigma_3 e^{i\phi}\omega\sigma_2) + \gamma_k^{33}(\sigma_3\omega\sigma_3)]$$

Il secondo membro si scrive invece

$$\sum_k \quad [\gamma_k^{00}(\sigma_0\omega\sigma_1) + \gamma_k^{01}(\sigma_0\omega e^{-i\phi}\sigma_0) + \gamma_k^{02}(\sigma_0\omega\sigma_2) + \gamma_k^{03}(\sigma_0\omega\sigma_3) +$$
$$+\gamma_k^{10}(e^{i\phi}\sigma_1\omega\sigma_1) + \gamma_k^{11}(\sigma_1\omega\sigma_0) + \gamma_k^{12}(e^{i\phi}\sigma_1\omega\sigma_2) + \gamma_k^{13}(e^{i\phi}\sigma_1\omega\sigma_3) +$$
$$+\gamma_k^{20}(\sigma_2\omega\sigma_1) + \gamma_k^{21}(e^{-i\phi}\sigma_2\omega\sigma_0) + \gamma_k^{22}(\sigma_2\omega\sigma_2) + \gamma_k^{23}(e^{-i\phi}\sigma_2\omega\sigma_3) +$$

$$+\gamma_k^{30}(e^{i\phi}\sigma_3\omega\sigma_1)+\gamma_k^{31}(\sigma_3\omega\sigma_0)+\gamma_k^{32}(\sigma_3 e^{i\phi}\omega\sigma_2)+\gamma_k^{33}(\sigma_3\omega\sigma_3)]$$

Poichè l'uguaglianza tra il primo ed il secondo membro deve valere per ogni $\phi$ la (B.1) è equivalente alle tre seguenti condizioni che si trovano uguagliando i termini con la stessa dipendenza dal parametro $\phi$ stesso:

- **Condizione I**

$$\sum_k \quad [\gamma_k^{12}(\sigma_1\omega\sigma_2)+\gamma_k^{13}(\sigma_1\omega\sigma_3)+\gamma_k^{21}(\sigma_2\omega\sigma_0)+\gamma_k^{30}(\sigma_3\omega\sigma_1)+$$
$$-\gamma_k^{02}(\sigma_0\omega\sigma_2)-\gamma_k^{03}(\sigma_0\omega\sigma_3)-\gamma_k^{20}(\sigma_2\omega\sigma_1)-\gamma_k^{31}(\sigma_3\omega\sigma_0)]=0$$

- **Condizione II.**

$$\sum_k \quad [\gamma_k^{01}(\sigma_0\omega\sigma_0)+\gamma_k^{02}(\sigma_0\omega\sigma_2)+\gamma_k^{03}(\sigma_0\omega\sigma_3)+\gamma_k^{31}(\sigma_3\omega\sigma_0)+$$
$$-\gamma_k^{10}(\sigma_1\omega\sigma_1)-\gamma_k^{12}(\sigma_1\omega\sigma_2)-\gamma_k^{13}(\sigma_1\omega\sigma_3)-\gamma_k^{30}(\sigma_3\omega\sigma_1)]=0$$

- **Condizione III.**

$$\sum_k [\gamma_k^{10}(\sigma_1\omega\sigma_1)+\gamma_k^{20}(\sigma_2\omega\sigma_1)-\gamma_k^{21}(\sigma_2\omega\sigma_0)-\gamma_k^{01}(\sigma_0\omega\sigma_0)]=0$$

Se scriviamo la generica matrice densità $\omega \in End(\mathcal{H})$ come[1]

$$\omega=\begin{pmatrix}\alpha & \gamma\\ \gamma^* & 1-\alpha\end{pmatrix} \qquad (\alpha\in[0,1]\subset R,\gamma\in\mathbb{C}) \tag{B.3}$$

($|\gamma|^2=\alpha(1-\alpha)$), possiamo esplicitare i vari termini contenuti nelle somme

$$\begin{aligned}
\sigma_0\omega\sigma_0 &= \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}\alpha&\gamma\\\gamma^*&1-\alpha\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\\
&= \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&\alpha\\0&\gamma^*\end{pmatrix}=\begin{pmatrix}0&\gamma^*\\0&0\end{pmatrix}\\
\sigma_0\omega\sigma_1 &= \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}\alpha&\gamma\\\gamma^*&1-\alpha\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}=\\
&= \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}\gamma&0\\1-\alpha&0\end{pmatrix}=\begin{pmatrix}1-\alpha&0\\0&0\end{pmatrix}
\end{aligned}$$

[1]Ricordiamo che $\omega$ è stato puro.

$$
\begin{aligned}
\sigma_0\omega\sigma_2 &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \gamma^* & 1-\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \\
&= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ \gamma^* & 0 \end{pmatrix} = \begin{pmatrix} \gamma^* & 0 \\ 0 & 0 \end{pmatrix} \\
\sigma_0\omega\sigma_3 &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \gamma^* & 1-\alpha \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \\
&= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & \alpha \\ 0 & \gamma^* \end{pmatrix} = \begin{pmatrix} 0 & 1-\alpha \\ 0 & 0 \end{pmatrix} \\
\sigma_1\omega\sigma_0 &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \alpha \\ 0 & \gamma^* \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix} \\
\sigma_1\omega\sigma_1 &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \gamma & 0 \\ 1-\alpha & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \gamma & 0 \end{pmatrix} \\
\sigma_1\omega\sigma_2 &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ \gamma^* & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \alpha & 0 \end{pmatrix} \\
\sigma_1\omega\sigma_3 &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \gamma \\ 0 & 1-\alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \gamma \end{pmatrix} \\
\sigma_2\omega\sigma_0 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & \alpha \\ 0 & \gamma^* \end{pmatrix} = \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} \\
\sigma_2\omega\sigma_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \gamma & 0 \\ 1-\alpha & 0 \end{pmatrix} = \begin{pmatrix} \gamma & 0 \\ 0 & 0 \end{pmatrix} \\
\sigma_2\omega\sigma_2 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ \gamma^* & 0 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \\
\sigma_2\omega\sigma_3 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & \gamma \\ 0 & 1-\alpha \end{pmatrix} = \begin{pmatrix} 0 & \gamma \\ 0 & 0 \end{pmatrix} \\
\sigma_3\omega\sigma_0 &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \alpha \\ 0 & \gamma^* \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \gamma^* \end{pmatrix} \\
\sigma_3\omega\sigma_1 &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \gamma & 0 \\ 1-\alpha & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1-\alpha & 0 \end{pmatrix} \\
\sigma_3\omega\sigma_2 &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ \gamma^* & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \gamma^* & 0 \end{pmatrix} \\
\sigma_3\omega\sigma_3 &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \gamma \\ 0 & 1-\alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1-\alpha \end{pmatrix}
\end{aligned}
$$

Se indichiamo $\sum_k \gamma_k^{\alpha\beta}$ con $\Gamma_{\alpha\beta}$ le condizioni I, II e III diventano

- **I**

$$\begin{pmatrix} \Gamma_{02}\gamma^* & \Gamma_{21}\alpha + \Gamma_{03}(1-\alpha) + \Gamma_{20}\alpha \\ \Gamma_{12}\alpha + \Gamma_{31}(1-\alpha) + \Gamma_{30}(1-\alpha) & \Gamma_{13}\gamma \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

- **II**

$$\begin{pmatrix} \Gamma_{02}\gamma^* & \Gamma_{01}\gamma^* + \Gamma_{03}(1-\alpha) \\ \Gamma_{10}\gamma + \Gamma_{12}\alpha + \Gamma_{30}(1-\alpha) & \Gamma_{31}\gamma^* + \Gamma_{13}\gamma \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

- **III**

$$\begin{pmatrix} \Gamma_{20}\gamma & \Gamma_{21}\alpha + \Gamma_{01}\gamma^* \\ \Gamma_{10}\gamma & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Osserviamo che per definizione

$$\Gamma_{\alpha\beta} = \sum_k \gamma_k^{\alpha\beta} = \sum_k c_k^{\alpha} c_k^{*\beta}$$

e

$$\Gamma_{\beta\alpha} = \sum_k \gamma_k^{\beta\alpha} = \sum_k c_k^{\beta} c_k^{*\alpha} = \Gamma_{\alpha\beta}^*$$

per cui $\Gamma_{\alpha\beta} = 0$ se e solo se $\Gamma_{\beta\alpha} = 0$. Utilizzando questo fatto le condizioni I, II e III si traducono infine nelle seguenti condizioni sui coefficienti $\Gamma_{\alpha\beta}$:

$$\begin{aligned} &\Gamma_{01} = \Gamma_{02} = \Gamma_{03} = 0 \\ &\Gamma_{10} = \Gamma_{12} = \Gamma_{13} = 0 \\ &\Gamma_{20} = \Gamma_{21} = 0 \\ &\Gamma_{30} = \Gamma_{31} = 0 \end{aligned} \tag{B.4}$$

che è quello che volevamo dimostrare.

# Appendice C

# GRAFICI

Figura C.1: $e(1, M) = \eta(1, M)$, $e'(1, M) = \tilde{\eta}\prime(1, M)$

Figura C.2: $e(2, M) = \eta(2, M)$, $e'(2, M) = \tilde{\eta}\prime(2, M)$

Figura C.3: $e(3, M) = \eta(3, M)$, $e'(3, M) = \tilde{\eta}\prime(3, M)$

Figura C.4: $e(4, M) = \eta(4, M)$, $e'(4, M) = \tilde{\eta}\prime(4, M)$

# Bibliografia


[1] Carl W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, cap VIII, New York, San Francisco and London, 1976

[2] G. M. D'Ariano, *Quantum Estimation Theory and Optical Detection* in *Quantum Optics and the Spectroscopy of Solids*, ed. by T. Hakioglu and S. Shumovsky, pp.139-174, Kluwer Academic Publishers, 1997, Printed in the Netherlands.

[3] G. M D'Ariano, C. Macchiavello, M. F. Sacchi, Physics Letters A, **248**, 103-108, (1998)

[4] A. Kolmogorov, *Foundations of the theory of Probability*, Chelsea Bronx, New York, 1968, $2^a$ edizione.

[5] S. Massar e S. Popescu, Physical Review Letters **74**, 1259 (1995).

[6] N. Gisin e S. Massar, Physical Review Letters **79**, 2153 (1997).

[7] R. F. Werner, Physical Review A **58**, 1827 (1998).

[8] M. Ozawa, *Squeezed States and Nonclassical Light* , ed. by P.Tombesi and E.R.Pike, pag 263, Plenum, New York, 1989.

[9] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North Holland, Amsterdam, 1982.

[10] H. F. Jones *Groups, Representations and Physics*, Adam Hilger,pag 161, Bristol and New York, 1990.

[11] W. F. Stinespring, Proceedings American Mathematical Society **6**, 211-216, (1955).

[12] D. Bruß, D. DiVincenzo, A. Ekert, C. Fuchs, C. Macchiavello e J. Smolin, Physical Review A **57**, 2368 (1998).

[13] Dagmar Bruß, note non pubblicate.

[14] H. Bennett, G. Brassard e A. Ekert, Le Scienze **292**, pag.84 (Dicembre 1992).

[15] D. Bruß, A. Ekert e C. Macchiavello, Physical Review Letters **81**, 2598 (1998).

[16] Horace P. Yuen, Physics Letters **113A**, 405 (1986).

[17] G. M. D'Ariano e H. P. Yuen, Physical Review Letters **76**, 2832 (1996).

[18] K. Kraus, Annals of Physics **64**, 311-335 (1971)

[19] W. K. Wooters e W. H. Zurek, Nature (London) **299**, 802 (1982).

[20] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu e A. Peres, Physical Review A **56**, 1163 (1997)

[21] G. Lindbland, Commun. Math. Phys. **48** 199 (1976)

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

# Ringraziamenti

Desidero ringraziare innanzitutto il Prof. G. M. D'Ariano e la Dott. Chiara Macchiavello che mi hanno seguito durante lo svolgimento della tesi, mettendomi a disposizione il loro tempo e la loro competenza, molto spesso anche per interi pomeriggi. Da loro ho anche ricevuto l'incoraggiamento e gli apprezzamenti che mi hanno permesso di portare a termine questo lavoro con serenità e determinazione. Mi hanno anche dato l'opportunità di incontrare diverse persone che lavorano nel campo della Fisica dell'Informazione Quantistica, tra le quali un ringraziamento particolare a Dagmar Bruß.
Ringrazio poi Paolo, con cui ho condiviso le ansie e le preoccupazioni di questi mesi di lavoro.

Questa tesi chiude simbolicamente il periodo della mia vita universitaria; vorrei utilizzarla perciò per ringraziare tutte le persone che mi sono state vicine in questi anni.
Un grazie davvero speciale ad Angela, Raoul (cicio!) e Benedetta (cicia!), per i bei momenti vissuti insieme (...quelli brutti li ho superati sempre grazie a loro!) e per la loro amicizia, che è stata e sarà un punto fermo nella mia vita.
Grazie a Christian, la cui lontananza mi pesa sempre tanto.
Grazie anche a Silvia (che ringrazio altrimenti tra qualche anno mi licenzia!), Francesca, Linda, Marella, Elisabetta, Matteo il Coccio, Matteo il Morač, Marco l'Oppe e alla Marga.
Grazie alla Corač e alla Depa, le mie colonne preferite.
Grazie a Mission ...anche per avermi aiutato a fare i grafici della tesi.

*Liebe hat mich glücklich gemacht*