

Università Cattolica del Sacro Cuore di Brescia

Facoltà di Scienze matematiche, fisiche e naturali

Anno accademico 2003-04

Tesi per la laurea di primo livello

# Teletrasporto quantistico

**Autore:** *Diego Fasoli*

Matricola 3000854

**Relatore:** *Prof. Fausto Borgonovi*

**Correlatore:** *Prof. Franco Dalfovo*

## Abstract

Il teletrasporto è, in generale, la capacità di viaggiare semplicemente riapparendo in qualche luogo arbitrariamente lontano, senza passare fisicamente per tutti i punti che separano il luogo di partenza da quello di arrivo, anche se ciò che viene trasferito non è la materia costituente l'oggetto, bensì l'insieme delle sue proprietà, ovvero il suo stato, e ad una velocità comunque non superiore a quella della luce.

Esistono differenti tecniche di teletrasporto, che si distinguono in classiche e quantistiche.

La tecnica migliore sotto ogni aspetto è quella del teletrasporto quantistico, introdotta nel 1993 da Bennett *et al.* [1], che fa uso di un particolare fenomeno noto come *entanglement*, implementabile per esempio attraverso la tecnica ottica.

La possibilità di disporre di un *entanglement* massimale, assieme a porte quantistiche e trasmissione classica affidabili, è fondamentale per teletrasportare uno stato senza distorsioni.

Il teletrasporto è importante non solo dal punto di vista concettuale, in quanto costituisce una delle incredibili conseguenze della meccanica quantistica, ma anche dal punto di vista applicativo, svolgendo un ruolo chiave nella creazione delle memorie quantistiche, nonché nella protezione di trasmissioni dati e nella progettazione di porte quantistiche affidabili.

# Indice

<b>Premessa</b>	<b>3</b>
<b>Introduzione</b>	<b>3</b>
<b>1 Analisi del teletrasporto</b>	<b>5</b>
1.1 Teletrasporto quantistico . . . . .	6
1.1.1 Teletrasporto quantistico di uno stato sconosciuto . . . . .	6
1.1.2 Teletrasporto quantistico di uno stato noto . . . . .	11
1.2 Teletrasporto classico a variabili locali nascoste . . . . .	13
<b>2 Fonti di disturbo per il teletrasporto quantistico</b>	<b>14</b>
2.1 Imperfezioni delle porte quantistiche . . . . .	14
2.2 Errori nella trasmissione dell'informazione classica . . . . .	15
2.3 Entanglement non massimale . . . . .	15
<b>3 Realizzazione sperimentale del teletrasporto quantistico</b>	<b>21</b>
<b>4 Applicazioni del teletrasporto quantistico</b>	<b>25</b>
4.1 Memorie quantistiche . . . . .	26
4.2 Protezione delle trasmissioni dati dal rumore quantistico . . . . .	26
4.3 Porte quantistiche più affidabili . . . . .	26
4.4 Testare la validità della meccanica quantistica . . . . .	31
<b>5 Appendice</b>	<b>32</b>
5.1 Qubit e stati entangled . . . . .	32
5.2 Entropia di Shannon, entropia di von Neumann e ridondanza . . . . .	34
5.3 Porte quantistiche X, Y, Z, H e CNOT . . . . .	35
5.4 Fedeltà classica e quantistica . . . . .	38
<b>Bibliografia</b>	<b>39</b>

# Premessa

Il lavoro inizia con la seguente introduzione, nella quale viene presentato in modo intuitivo (e quindi poco rigoroso) cosa sia il teletrasporto in generale, per poi proseguire, nelle sezioni 1 e 2, con una spiegazione fisica e matematica dettagliata degli aspetti teorici del problema.

Gli aspetti sperimentali del teletrasporto quantistico vengono invece analizzati nella sezione 3, prestando particolare attenzione alla tecnica di implementazione ottica, in quanto essa è stata la prima, a livello storico, ad essere utilizzata nella verifica sperimentale del problema.

Per concludere, nella sezione 4, vengono analizzate le principali applicazioni oggi note del teletrasporto quantistico. Come complemento di questo lavoro è stata poi aggiunta un'appendice, ovvero la sezione 5, nella quale vengono spiegati in modo dettagliato i prerequisiti necessari per la comprensione di tutte le sezioni precedenti.

## Introduzione

Il teletrasporto quantistico è un argomento che appartiene all'ambito della *computazione quantistica* e dell'*informazione quantistica*, un campo di ricerca molto recente che si occupa della manipolazione degli stati quantistici e collocabile poi, a sua volta, nell'ambito della meccanica quantistica NON RELATIVISTICA.

Il teletrasporto è, in generale, la capacità di viaggiare semplicemente riapparendo in qualche luogo arbitrariamente lontano, senza passare fisicamente per tutti i punti che separano il luogo di partenza da quello di arrivo.

Un'importante precisazione da fare è rappresentata dal fatto che ciò che viene teletrasportato non è la materia costituente l'oggetto, bensì l'insieme delle sue proprietà, ovvero il suo stato.

Questo stato, una volta teletrasportato in qualche luogo lontano, viene lì utilizzato per "modellare" un altro blocco di materia, che non coincide con quella ORIGINALE dell'oggetto.

In altri termini, un oggetto da teletrasportare può essere completamente caratterizzato dalle sue proprietà, il che implica che per realizzare una sua copia in qualche luogo lontano non occorrono necessariamente le parti dell'oggetto originale: tutto quello che serve è trasmettere le informazioni contenenti le proprietà del corpo, così che esse possano essere utilizzate per ricostruirlo altrove.

Esistono differenti modalità di teletrasporto, cioè differenti procedure che permettono di trasmettere le proprietà dell'oggetto, e che si contraddistinguono tra loro proprio per la tecnica con la quale riescono a trasmettere questa informazione.

La modalità di trasmissione dell'informazione certamente più semplice, sia dal punto di vista concettuale che costruttivo, è rappresentata dalla MISURAZIONE diretta dello stato dell'oggetto e dalla trasmissione, tramite un canale di comunicazione classica, della descrizione di tale stato in termini di bit [2].

La comunicazione nel canale classico può essere realizzata per esempio trasmettendo impulsi di tensione o di corrente in un cavo elettrico od impulsi luminosi in una fibra ottica, collegante i due interlocutori.

Questa rappresenta una particolare tecnica di teletrasporto CLASSICO, che presenta però una serie di problemi non superabili.

Intendendo come stato classico quello in cui collassa la funzione d'onda di un sistema quantistico dopo una misurazione, allora tale stato sarà descritto da un numero finito di bit solamente nel caso in cui l'oggetto da teletrasportare possa trovarsi in un numero finito di questi stati classici: per attuare questa descrizione basta semplicemente associare, secondo una determinata convenzione, ciascuno di questi stati classici ad una particolare combinazione dei bit considerati.

Quindi in tal caso l'oggetto può essere teletrasportato trasmettendo, nel canale di comunicazione classica, una quantità finita di informazione classica, ovvero di bit.

Possiamo pertanto concludere che questo particolare tipo di teletrasporto classico ha successo nel teletrasportare uno stato classico del genere appena descritto.

I problemi di questa procedura nascono però quando si cerca di utilizzarla per il teletrasporto di uno stato quantistico, ovvero di una combinazione lineare (in generale a coefficienti complessi) di stati classici.

Infatti, supponiamo per esempio di avere un sistema quantistico che possa assumere solamente due stati classici  $|0\rangle$  e  $|1\rangle$ .

Esso si troverà allora in generale nello stato quantistico seguente (vedere anche il paragrafo 5.1):

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

Come si osserva, questo stato è completamente caratterizzato dalle costanti reali  $\theta$  e  $\phi$ , che, in quanto reali, presenteranno in generale un numero infinito di decimali.

Pertanto, per descrivere con precisione infinita questo stato quantistico, è necessario descrivere con precisione infinita le due costanti  $\theta$  e  $\phi$  e pertanto sono in generale necessari  $2 \cdot \infty$  bit di informazione classica.

In altri termini, questa modalità di teletrasporto classico non può essere utilizzata per teletrasportare con precisione infinita uno stato quantistico, il che implica che l'oggetto teletrasportato subirà una deformazione durante questa procedura.

Un secondo problema che affligge questo particolare tipo di teletrasporto classico è rappresentato dal fatto che, per poter descrivere le costanti  $\theta$  e  $\phi$ , è necessario prima conoscerle.

Ma per conoscerle è necessario effettuare delle misurazioni sullo stato quantistico.

Tramite una sola misura però non è possibile ottenere i valori di queste due costanti.

Bisogna invece preparare tanti sistemi identici a quello considerato, tutti nello stesso stato  $|\psi\rangle$ , ed effettuare per ognuno la misura di tale stato.

Si otterrà quindi a volte, come risultato della misura, lo stato  $|0\rangle$ , mentre a volte lo stato  $|1\rangle$ .

Quando il numero di sistemi identici sui quali si effettua la misurazione tende ad infinito, si ha che il numero di volte che si verifica lo stato  $|0\rangle$  oppure lo stato  $|1\rangle$  tende a diventare uguale alle loro rispettive probabilità di verificarsi, un risultato noto come *legge dei grandi numeri*.

Una volta note le probabilità degli eventi  $|0\rangle$  ed  $|1\rangle$  è possibile determinare lo stato quantistico.

In realtà, per essere precisi, questo metodo permette di conoscere solamente la costante  $\theta$ .

Per determinare anche la costante  $\phi$  sarà necessario effettuare delle misurazioni, sempre sullo stato  $|\psi\rangle$ , di altre osservabili, sempre con infiniti sistemi identici (basta vedere come esempio l'esperimento di Stern-Gerlach).

Quindi solamente con infinite misurazioni è possibile conoscere con precisione infinita lo stato quantistico  $|\psi\rangle$ .

Quindi, anche ammesso che sia possibile avere a disposizione diverse copie del sistema e tutte nello stesso stato, non sarà possibile ricostruirlo esattamente, il che introduce una ulteriore distorsione dell'oggetto teletrasportato.

Più realisticamente, comunque, non saranno disponibili copie dell'oggetto da teletrasportare (basta pensare al caso in cui si voglia teletrasportare una persona) e quindi si dovrà cercare di applicare la procedura di teletrasporto classico esaminata a questa situazione restrittiva.

L'oggetto da teletrasportare potrà anche essere classico, ma esso è infine composta da atomi e molecole, che obbediscono alle leggi della meccanica quantistica.

Quindi ad ogni modo bisognerà restringere l'analisi a quella del teletrasporto di uno stato quantistico generico.

Si potrebbe per esempio pensare di ricostruire l'oggetto acquisendo le informazioni della posizione e della velocità di ciascuna particella che lo costituisce.

Avendo però a disposizione solamente una copia dell'oggetto, bisognerà effettuare su ciascuna particella prima una misura della posizione e poi una misura della velocità, o viceversa (in altri termini le misure di posizione e velocità vengono effettuate sulla stessa particella, mentre, qualora fossero state a disposizione delle copie del sistema, si sarebbe potuta eseguire la misura di posizione su una copia, e quella di velocità su un'altra).

Il problema però è che le grandezze posizione e velocità sono incompatibili, il che implica che la misurazione di una influenza il risultato della misurazione dell'altra.

Infatti, in accordo con il cosiddetto *postulato della misura* della meccanica quantistica, le proprietà fisiche incompatibili (cioè quelle descritte da operatori che non commutano tra di loro, in questo esempio la posizione e la velocità) di un oggetto non possono essere misurate contemporaneamente con precisione arbitraria.

E' da ricordare infatti che la misura di grandezze compatibili comporta la formazione di termini di interferenza che non sono invece presenti nella misura di grandezze incompatibili, il che è indice di una perturbazione introdotta dalla misura sul sistema studiato.

E' questa perturbazione che altera l'informazione circa le altre proprietà del sistema che vogliamo misurare.

Questa caratteristica dei sistemi quantistici viene solitamente identificata attraverso il principio di indeterminazione di Heisenberg, anche se in realtà non è questa la corretta interpretazione del principio.

Infatti anche una singola misura causa la perturbazione del sistema, mentre invece il principio di indeterminazione di Heisenberg vale per misure effettuate su un gran numero di copie del sistema.

Ad ogni modo, l'effetto di una misura è quello di alterare il sistema, il che implica che, tramite una sola misurazione, non è possibile conoscere completamente lo stato.

Questo quindi comporta che lo stato quantistico subirà una deformazione durante questa procedura di teletrasporto classico.

Un problema insormontabile di tale procedura è rappresentato quindi dal fatto che, per trasmettere l'informazione, richiede che questa sia conosciuta.

Infatti questa tecnica non potrà mai essere utilizzata per il teletrasporto di uno stato, classico o quantistico, sconosciuto.

Un altro problema di questa procedura, come visto in precedenza, sta nel fatto che essa si basa su una descrizione diretta dello stato, la quale richiede infiniti bit nel caso di uno stato quantistico.

Esiste comunque una seconda tecnica di teletrasporto classico, che, come verrà meglio spiegato nel paragrafo 1.2, si basa sull'uso di variabili locali nascoste (LHV) [3], per ipotesi condivise tra il trasmettitore ed il ricevitore dello stato da teletrasportare.

Il fatto di utilizzare delle LHV permette di etichettare questa procedura come classica, dato che le LHV sono delle grandezze introdotte per tentare di riformulare la meccanica quantistica in un modo matematicamente equivalente ma tale che essa abbia una struttura più simile a quella della fisica classica.

Anche questa tecnica, come la precedente, non può essere utilizzata nel teletrasporto di stati classici o quantistici sconosciuti, ma solo di stati classici o quantistici noti.

Comunque sappiamo già che anche la tecnica di teletrasporto classico precedente può essere utilizzata per teletrasportare, tramite una quantità finita di bit, uno stato classico noto ed appartenente ad un insieme finito di stati classici.

Però la tecnica a variabili locali nascoste introduce un importante miglioramento rispetto alla tecnica precedente, in quanto essa permette di teletrasportare, con precisione infinita (e quindi senza distorsione), anche uno stato quantistico noto tramite una quantità finita di informazione, trasmessa sempre tramite un canale di comunicazione classica.

Bisogna invece ricordare che la tecnica precedente richiedeva una quantità infinita di informazione per poter teletrasportare uno stato quantistico senza distorsione, oppure che, utilizzando un numero finito di bit, essa avrebbe causato la distorsione dello stato quantistico stesso.

Questo miglioramento è dovuto al fatto che la tecnica a variabili locali nascoste, a differenza della precedente, si basa su una modalità di trasmissione dell'informazione, attuabile attraverso le LHV appunto, che non è realizzata attraverso la descrizione diretta, tramite l'informazione classica, delle costanti reali che definiscono lo stato quantistico.

Esiste infine la tecnica del teletrasporto quantistico, proposta da Bennett *et al.* nel 1993 e che, a differenza delle prime, utilizza un fenomeno noto con il nome di *entanglement*.

Alcuni autori, forse troppo prematuramente, affermano che l'entanglement è un fenomeno non riproducibile in maniera completamente classica.

Nel paragrafo 1.2 verrà comunque chiarificato, anche se brevemente, che questa affermazione, alla luce delle recenti scoperte, deve essere ridimensionata.

Ad ogni modo il fenomeno dell'entanglement permette di ottenere un ulteriore miglioramento nel campo del teletrasporto, in quanto permette di teletrasportare, a differenza delle due tecniche precedenti, anche stati classici o quantistici SCONOSCIUTI, questi ultimi pure quanto-meccanicamente indefiniti (che sono un caso estremo di stati sconosciuti: vedere a proposito il paragrafo 5.1), sempre con una quantità finita di informazione classica.

Inoltre il fenomeno dell'entanglement permette di teletrasportare, senza distorsione, uno stato quantistico noto con una quantità di informazione (trasmessa sempre attraverso un canale di comunicazione classico) minore rispetto a quella richiesta nel teletrasporto classico LHV.

Comunque, così come la tecnica di teletrasporto LHV, questa tecnica quantistica permette di teletrasportare anche uno stato quantistico per il fatto che anch'essa si basa su una modalità di trasmissione dell'informazione, attuabile grazie all'entanglement, che non è realizzata attraverso la descrizione diretta, tramite l'informazione classica, delle costanti reali che definiscono lo stato quantistico.

Siccome, da quanto affermato, quella quantistica costituisce la tecnica di teletrasporto migliore oggi nota, questo lavoro si dedicherà principalmente al suo studio, evitando di addentrarsi in una descrizione eccessivamente dettagliata della tecnica di teletrasporto a variabili locali nascoste.

## 1 Analisi del teletrasporto

Dopo aver descritto intuitivamente, nella precedente sezione, che cos'è il teletrasporto, procediamo ora con l'analizzarlo in modo rigoroso.

Verrà di seguito esposta prima di tutto la tecnica di teletrasporto di Bennett *et al.* [1], dato che, tra quelle enunciate, è la migliore.

In realtà questa tecnica è nata direttamente per teletrasportare stati quantistici sconosciuti, ma può comunque essere estesa anche al caso del teletrasporto di stati quantistici noti [3]: è per questo motivo che verrà analizzato per primo il caso degli stati sconosciuti.

Per dei valori particolari dei coefficienti della combinazione lineare che rappresenta lo stato quantistico da teletrasportare è possibile poi ottenere uno stato classico e quindi a questo caso non verrà dedicato un apposito paragrafo: semplicemente verrà considerato come un caso particolare di quello di stato quantistico. Infine verrà esposta la tecnica di teletrasporto classico a variabili locali nascoste, nel caso di stato quantistico noto. Anche in questo caso per dei valori particolari dei coefficienti della combinazione lineare che rappresenta lo stato quantistico è possibile ottenere uno stato classico e quindi anche a questo caso non verrà dedicato alcun paragrafo particolare.

## 1.1 Teletrasporto quantistico

La definizione di teletrasporto quantistico è la seguente:

*il teletrasporto quantistico è una tecnica per spostare tra due punti degli stati classici o quantistici, noti o sconosciuti, perfino in assenza di un canale di comunicazione quantistica che li colleghi, attraverso la loro condivisione di uno stato entangled e la trasmissione di un numero finito di bit attraverso un canale di comunicazione classica.*

### 1.1.1 Teletrasporto quantistico di uno stato sconosciuto

Viene ora proposto lo schema in termini di porte quantistiche [1][4] che permette di realizzare il teletrasporto quantistico, tra due osservatori convenzionalmente indicati come Alice (A) e Bob (B), del generico stato  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , dove i valori di  $\alpha$  e  $\beta$  sono supposti sconosciuti.

Più precisamente, lo stato  $|\psi\rangle$  viene teletrasportato da Alice a Bob, per la convenzione di lettura da sinistra a destra degli schemi a blocchi.

Si osserva che, qualora siano  $\alpha \neq 0$  e  $\beta \neq 0$ , si ottiene il teletrasporto di uno stato quantistico, mentre ponendo  $\alpha = 0$  oppure  $\beta = 0$  si ottiene automaticamente il teletrasporto di uno stato classico.

Vediamo ora lo schema a blocchi:

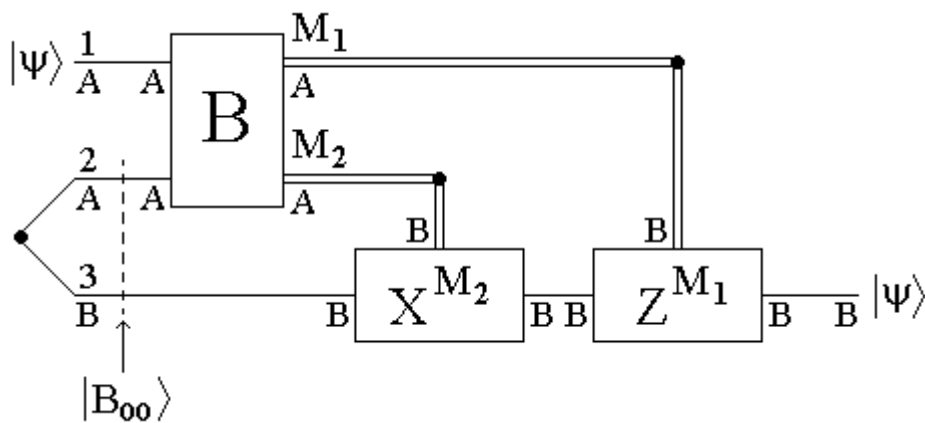


Figura 1.1

Questo schema viene suddiviso in parti alle quali vengono convenzionalmente attribuiti dei nomi.

La prima sezione della procedura del teletrasporto consiste nella preparazione dello stato di Bell  $|B_{00}\rangle$  (si rimanda al paragrafo 5.1 per la descrizione degli stati di Bell) e viene pertanto definita *preparazione di Bell*.

La seconda sezione è invece rappresentata dalla misurazione nella base di Bell e viene realizzata attraverso il blocco B, dove B sta per “Bell” e quindi non è da confondere con “Bob”.

Questo blocco permette cioè di misurare le componenti del suo stato d’ingresso lungo i quattro stati della base di Bell, anche se esso non fornisce in uscita gli stati di Bell quantistici veri e propri, bensì una coppia di stati classici, che permettono comunque di riconoscere lo stato di Bell che si è verificato.

Questa sezione viene pertanto definita *misurazione di Bell*.

La terza ed ultima sezione consiste invece nella trasformazione della parte dello stato entangled che appartiene a Bob, attraverso l'applicazione delle porte quantistiche X, iY o Z (si rimanda al paragrafo 5.3 per la loro descrizione). Per questo la terza sezione viene definita *trasformazione di Bell*.

Le linee 1 e 2 dello schema di figura 1.1 rappresentano rispettivamente lo stato  $|\psi\rangle$  da trasmettere, in possesso inizialmente di Alice, e la parte dello stato  $|B_{00}\rangle$  in possesso sempre di Alice.

La linea 3 rappresenta invece la parte rimanente dello stato  $|B_{00}\rangle$ , ovvero quella in possesso di Bob.

Si può ora osservare che, grazie alla proprietà di completezza della base di Bell  $\{|B_{00}\rangle; |B_{01}\rangle; |B_{10}\rangle; |B_{11}\rangle\}$ , e per il fatto che:

$$\begin{aligned} (\langle B_{00} | \otimes I_2)(|\psi\rangle |B_{00}\rangle) &= \frac{1}{2}(\alpha |0\rangle + \beta |1\rangle) = \frac{1}{2}|\psi\rangle \\ (\langle B_{01} | \otimes I_2)(|\psi\rangle |B_{00}\rangle) &= \frac{1}{2}(\beta |0\rangle + \alpha |1\rangle) = \frac{1}{2}X|\psi\rangle \\ (\langle B_{10} | \otimes I_2)(|\psi\rangle |B_{00}\rangle) &= \frac{1}{2}(\alpha |0\rangle - \beta |1\rangle) = \frac{1}{2}Z|\psi\rangle \\ (\langle B_{11} | \otimes I_2)(|\psi\rangle |B_{00}\rangle) &= \frac{1}{2}(-\beta |0\rangle + \alpha |1\rangle) = \frac{1}{2}(-iY)|\psi\rangle \end{aligned} \quad (1.1)$$

il complesso degli stati delle linee 1, 2 e 3 d'ingresso può essere scritto nel modo seguente:

$$\begin{aligned} |\psi\rangle |B_{00}\rangle &= (I_4 \otimes I_2)(|\psi\rangle |B_{00}\rangle) = \left[ \left( \sum_{x,y=0}^1 |B_{xy}\rangle \langle B_{xy}| \right) \otimes I_2 \right] (|\psi\rangle |B_{00}\rangle) = \frac{1}{2} [ |B_{00}\rangle |\psi\rangle + |B_{01}\rangle X|\psi\rangle + \\ &+ |B_{10}\rangle Z|\psi\rangle + |B_{11}\rangle (-iY)|\psi\rangle ] \end{aligned} \quad (1.2)$$

Abbiamo già detto che il blocco B, applicato da Alice, ha la capacità di misurare le componenti del suo ingresso rispetto agli stati di Bell, ma rappresentando gli stati di Bell in uscita tramite una coppia di stati classici. Pertanto il blocco B è esprimibile nel modo seguente:

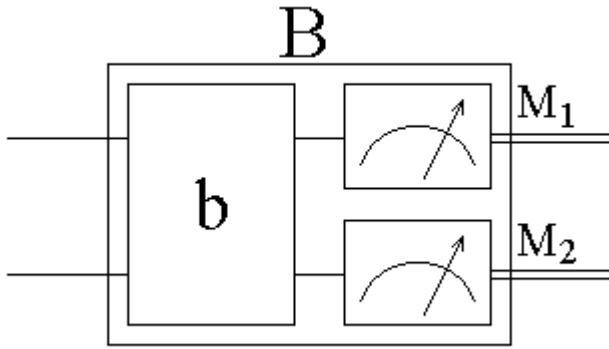


Figura 1.2

dove i blocchi dotati di freccia rappresentano dei blocchi di misurazione (descritti a loro volta da operatori di misurazione), mentre le linee doppie alle loro uscite rappresentano dei bit classici (in accordo con il postulato della misura, dove la misura è effettuata rispetto alla base computazionale).

Nello schema di figura 1.2, b è un operatore lineare, definito *operatore di Bell*, tale che:

$$b|B_{xy}\rangle = |xy\rangle \quad (1.3)$$

$$\forall x,y \in \{0;1\}.$$

Pertanto la rappresentazione matriciale di  $b$ , rispetto alla base  $\{|00\rangle;|01\rangle;|10\rangle;|11\rangle\}$  oppure rispetto alla base di Bell  $\{|B_{00}\rangle;|B_{01}\rangle;|B_{10}\rangle;|B_{11}\rangle\}$ , è la seguente:

$$b = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix} \quad (1.4)$$

Comunque questa rappresentazione matriciale non è invariante rispetto al generico cambiamento di base.

Come abbiamo già detto,  $b$  è un operatore lineare, mentre gli operatori di misurazione non lo sono.

Pertanto anche  $B$  complessivamente non è lineare.

Si osserva poi che mentre il blocco  $B$  agisce sulle linee 1 e 2, la linea 3 non subisce alcuna alterazione, il che è descritto dall'operatore identità  $I_2$ .

Ricordando poi l'espressione (1.2) per lo stato  $|\psi\rangle|B_{00}\rangle$ , si ottiene che:

$$(B \otimes I_2)(|\psi\rangle|B_{00}\rangle) = (B \otimes I_2) \left\{ \frac{1}{2} [ |B_{00}\rangle|\psi\rangle + \dots + |B_{11}\rangle(-iY)|\psi\rangle ] \right\} = \begin{cases} |00\rangle|\psi\rangle & \text{con } P=1/4 \\ |01\rangle X|\psi\rangle & \text{con } P=1/4 \\ |10\rangle Z|\psi\rangle & \text{con } P=1/4 \\ |11\rangle(-iY)|\psi\rangle & \text{con } P=1/4 \end{cases} \quad (1.5)$$

dove  $P$  rappresenta la probabilità che l'applicazione dell'operatore  $B \otimes I_2$  dia quel particolare risultato, tra i quattro possibili elencati.

Osservando che  $-iY = XZ$ , è possibile esprimere in modo compatto l'uscita dell'operatore  $B \otimes I_2$  nel modo seguente:

$$|M_1\rangle|M_2\rangle X^{M_2} Z^{M_1} |\psi\rangle \quad (1.6)$$

con  $P=1/4$ ,  $\forall M_1, M_2 \in \{0;1\}$ .

Essendo  $X$  e  $Z$  degli operatori unitari (vedere il paragrafo 5.3), si ha che  $XX^\dagger = I_2$  e  $ZZ^\dagger = I_2$ , ovvero che  $X^{-1} = X^\dagger = X$  e  $Z^{-1} = Z^\dagger = Z$ .

Pertanto ne segue anche che  $(XZ)^{-1} = Z^{-1}X^{-1} = ZX$ .

Quindi, in base a questi risultati, è possibile osservare che l'inverso dell'operatore  $X^{M_2}Z^{M_1}$ , comparso nell'espressione (1.6), è:

$$Z^{M_1} X^{M_2} \quad (1.7)$$

e quindi, applicandolo al terzo qubit (cioè quello che si trova sulla linea 3) della scrittura (1.5) dell'uscita di  $B \otimes I_2$ , si ottiene come risultato lo stato  $|\psi\rangle$ , indipendentemente dall'uscita dell'operatore  $B \otimes I_2$ .

Il primo ed il secondo qubit della scrittura (1.5) dell'uscita di  $B \otimes I_2$  funzionano invece come segnali (classici) di abilitazione delle porte  $X$  e  $Z$ , come mostrato nello schema a blocchi di figura 1.1..

Quindi, indipendentemente dall'uscita dell'operatore  $B \otimes I_2$ , che non può essere prevista in modo deterministico, Bob riesce a ricostruire lo stato  $|\psi\rangle$  che prima era in possesso di Alice.

Questo stato non è passato per tutti i punti dello spazio che separa Alice e Bob, poiché non è mai stato ipotizzato che tra di essi sia presente un canale di comunicazione quantistica che abbia permesso tal cosa a  $|\psi\rangle$ .

Ne segue quindi, in base alla definizione data nell'introduzione, che lo stato quantistico  $|\psi\rangle$  è stato teletrasportato.

E questo risultato è stato ottenuto utilizzando uno stato entangled ed una trasmissione di due stati classici, ovvero  $|M_1\rangle$  ed  $|M_2\rangle$ , cioè i segnali che abilitano le porte  $X$  e  $Z$ , attraverso un canale di comunicazione classica.



Gli stati  $|M_1\rangle$  ed  $|M_2\rangle$  quindi non sono altro che il risultato ottenuto dalla misura nella base di Bell effettuata da Alice, e che comunicati a Bob tramite un canale classico, gli dicono come trasformare lo stato in suo possesso al fine di ricostruire  $|\psi\rangle$ .

In modo intuitivo, è possibile affermare che nel teletrasporto si forma una doppia correlazione: la prima tra lo stato  $|\psi\rangle$  da teletrasportare e la parte di Alice dello stato  $|B_{00}\rangle$ , e la seconda tra le due parti dello stato  $|B_{00}\rangle$ .

E' questo fenomeno che permette di copiare lo stato  $|\psi\rangle$  da Alice a Bob.

Infatti la prima correlazione trasferisce l'informazione quantistica dello stato  $|\psi\rangle$  alla parte di Alice dello stato  $|B_{00}\rangle$ , mentre la seconda correlazione la trasferisce dalla parte di Alice alla parte di Bob dello stato  $|B_{00}\rangle$ , e quindi tale informazione quantistica giunge a Bob.

In realtà il termine "copiare" prima utilizzato non è corretto, a causa del teorema di non clonazione [4].

Questo teorema dimostra infatti in modo rigoroso che non è possibile che Alice disponga ancora dello stato  $|\psi\rangle$  a teletrasporto avvenuto.

Si può giungere alla stessa conclusione osservando che, durante la misura nella base di Bell, lo stato  $|\psi\rangle$  sulla linea 1 perde la sua identità poiché diventa entangled con la parte dello stato di Bell  $|B_{00}\rangle$  della linea 2.

Quindi lo stato  $|\psi\rangle$  posseduto da Alice è distrutto.

E' inoltre importante osservare che la misura nella base di Bell non rivela nessuna informazione sulle proprietà degli stati situati sulle linee 1 e 2.

Questo è il vero motivo per il quale il teletrasporto quantistico di un qubit riesce nel suo scopo, mentre il teletrasporto classico di un qubit sconosciuto fallisce.

In altri termini, la misura nella base di Bell non fornisce alcuna informazione sugli stati delle linee 1 e 2 e quindi non distrugge l'informazione quantistica in esse contenuta.

Cioè distruggere l'informazione quantistica vuol dire aver fatto scattare il postulato della misura, che impedisce, come già detto in precedenza, di conoscere con precisione le altre proprietà dello stato quantistico.

Ma siccome la misura nella base di Bell non distrugge questa informazione, lo stato quantistico  $|\psi\rangle$  può essere teletrasportato in modo che esso contenga ancora tutte le sue proprietà originali, e cioè con fedeltà (si rimanda al paragrafo 5.4 per la sua definizione) pari ad 1.

Nello schema a blocchi di figura 1.1 non è stato mostrato né come possa essere prodotto lo stato di Bell  $|B_{00}\rangle$  né come sia possibile creare l'operatore di Bell b.

Di seguito ne riportiamo due esempi, nei quali facciamo uso delle porte H e CNOT (si rimanda al paragrafo 5.3 per la descrizione di tali porte).

Per quanto riguarda la produzione dello stato  $|B_{00}\rangle$  si ha che:

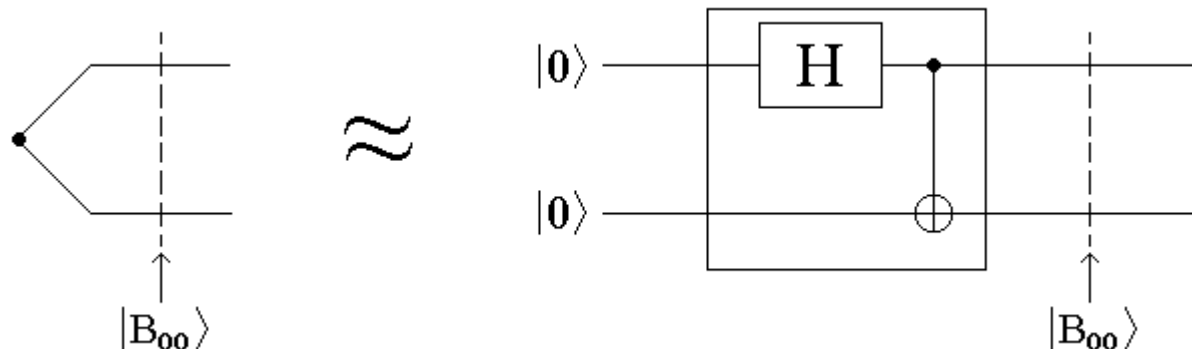


Figura 1.3

dove il simbolo  $\approx$  indica che i due blocchi sono equivalenti, cioè forniscono lo stesso risultato in uscita.

Infatti si può facilmente osservare che l'uscita del sistema di destra della figura 1.3 è:

$$\begin{aligned} |\psi_{OUT}\rangle &= CNOT(H|0\rangle;|0\rangle) = CNOT\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}};|0\rangle\right) = \frac{1}{\sqrt{2}}[CNOT(|0\rangle;|0\rangle) + CNOT(|1\rangle;|0\rangle)] = \\ &= \frac{|00\rangle+|11\rangle}{\sqrt{2}} = |B_{00}\rangle \end{aligned} \quad (1.8)$$

Per quanto riguarda invece la creazione dell'operatore b si ha che:

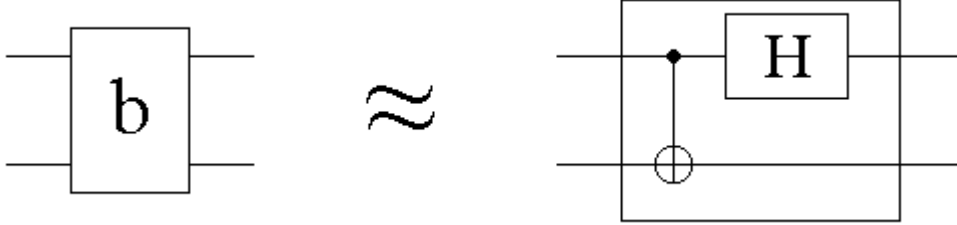


Figura 1.4

poiché si può dimostrare, con conti analoghi a quelli (1.8), che anche il sistema di destra della figura 1.4 soddisfa le relazioni (1.3).

Passiamo ora ad analizzare un'importante considerazione riguardante il teletrasporto quantistico, cioè la velocità di trasferimento dell'informazione che, per la teoria della relatività speciale (anche se non siamo nell'ambito della meccanica quantistica relativistica), non deve superare quella della luce.

Effettivamente questa legge è verificata nel teletrasporto quantistico.

Per dimostrarlo in modo intuitivo, basta osservare che Bob non è in grado di ricostruire lo stato  $|\psi\rangle$  finché non riceve da Alice la coppia di stati classici che gli riferiscono quale operatore utilizzare tra X, iY e Z.

Quindi parte dell'informazione necessaria per ricostruire  $|\psi\rangle$  è contenuta in questa coppia di bit, che però viaggia nel canale classico ad una velocità non superiore a quella della luce, e che quindi impedisce complessivamente un trasferimento superluminare dell'informazione.

E' possibile dimostrare anche in modo rigoroso questa affermazione [4], tramite l'operatore densità ed il calcolo della traccia parziale.

Ricordando le espressioni (1.1) riportate precedentemente (in termini delle costanti incognite  $\alpha$  e  $\beta$  che compaiono nella combinazione lineare che definisce lo stato  $|\psi\rangle$ ) e le relative probabilità dell'operatore B, si ottiene che l'operatore densità  $\rho$  del sistema composto di Alice e Bob è il seguente:

$$\begin{aligned} \rho &= \frac{1}{4} [ |00\rangle(\alpha|0\rangle + \beta|1\rangle)\langle 00|(\alpha^*\langle 0| + \beta^*\langle 1|) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)\langle 01|(\alpha^*\langle 1| + \beta^*\langle 0|) + \\ &+ |10\rangle(\alpha|0\rangle - \beta|1\rangle)\langle 10|(\alpha^*\langle 0| - \beta^*\langle 1|) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\langle 11|(\alpha^*\langle 1| - \beta^*\langle 0|) ] \end{aligned} \quad (1.9)$$

Ora basta determinare l'operatore densità ridotto  $\rho^B$ , calcolando la traccia parziale di  $\rho$  sul sottosistema di Alice:

$$\begin{aligned} \rho^B &= tr_A \rho = \frac{1}{4} [ (\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) + (\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|) + \\ &+ (\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) + (\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|) ] = \frac{1}{4} [ 2(|\alpha|^2 + |\beta|^2)|0\rangle\langle 0| + \\ &+ 2(|\alpha|^2 + |\beta|^2)|1\rangle\langle 1| ] = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I_2}{2} \end{aligned} \quad (1.10)$$

avendo utilizzato il fatto che  $tr(|00\rangle\langle 00|) = tr(|01\rangle\langle 01|) = tr(|10\rangle\langle 10|) = tr(|11\rangle\langle 11|) = 1$ , la condizione di normalizzazione  $|\alpha|^2 + |\beta|^2 = 1$  dello stato  $|\psi\rangle$  e la proprietà di completezza della base  $\{|0\rangle; |1\rangle\}$ .

Abbiamo quindi ottenuto che lo stato del sistema di Bob, dopo che Alice ha effettuato la misurazione nella base di Bell ma prima che Bob abbia acquisito il risultato di questa misura, è  $I_2/2$ , INDIPENDENTEMENTE dalla stato  $|\psi\rangle$  da teletrasportare.

Quindi lo stato del sistema di Bob in questa situazione è  $I_2/2$  per ogni stato  $|\psi\rangle$  e ne segue pertanto che  $I_2/2$  non ha alcuna dipendenza dallo stato  $|\psi\rangle$  stesso.

In tal modo ogni misurazione effettuata da Bob sullo stato del suo sistema non conterrà alcuna informazione su  $|\psi\rangle$ , il che impedisce la trasmissione dell'informazione, da Alice a Bob, ad una velocità maggiore di quella della luce.

### 1.1.2 Teletrasporto quantistico di uno stato noto

Viene ora proposto lo schema in termini di porte quantistiche che permette di realizzare il teletrasporto quantistico, tra Alice e Bob, dello stato quantistico generico  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , dove i valori di  $\alpha$  e  $\beta$  sono supposti noti [3].

Prima di mostrare questo sistema, bisogna osservare che, in base alla scrittura utilizzata nell'introduzione (vedere a proposito anche il paragrafo 5.1) per indicare un qubit, deve essere  $\alpha = \cos(\theta/2)$  e  $\beta = e^{i\phi}\sin(\theta/2)$ .

Di seguito viene però utilizzata contemporaneamente la scrittura con  $\alpha$  e  $\beta$  per comodità.

Vediamo ora lo schema a blocchi:

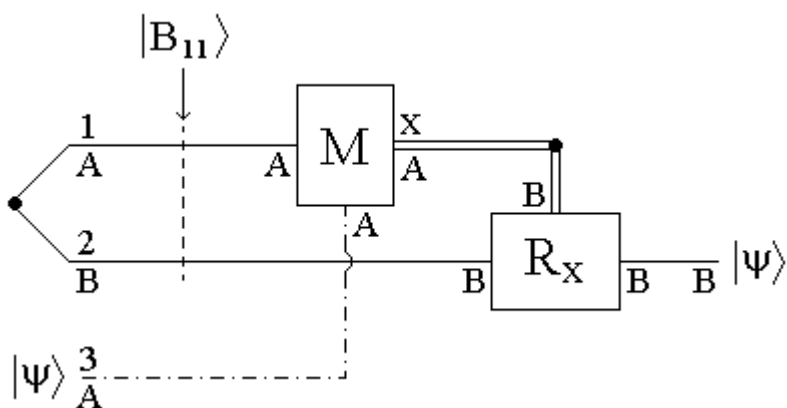


Figura 1.5

Le linee 1 e 2 dello schema rappresentano rispettivamente la parte di Alice e la parte di Bob dello stato entangled  $|B_{11}\rangle$  tra di essi condiviso (in questo protocollo, a differenza di quello del paragrafo precedente, viene utilizzato lo stato  $|B_{11}\rangle$  anziché lo stato  $|B_{00}\rangle$ , semplicemente per il fatto che questa scelta permette di formulare il procedimento di teletrasporto di uno stato noto in modo più elegante: comunque volendo poteva essere utilizzato uno qualsiasi degli stati di Bell).

La linea 3 rappresenta invece i valori noti delle costanti  $\alpha$  e  $\beta$  (oppure  $\theta$  e  $\phi$ ), in possesso di Alice e sconosciuti a Bob, e che vengono comunicati al blocco di misurazione M.

Per esempio la linea 3 potrebbe riportare un segnale analogico sinusoidale che tramite la sua ampiezza comunichi il valore di  $\theta$ , mentre tramite la sua frequenza il valore di  $\phi$ .

Per comprendere il protocollo di figura 1.5, consideriamo innanzitutto lo stato  $|\varphi\rangle = \chi|0\rangle + \delta|1\rangle$  tale che  $\{|\psi\rangle; |\varphi\rangle\}$  costituisca una base ortonormale dello spazio generato dalla coppia  $\{|0\rangle; |1\rangle\}$ , e che soddisfi la relazione di completezza.

Si dimostra allora che, posto  $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$ , deve essere  $|\varphi\rangle = -\sin(\theta/2)|0\rangle + e^{i\phi}\cos(\theta/2)|1\rangle$  (vedere il paragrafo 5.1).

Bisogna ricordare inoltre che lo stato  $|B_{11}\rangle$  è invariante sotto rotazione della base rispetto alla quale esso è rappresentato (vedere sempre il paragrafo 5.1), ovvero in particolare che:

$$|B_{11}\rangle = \frac{|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle}{\sqrt{2}} \quad (1.11)$$

Poniamo ora che il blocco M presenti la seguente struttura:

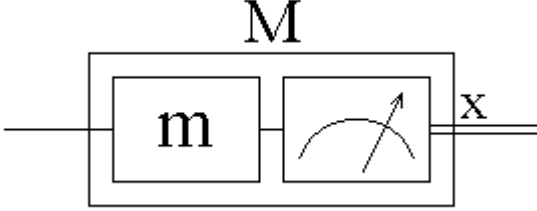


Figura 1.6

dove il blocco lineare  $m$  è definito nel seguente modo:

$$m = \begin{pmatrix} \text{sen}(\theta/2) & -e^{-i\phi} \cos(\theta/2) \\ \cos(\theta/2) & e^{-i\phi} \text{sen}(\theta/2) \end{pmatrix} \quad (1.12)$$

Questo vuol dire che la linea 3 ha comunicato al blocco  $m$  i valori, noti ad Alice, delle costanti  $\theta$  e  $\phi$ . In altri termini, la linea 3 ha comunicato al blocco  $m$  quale funzione logica esso debba avere.

Inoltre, per come abbiamo definito  $m$ , si ha che  $m|\phi\rangle = -|0\rangle$  e che  $m|\psi\rangle = |1\rangle$ .

In tal modo, ricordando inoltre l'espressione (1.11) dello stato  $|B_{11}\rangle$ , ne segue che:

$$(M \otimes I_2)|B_{11}\rangle = \begin{cases} |0\rangle|\psi\rangle, & \text{con } P = 1/2 \\ |1\rangle|\phi\rangle, & \text{con } P = 1/2 \end{cases} \quad (1.13)$$

Come si può osservare, l'uscita  $x$  del blocco  $M$  può essere solamente  $|0\rangle$  od  $|1\rangle$ , e seleziona pertanto rispettivamente, di volta in volta, dopo la trasmissione attraverso il canale classico, una delle due funzioni logiche  $R_0$  ed  $R_1$ , indicate in modo compatto come  $R_x$ , del blocco appartenente a Bob.

Poniamo ora  $R_0 \equiv I_2$ , in modo tale che:

$$R_0|\psi\rangle = I_2|\psi\rangle = |\psi\rangle \quad (1.14)$$

Poniamo invece  $R_1 \equiv C(iY)$ , dove  $C$  rappresenta il cosiddetto *operatore di coniugazione*, ovvero quell'operatore unitario che ad uno stato associa il suo complesso coniugato, in modo tale che:

$$\begin{aligned} R_1|\phi\rangle &= C(iY) \left[ -\text{sen}(\theta/2)|0\rangle + e^{i\phi} \cos(\theta/2)|1\rangle \right] = C \left[ e^{i\phi} \cos(\theta/2)|0\rangle + \text{sen}(\theta/2)|1\rangle \right] = \\ &= e^{-i\phi} \cos(\theta/2)|0\rangle + \text{sen}(\theta/2)|1\rangle = e^{-i\phi} \left[ \cos(\theta/2)|0\rangle + e^{i\phi} \text{sen}(\theta/2)|1\rangle \right] = |\psi\rangle \end{aligned} \quad (1.15)$$

Nell'ultimo passaggio è stato utilizzato il fatto che il fattore di fase  $e^{-i\phi}$  non è fisicamente osservabile.

In tal modo, indipendentemente dall'uscita dell'operatore  $M$ , si ottiene che lo stato ricostruito da Bob è  $|\psi\rangle$ .

Ovviamente a questo punto, pur avendo a disposizione lo stato  $|\psi\rangle$ , Bob non potrà determinare i valori di  $\theta$  e  $\phi$  tramite misurazione, a meno che egli non si faccia teletrasportare da Alice infiniti stati  $|\psi\rangle$  tutti uguali.

Quindi, nella realtà, non potendo trasmettere infiniti stati, anche dopo il teletrasporto lo stato  $|\psi\rangle$  non sarà noto a Bob, mentre ad Alice ovviamente sì.

## 1.2 Teletrasporto classico a variabili locali nascoste

La definizione di teletrasporto classico è la seguente:

*il teletrasporto classico è una tecnica per spostare tra due punti degli stati classici o quantistici noti, perfino in assenza di un canale di comunicazione quantistica che li colleghi, attraverso la loro condivisione di variabili locali nascoste e la trasmissione di un numero finito di bit attraverso un canale di comunicazione classica.*

Per effettuare il teletrasporto di uno stato quantistico noto tramite comunicazione di una quantità finita di informazione classica, non è indispensabile l'entanglement, dato che lo stesso risultato può essere ottenuto tramite la procedura del teletrasporto classico a variabili locali nascoste [3], che consiste appunto nel simulare interamente in modo classico la procedura del teletrasporto quantistico di un qubit noto.

In questa procedura, Alice è in possesso di uno stato quantistico arbitrario ma noto, che invece è sconosciuto a Bob. Se inoltre Alice e Bob condividono inizialmente delle variabili locali nascoste (LHV), cioè se essi possiedono un'identica (possibilmente infinita) lista di numeri casuali, si dimostra allora che effettuare il teletrasporto tramite queste variabili richiede solamente una quantità finita (e peraltro molto piccola) di informazione classica.

Questo protocollo di teletrasporto viene allora definito come classico, dato che le LHV sono delle grandezze associate a tale mondo, nel senso che storicamente sono state introdotte per cercare di riformulare la meccanica quantistica in un modo matematicamente equivalente ma tale da conferirle una struttura più simile a quella della fisica classica.

Effettuando invece il teletrasporto classico utilizzando un canale di comunicazione classica monolaterale, cioè unidirezionale, ma senza condividere delle variabili locali nascoste, richiede in contrasto la trasmissione di un numero infinito di bit (poiché Alice deve trasmettere a Bob la descrizione del suo stato, e cioè i valori degli angoli  $\theta$  e  $\phi$ ).

Nella procedura di teletrasporto LHV, l'obiettivo di Bob è quello di simulare le statistiche di ogni misurazione su un qubit noto ad Alice (ma ad esso sconosciuto), ovvero quello di generare una statistica di misurazione identica a quella prevista dalla meccanica quantistica, ma senza che Alice gli trasmetta effettivamente il proprio qubit, e comunque tutte le possibili misurazioni effettuate da Bob possono in realtà essere simulate da Alice trasmettendo pochi bit classici a Bob stesso, come se il qubit fosse stato effettivamente teletrasportato.

Qualora Bob utilizzi delle misurazioni proiettive [4], il miglior protocollo noto per realizzare il teletrasporto LHV di un qubit noto è basato sulla generalizzazione del cosiddetto *protocollo di Steiner* [5] ed è legato agli schemi di simulazione classica delle correlazioni di Bell recentemente scoperti da Brassard *et al.* [6].

Con questo protocollo una media di 2,19 bit di comunicazione classica monolaterale è sufficiente per completare la procedura.

Questi 2,19 bit rappresentano l'entropia di Shannon dell'informazione classica trasmessa, ovvero la media, calcolata su tutti i possibili stati quantistici che possono essere teletrasportati (e quindi su tutte le possibili combinazioni dei coefficienti complessi che compaiono nella sovrapposizione lineare dello stato quantistico stesso, incluse le combinazioni che trasformano lo stato quantistico in uno classico), della quantità d'informazione classica trasmessa. E' da osservare quindi che sono richiesti solamente 1,19 bit in più della quantità di informazione classica necessaria per effettuare il teletrasporto quantistico (cioè richiesta nel caso in cui Alice e Bob condividano tra loro una coppia entangled, anziché delle variabili locali nascoste) di un qubit noto.

Qualora invece Bob effettui una misurazione POVM [4], il miglior algoritmo conosciuto è meno efficiente di quello per la misurazione proiettiva ed utilizza mediamente un totale di 6,38 bit di comunicazione, per giunta questa volta bilaterale, cioè effettuata sia da Alice a Bob che da Bob ad Alice.

Comunque tramite l'uso esclusivo delle LHV non è possibile simulare tutti gli aspetti del teletrasporto quantistico di un qubit noto, come per esempio la non-località della coppia di Bell da quest'ultimo utilizzata.

E' infatti ben noto come ogni modello a variabili locali nascoste non possa riprodurre alcuna correlazione quantistica (e cioè la non-località), come riflesso dall'osservanza della disuguaglianza di Bell (infatti le LHV soddisfano tale disuguaglianza, cosa che invece non succede per l'entanglement).

Da sole quindi le LHV non sono in grado di riprodurre le correlazioni insite in tale fenomeno quantistico.

Steiner [5] e Brassard *et al.* [6] hanno però dimostrato che integrare un modello a variabili locali nascoste con una quantità molto piccola di comunicazione classica è sufficiente a simulare perfettamente le correlazioni quantistiche.

Cioè il modello del teletrasporto classico LHV permette di simulare classicamente anche le correlazioni quantistiche tipiche dell'entanglement.

Questi risultati dimostrano come i modelli a variabili locali nascoste siano piuttosto vicini alla meccanica quantistica: solo una piccola quantità di informazione classica (cioè 1,19 bit al massimo: infatti la procedura potrebbe non essere ottimale, il che porterebbe ad un divario addirittura inferiore) è sufficiente per riempire il divario tra di esse, almeno per sistemi aventi bassa dimensione.

Invece, al crescere della dimensione, la quantità di informazione richiesta aumenta esponenzialmente.

Questo potrebbe essere dovuto al fatto che il protocollo non sia ottimale.

Comunque esso è notevolmente efficiente, dato che se si limita a due il numero medio per simulazione dei bit comunicati, la fedeltà del teletrasporto (si rimanda al paragrafo 5.4 per la sua definizione) risulta essere pari a 0,957.

Invece, utilizzando solamente le variabili locali nascoste, e cioè utilizzando 0 bit di trasmissione classica, si ottiene una fedeltà pari a 0,5.

Un'importante conclusione circa la procedura di teletrasporto classico LHV riguarda l'interpretazione delle recenti realizzazioni sperimentali del teletrasporto.

Infatti bisogna essere cauti quando si afferma che questi esperimenti dimostrano che l'entanglement non possa essere simulato tramite soli mezzi classici, poiché la scoperta di Steiner [5] e Brassard *et al.* [6] ha effettivamente dimostrato il contrario.

## 2 Fonti di disturbo per il teletrasporto quantistico

Dall'analisi del teletrasporto quantistico effettuata nella sezione precedente, si è constatato come sia possibile teoricamente far giungere a Bob lo stesso stato  $|\psi\rangle$  posseduto da Alice.

In altri termini, è possibile teoricamente teletrasportare lo stato  $|\psi\rangle$  in modo perfetto, cioè con fedeltà (si rimanda al paragrafo 5.4 per la sua definizione) pari ad 1.

Purtroppo questo discorso è valido appunto solamente in modo teorico.

Infatti esistono tutta una serie di fenomeni che sono in grado di degradare lo stato  $|\psi\rangle$ , il che comporta un teletrasporto con fedeltà minore di 1.

Di seguito vengono analizzati questi fenomeni.

### 2.1 Imperfezioni delle porte quantistiche

Indipendentemente dalla tecnica utilizzata per realizzare le porte quantistiche (oscillatori armonici, fotoni e mezzi otticamente non lineari, risonanza magnetica nucleare, eccetera), esse saranno affette dal cosiddetto *rumore quantistico* (a volte chiamato *decoerenza*), costituito da una serie di processi incontrollabili che alterano l'evoluzione desiderata del sistema [4].

Il rumore quantistico rappresenta l'interazione, più o meno forte (dipende dalla tecnica con la quale è realizzato il sistema considerato, in questo caso una porta quantistica), del sistema con l'ambiente esterno o, più in generale, qualsiasi processo che causi una perdita di informazione quantistica nel sistema.

Per esempio, si potrebbe pensare di utilizzare come qubit le sovrapposizioni lineari degli stati corrispondenti a due livelli energetici di un atomo.

Le transizioni tra i due livelli possono essere stimulate da una radiazione elettromagnetica incidente, che potrebbe anche causare però, con una probabilità non nulla, delle transizioni ad altri livelli elettronici dell'atomo, diversi dai due considerati.

Questa è una forma di rumore quantistico possibile.

Per ovviare a questo problema non basta sviluppare delle tecniche costruttive caratterizzate da un basso accoppiamento con l'ambiente esterno, al fine di favorire la riduzione del rumore.

Infatti un sistema completamente isolato dall'ambiente esterno non può essere molto utile, in quanto il sistema deve poter ricevere dall'esterno le informazioni da elaborare e deve poter fornire all'esterno i risultati di tale elaborazione, cosa non possibile se esso fosse completamente isolato.

Si sono sviluppate allora delle tecniche differenti, basate sulla correzione degli errori causati dal rumore.

Queste tecniche si basano sull'uso di codici che proteggono l'informazione quantistica dal rumore.

Codificare un messaggio (classico o quantistico) significa aggiungervi dell'informazione ridondante (vedere al riguardo la definizione rigorosa di ridondanza riportata al paragrafo 5.2), cioè ripetuta (in tal modo quindi il messaggio codificato non conterrà l'informazione media per carattere massima possibile).

In tal modo, anche se parte del messaggio codificato è alterata dal rumore, esso contiene comunque abbastanza ridondanza da permettere di ricostruire completamente il messaggio originale (tramite un'operazione di decodifica). Questa discussione richiede comunque che le operazioni di codifica e di decodifica possano essere effettuate perfettamente, cioè senza errori, cosa in realtà non possibile.

Esiste però un importante risultato, definito *fault-tolerant quantum computation theory* (teoria della computazione quantistica tollerante verso gli errori), che permette di rimuovere l'assunzione di codifica e decodifica perfette. Comunque, a differenza della codifica e decodifica classiche, le versioni quantistiche presentano delle difficoltà da superare, rappresentate dall'impossibilità di clonare i qubit, dal fatto che gli errori quantistici sono continui e dal fatto che le misurazioni distruggono l'informazione quantistica.

In realtà nessuno di questi problemi è determinante e quindi è stato possibile sviluppare diversi tipi di codice per proteggere l'informazione quantistica dal rumore, e che utilizzati nelle porte quantistiche permettono di aumentarne l'affidabilità.

## 2.2 Errori nella trasmissione dell'informazione classica

Anche la trasmissione della coppia di bit, da parte di Alice, sul canale di trasmissione classico può essere affetta da rumore (classico).

Si utilizzano allora delle tecniche classiche di codifica e decodifica, per la protezione dell'informazione.

Le più note sono quelle che si basano sul controllo della parità, sulla protezione a ridondanza di blocco e sui codici ciclici [7].

Tutte queste tecniche sono state sviluppate per ottenere la massima efficienza di protezione dagli errori, utilizzando la minima ridondanza possibile.

## 2.3 Entanglement non massimale

Nello schema della figura 1.1 per il teletrasporto quantistico di uno stato sconosciuto è stato fatto uso di uno tra gli stati di Bell, che non sono gli unici stati entangled bi-ripartiti possibili.

La generalizzazione dello stato  $|B_{00}\rangle$  utilizzato in questo protocollo (e che comunque poteva essere impiegato anche nel teletrasporto di uno stato quantistico noto) assume la seguente forma [4][8][9]:

$$|\eta\rangle \equiv \cos\theta|00\rangle + \sin\theta|11\rangle \quad (2.1)$$

con  $\theta \in ]0; \pi[ \setminus \{\pi/2\}$  radianti, affinché lo stato sia ancora entangled.

Non si considerano i valori di  $\theta$  appartenenti all'intervallo  $[\pi; 2\pi[$  radianti dato che essi corrispondono agli stati  $|\eta\rangle$  che si ottengono per  $\theta$  appartenente all'intervallo  $[0; \pi[$  radianti, ma moltiplicati per il fattore di fase  $-1$ , e siccome un qualsiasi fattore di fase non è distinguibile in meccanica quantistica, ne segue che questi due intervalli di  $\theta$  contengono gli stessi stati e quindi il secondo intervallo può essere tralasciato.

Non si considerano nemmeno i valori  $\theta=0$  e  $\theta=\pi/2$  poiché per essi lo stato  $|\eta\rangle$  non è entangled, come verrà spiegato tra breve.

Come si può osservare, per  $\theta=\pi/4$  si ottiene lo stato  $|B_{00}\rangle$ , il che dimostra effettivamente come lo stato  $|\eta\rangle$  sia una generalizzazione dello stato  $|B_{00}\rangle$ , mentre per  $\theta=3\pi/4$  si ottiene lo stato  $|B_{10}\rangle$ .

E' possibile definire una grandezza nota con il nome di *entanglement*, solitamente indicata attraverso il simbolo  $E$ , che si misura in *ebit* (seguendo la terminologia di Schumacher) e che caratterizza ogni stato quantistico almeno doppio.

Ipotizzando che un qubit doppio sia condiviso da Alice e Bob, l'entanglement  $E$  di questo stato è definito (vedere più avanti per la giustificazione) come l'entropia di von Neumann di  $\rho^A$  o di  $\rho^B$  (è indifferente), dove  $\rho^A$  e  $\rho^B$  rappresentano gli operatori densità ridotti rispettivamente per la parte di Alice e per la parte di Bob del qubit doppio in questione.

Nel caso in cui Alice e Bob condividano lo stato  $|\eta\rangle$ , si ha che:

$$E = S(\rho_A) = S(\rho_B) = -tr(\rho_A \log_2 \rho_A) = -tr(\rho_B \log_2 \rho_B) = -\left[ (\cos^2 \theta) (\log_2 \cos^2 \theta) + (\sin^2 \theta) (\log_2 \sin^2 \theta) \right] \quad (2.2)$$

Si osserva quindi che per  $\theta=0$  e per  $\theta=\pi/2$  si ha  $E=0$  ebit.

Per  $\theta=0$  si ottiene infatti che  $|\eta\rangle=|00\rangle=|0\rangle|0\rangle$ , mentre per  $\theta=\pi/2$  si ottiene che  $|\eta\rangle=|11\rangle=|1\rangle|1\rangle$ .

In entrambe i casi si ottiene quindi che le due parti dello stato  $|\eta\rangle$  sono quanto-meccanicamente definite (cioè che lo stato  $|\eta\rangle$  è separabile) e pertanto lo stato non è entangled ( $E=0$  ebit appunto): per questo motivo sono stati precedentemente esclusi i valori  $\theta=0$  e  $\theta=\pi/2$  nella definizione (2.1) dello stato  $|\eta\rangle$ .

Lo stato  $|\eta\rangle$  viene classificato come *stato massimamente entangled* quando  $E=1$  ebit, ovvero quando  $\theta=\pi/4$  oppure  $\theta=3\pi/4$ , e cioè quando  $|\eta\rangle$  è uguale allo stato di Bell  $|B_{00}\rangle$  od a quello  $|B_{10}\rangle$ .

In modo analogo si dimostra che anche i due rimanenti stati di Bell  $|B_{01}\rangle$  e  $|B_{11}\rangle$  sono massimamente entangled.

Gli stati  $|\eta\rangle$ , per i valori di  $\theta$  rimanenti, possiedono  $E \in ]0;1[$  ebit e vengono pertanto definiti *stati parzialmente entangled*.

Dimostriamo ora che è proprio il fatto che lo stato  $|B_{00}\rangle$  sia massimamente entangled che permette, in caso di porte quantistiche e trasmissione classica perfette, di ottenere il teletrasporto quantistico di uno stato con fedeltà pari ad 1. Prendiamo in considerazione il teletrasporto quantistico di uno stato sconosciuto.

Ripetendo i conti effettuati nel paragrafo 1.1.1, ovvero nel caso di impiego di  $|B_{00}\rangle$ , ma utilizzando questa volta lo stato  $|\eta\rangle$ , si ottiene che lo stato  $|\psi_{OUT}\rangle$  ricostruito da Bob (dopo l'applicazione dell'operatore  $Z^{M_1}X^{M_2}$ ) non è sempre lo stesso per ognuno dei quattro valori dello stato  $|M_1\rangle|M_2\rangle$ .

Infatti, nel caso  $|M_1\rangle|M_2\rangle=|0\rangle|0\rangle$  oppure nel caso  $|M_1\rangle|M_2\rangle=|1\rangle|0\rangle$ , e quindi con una probabilità pari ad  $1/4+1/4=1/2$ , questo stato vale:

$$|\psi_{OUT1}\rangle = \frac{\alpha \cos \theta |0\rangle + \beta \sin \theta |1\rangle}{\sqrt{|\alpha|^2 \cos^2 \theta + |\beta|^2 \sin^2 \theta}} \quad (2.3)$$

mentre nel caso  $|M_1\rangle|M_2\rangle=|0\rangle|1\rangle$  oppure nel caso  $|M_1\rangle|M_2\rangle=|1\rangle|1\rangle$ , e quindi con una probabilità pari ad  $1/4+1/4=1/2$ , questo stato vale:

$$|\psi_{OUT2}\rangle = \frac{\alpha \sin \theta |0\rangle + \beta \cos \theta |1\rangle}{\sqrt{|\alpha|^2 \sin^2 \theta + |\beta|^2 \cos^2 \theta}} \quad (2.4)$$

Pertanto, lo stato ricostruito da Bob è uno stato misto, che possiede l'operatore densità  $\rho_{OUT}=(1/2)|\psi_{OUT1}\rangle\langle\psi_{OUT1}|+(1/2)|\psi_{OUT2}\rangle\langle\psi_{OUT2}|$ , rappresentato dalla seguente matrice:

$$\rho_{OUT} = \frac{1}{2(|\alpha|^2 \cos^2 \theta + |\beta|^2 \sin^2 \theta)} \begin{pmatrix} |\alpha|^2 \cos^2 \theta & \alpha\beta^* \cos \theta \sin \theta \\ \alpha^* \beta \cos \theta \sin \theta & |\beta|^2 \sin^2 \theta \end{pmatrix} + \frac{1}{2(|\alpha|^2 \sin^2 \theta + |\beta|^2 \cos^2 \theta)} \begin{pmatrix} |\alpha|^2 \sin^2 \theta & \alpha\beta^* \cos \theta \sin \theta \\ \alpha^* \beta \cos \theta \sin \theta & |\beta|^2 \cos^2 \theta \end{pmatrix} \quad (2.5)$$

Ricordando invece che lo stato  $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$  da teletrasportare di Alice è uno stato puro avente un operatore densità  $\rho_{IN}=|\psi\rangle\langle\psi|$ , si ottiene la seguente espressione della fedeltà (ricavabile attraverso la (5.21) del paragrafo 5.4) con la quale avviene il teletrasporto quantistico dello stato sconosciuto  $|\psi\rangle$ :



$$F(\rho_{IN}; \rho_{OUT}) = \sqrt{\frac{(|\alpha|^2 \cos \theta + |\beta|^2 \sin \theta)^2}{2(|\alpha|^2 \cos^2 \theta + |\beta|^2 \sin^2 \theta)} + \frac{(|\alpha|^2 \sin \theta + |\beta|^2 \cos \theta)^2}{2(|\alpha|^2 \sin^2 \theta + |\beta|^2 \cos^2 \theta)}} \quad (2.6)$$

con  $\theta \in ]0; \pi[ \setminus \{\pi/2\}$  radianti e  $|\beta|^2 = 1 - |\alpha|^2$ , con  $|\alpha| \in [0; 1]$ .

Si osserva ora che per  $\theta = \pi/4$ , ovvero per  $|\eta\rangle = |B_{00}\rangle$ , si ottiene  $F=1$ , come dovrebbe essere.

Questo risultato poteva anche essere dedotto immediatamente dal fatto che, dalla formula (2.5) di  $\rho_{OUT}$ , per  $\theta = \pi/4$  si ottiene che  $\rho_{OUT} = \rho_{IN}$ .

Invece, per  $\theta = 3\pi/4$ , ovvero per  $|\eta\rangle = |B_{10}\rangle$ , si ottiene  $F = |2|\alpha|^2 - 1| \in [0; 1]$ , e quindi sembrerebbe che  $E=1$  ebit non implichi necessariamente  $F=1$ : in realtà ciò è dovuto al fatto che gli stati  $|\psi_{OUT1}\rangle$  e  $|\psi_{OUT2}\rangle$  riportati precedentemente sono

stati calcolati utilizzando la procedura di teletrasporto progettata per lavorare sullo stato  $|B_{00}\rangle$  e non sullo stato  $|B_{10}\rangle$ .

In altri termini, sostituendo nel protocollo della figura 1.1 l'operatore  $Z^{M_1} X^{M_2}$  con l'operatore  $Z^{NOT(M_1)} X^{M_2}$  (dove con  $NOT(M_1)$  si intende la negazione dello stato  $|M_1\rangle$ ) e calcolando nuovamente la fedeltà, per  $|\eta\rangle = |B_{10}\rangle$  si otterrà

$F=1$ , mentre per  $|\eta\rangle = |B_{00}\rangle$  si otterrà  $F = |2|\alpha|^2 - 1|$ .

Tornando al caso della formula (2.6) della fedeltà, nei casi esclusi  $\theta=0$  e  $\theta=\pi/2$ , ovvero nei casi con  $E=0$  ebit, si ottiene  $F=1/\sqrt{2}$ .

Quindi  $E=0$  ebit non implica  $F=0$ .

Per comprendere questo risultato consideriamo l'esempio in cui si voglia effettuare il teletrasporto nel caso  $\theta=0$ .

In tal caso si ottiene che  $|\psi_{OUT1}\rangle = |0\rangle$ , mentre  $|\psi_{OUT2}\rangle = |1\rangle$ ,  $\forall \alpha, \beta$ .

Quindi, nell'ipotesi in cui sia  $|\psi\rangle = |0\rangle$  e nell'ipotesi in cui sia capitato che  $|M_1\rangle|M_2\rangle = |0\rangle|1\rangle$  oppure che  $|M_1\rangle|M_2\rangle = |1\rangle|1\rangle$

(ovvero uno dei due casi nei quali  $|\psi_{OUT}\rangle = |\psi_{OUT2}\rangle$ ), si ottiene che  $|\psi_{OUT}\rangle = |1\rangle \neq |0\rangle = |\psi\rangle$  e quindi che il teletrasporto ha causato una deformazione dello stato.

Si potrebbe quindi pensare che  $F=0$ , dato che in questi due casi si ottiene  $\langle \psi_{OUT} | \psi \rangle = 0$ , ma ciò nonostante si ha che

$F>0$ , dato che bisogna considerare anche il contributo ad  $F$  derivante dai casi in cui  $|M_1\rangle|M_2\rangle = |0\rangle|0\rangle$  ed

$|M_1\rangle|M_2\rangle = |1\rangle|0\rangle$ , ovvero dai casi in cui  $|\psi_{OUT}\rangle = |\psi_{OUT1}\rangle = |0\rangle = |\psi\rangle$ , e quindi nei quali il teletrasporto avviene senza deformazioni dello stato, il che alza il valore complessivo di  $F$  al di sopra dello zero.

Lo stesso ragionamento può essere esteso al caso di  $|\psi\rangle$  generico e poi ulteriormente al caso di  $\theta = \pi/2$ .

Comunque, dalla formula (2.5) di  $\rho_{OUT}$ , per  $\theta=0$  e  $\theta=\pi/2$  si ottiene che  $\rho_{OUT} = I_2/2$ , indipendentemente dallo stato  $|\psi\rangle$ , il che mostra come non esista alcun legame tra ingresso ed uscita nel caso in cui venga effettuato il teletrasporto con  $E=0$  ebit.

Ovviamente per il teletrasporto quantistico di uno stato noto si può calcolare la fedeltà in modo analogo.

Da queste formule si osserva che il teletrasporto quantistico di uno stato noto o sconosciuto può avvenire con fedeltà minore di uno qualora Alice e Bob condividano uno stato parzialmente entangled.

Ma quali sono le cause che portano i due interlocutori a condividere un tale stato, anziché per esempio lo stato  $|B_{00}\rangle$ ?

Se Alice e Bob non condividono inizialmente lo stato  $|B_{00}\rangle$  utilizzato nel teletrasporto, è necessario, per esempio, che Alice crei le due parti di  $|B_{00}\rangle$  e che trasmetta a Bob, attraverso un canale di comunicazione quantistica preesistente, la parte che gli spetta.

Se però il canale di comunicazione quantistica è rumoroso, ne segue che la parte di  $|B_{00}\rangle$  che arriva a Bob sarà alterata.

Ipotizziamo che l'azione del rumore sia descritta da un operatore  $\varepsilon$  il quale, applicato ad una parte dello stato  $|B_{00}\rangle$ , fornisca di volta in volta un risultato, appartenente ad un insieme finito di possibilità, che si manifestano ciascuna con una probabilità definita.

Più precisamente, supponiamo che  $(I \otimes \varepsilon)|B_{00}\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$  (dove  $\theta \in ]0; \pi[ \setminus \{\pi/2\}$  radianti, poiché consideriamo solamente gli stati con  $E > 0$  ebit, ed inoltre  $\theta$  è fissato, cioè se per più di una volta  $(I \otimes \varepsilon)|B_{00}\rangle$  è risultato essere uguale a  $\cos\theta|00\rangle + \sin\theta|11\rangle$ , allora in ciascuna di esse l'angolo  $\theta$  è uguale) con probabilità  $p > 0$ , mentre  $(I \otimes \varepsilon)|B_{00}\rangle = |\lambda_n\rangle$ , con probabilità  $p_n$ ,  $\forall n \in \{1; 2; \dots; m\}$ , dove  $m$  rappresenta un numero intero maggiore di zero. Ovviamente dovrà essere  $p + \sum_n p_n = 1$ .

Lo stato  $|\lambda_n\rangle$  è quasi completamente generico, ovvero rappresenta un qubit doppio qualsiasi,  $\forall n \in \{1; 2; \dots; m\}$ , diverso però dallo stato  $\cos\theta|00\rangle + \sin\theta|11\rangle$ .

In tal modo rientrano in questa situazione, come casi particolari, diversi esempi di canali quantistici, come il *depolarizing channel*, l'*amplitude damping channel*, il *phase damping channel* ed il *phase flip channel* [4].

Analizziamo in particolare l'evento  $(I \otimes \varepsilon)|B_{00}\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ .

In tal caso, e quindi con probabilità  $p$ , il canale sarà capace di ridurre il grado di entanglement rispetto a quello che si sarebbe raggiunto in caso di trasmissione quantistica perfetta.

Comunque è da segnalare il fatto che questo ipotetico canale quantistico complessivamente riduce il grado di entanglement della coppia  $|B_{00}\rangle$  con una probabilità appartenente all'intervallo  $[p; 1]$ .

Infatti anche gli stati  $|\lambda_n\rangle$  potrebbero essere degli stati parzialmente entangled, del tipo  $\cos\theta|01\rangle + \sin\theta|10\rangle$  oppure del tipo  $\cos\phi|00\rangle + \sin\phi|11\rangle$ , con  $\phi \neq \theta$ .

Come già dimostrato, la condivisione di uno stato parzialmente entangled non è conveniente ai fini del teletrasporto quantistico.

Esiste però una tecnica che permette di ovviare a questo problema.

Essa si basa sulla capacità di concentrare più stati parzialmente entangled in uno o più stati (comunque minori in numero rispetto agli stati di partenza) massimamente entangled.

In questo modo basterà che Alice trasmetta a Bob, tramite più canali di comunicazione quantistica, le parti che gli spettano di ciascuno dei vari stati entangled da lei preparati e che entrambi attuino la tecnica di concentrazione degli stati entangled.

Così Alice e Bob si troveranno a condividere degli stati entangled con  $E=1$  e quindi riusciranno ad effettuare un teletrasporto quantistico con  $F=1$ , per cui il problema iniziale è risolto.

Di seguito viene mostrato un esempio di questa procedura, realizzato tramite misurazioni proiettive [4], rappresentate dai blocchi MP, e tramite porte CNOT (si rimanda al paragrafo 5.3 per la descrizione di questa porta), ipotizzando che

Alice e Bob condividano inizialmente due stati parzialmente entangled del tipo  $|\eta\rangle$ :

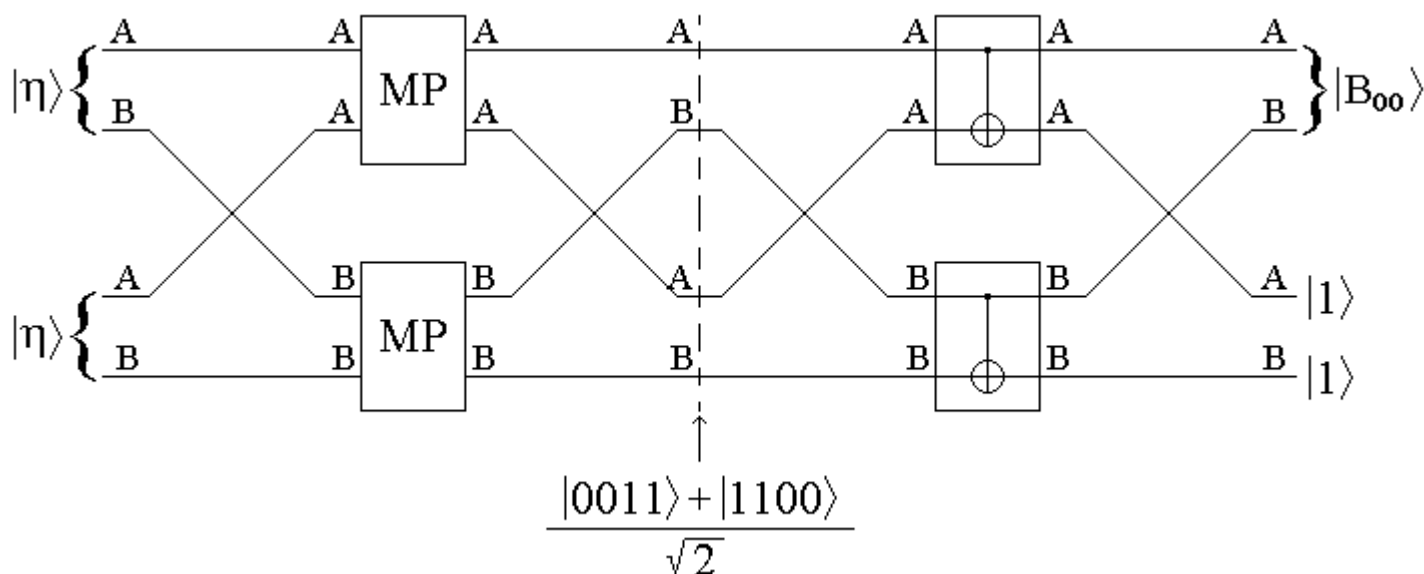


Figura 2.1

Vengono ora analizzate le varie sezioni di questo schema a blocchi.

Cominciamo con il riscrivere lo stato complessivo  $|\eta\rangle|\eta\rangle$  nel seguente modo:

$$|\eta\rangle|\eta\rangle = (\cos\theta|00\rangle + \sin\theta|11\rangle)(\cos\theta|00\rangle + \sin\theta|11\rangle) = \cos^2\theta|0000\rangle + \cos\theta\sin\theta(|0011\rangle + |1100\rangle) + \sin^2\theta|1111\rangle \quad (2.7)$$

I blocchi MP rappresentano l'operazione, effettuata sia da Alice che da Bob sulle rispettive parti dello stato  $|\eta\rangle|\eta\rangle$ , con le quali essi cercano di proiettare tale stato nel sottospazio avente base  $(|0011\rangle; |1100\rangle)$ .

In altri termini, con i blocchi MP Alice e Bob cercano di isolare la componente lungo gli stati  $|0011\rangle$  ed  $|1100\rangle$  dello stato  $|\eta\rangle|\eta\rangle$ , ovvero cercano di ottenere lo stato  $(|0011\rangle + |1100\rangle)/\sqrt{2}$ .

I blocchi MP rappresentano quindi, come già detto, delle misurazioni proiettive che Alice e Bob effettuano sulle rispettive parti dello stato  $|\eta\rangle|\eta\rangle$  e di conseguenza, in quanto misurazioni, non è garantito che il loro risultato sia effettivamente lo stato  $(|0011\rangle + |1100\rangle)/\sqrt{2}$ .

Infatti, con probabilità  $P=2\cos^2\theta\sin^2\theta$  tale misurazione dà come risultato lo stato desiderato  $(|0011\rangle + |1100\rangle)/\sqrt{2}$ , con  $P=\cos^2\theta$  lo stato  $|0000\rangle$  e con  $P=\sin^2\theta$  lo stato  $|1111\rangle$ .

Nell'ipotesi che la misurazione abbia dato come risultato lo stato  $(|0011\rangle + |1100\rangle)/\sqrt{2}$ , si osserva che le porte CNOT successive, applicate sia da Alice che da Bob sulle rispettive parti di tale stato, lo trasformano nel seguente modo:

$$(CNOT \otimes CNOT) \frac{|0011\rangle + |1100\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} |1\rangle|1\rangle = |B_{00}\rangle |1\rangle|1\rangle \quad (2.8)$$

Pertanto, con  $P=2\cos^2\theta\sin^2\theta = [\sin^2(2\theta)]/2 \leq 1/2$ , è possibile concentrare due stati parzialmente entangled in uno massimamente entangled, che risulterà condiviso tra Alice e Bob.

Di seguito viene quindi mostrata la procedura completa del teletrasporto quantistico, che illustra tutti i concetti discussi:

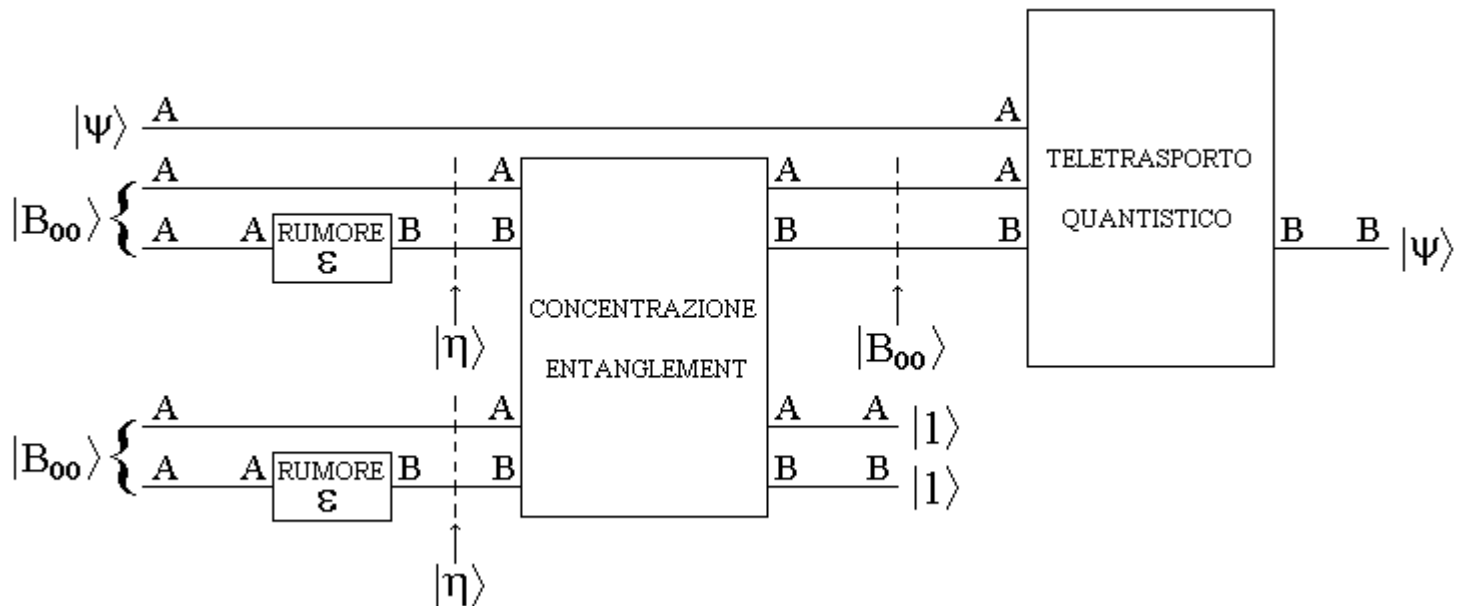


Figura 2.2

Si osserva che non esistono due operatori lineari  $L_A$  ed  $L_B$  tali che  $(L_A \otimes L_B)|\eta\rangle|\eta\rangle = (|0011\rangle + |1100\rangle)/\sqrt{2}$ , e quindi questo stato non è ottenibile attraverso l'uso esclusivo di porte quantistiche.

In altri termini, l'uso della misura proiettiva è necessario per ottenere lo stato  $(|0011\rangle + |1100\rangle)/\sqrt{2}$ , ma tale esito favorevole è incerto, in senso che la misura proiettiva comporta purtroppo la possibilità di ottenere, con una

probabilità non nulla, gli stati indesiderati  $|0000\rangle$  oppure  $|1111\rangle$ : è questo il prezzo da pagare se si vogliono concentrare i due stati parzialmente entangled.

Si osserva inoltre che la probabilità totale con la quale lo schema di figura 2.2 riesce ad effettuare un teletrasporto con  $F=1$  è ulteriormente ridotta dal fatto che il canale quantistico rumoroso presenta una probabilità non nulla di trasformare lo stato  $|B_{00}\rangle$  in uno stato non entangled, nel qual caso appunto la procedura di concentrazione di figura 2.1 è inutilizzabile: è sufficiente che almeno uno dei due canali fornisca in uscita uno stato non entangled affinché il protocollo fallisca.

Lo schema a blocchi di figura 2.1, essendo uno schema fisso, risulta inutilizzabile anche se i due stati condivisi da Alice e Bob dopo la trasmissione sono entrambi parzialmente entangled ma del tipo  $\cos\theta|00\rangle+\sin\theta|11\rangle$  e  $\cos\theta|01\rangle+\sin\theta|10\rangle$ , oppure del tipo  $\cos\theta|00\rangle+\sin\theta|11\rangle$  e  $\cos\varphi|00\rangle+\sin\varphi|11\rangle$ , con  $\varphi\neq\theta$ .

Invece, nel caso in cui  $p=1$ , si ha che la probabilità complessiva con la quale il teletrasporto quantistico avviene, tramite la procedura mostrata, con  $F=1$ , non viene ridotta dall'azione del canale quantistico.

Comunque in generale il canale quantistico riduce tale probabilità, dato che la procedura di concentrazione dell'entanglement è attuabile solamente nel caso in cui entrambe le uscite del canale diano come risultato lo stato  $\cos\theta|00\rangle+\sin\theta|11\rangle$ .

Siccome ciascuna di queste uscite avviene con probabilità  $p$  e siccome è necessario che esse si verifichino assieme, ne segue che il canale in generale altera la probabilità complessiva di avere  $F=1$  di un coefficiente moltiplicativo  $p^2$ , nell'ipotesi in cui i due canali quantistici siano indipendenti.

Quindi la probabilità complessiva di avere  $F=1$  è  $p^2[\sin^2(2\theta)]/2$ .

In realtà avremmo dovuto sommare anche il contributo di probabilità derivante dalla possibilità che entrambe le linee del canale forniscano lo stato  $\cos\varphi|00\rangle+\sin\varphi|11\rangle$ , con  $\varphi\neq\theta$ , ma questa situazione può verificarsi o meno a seconda del tipo di canale considerato.

Si osserva inoltre che condizione necessaria e sufficiente affinché il canale sia perfetto qualora venga trasmesso lo stato  $|B_{00}\rangle$ , è quella di avere  $p=1$  e  $\theta=\pi/4$ .

In tal caso non avrebbe alcun senso utilizzare la procedura di concentrazione dell'entanglement dato che gli stati condivisi da Alice e Bob sono sempre quelli  $|B_{00}\rangle$ , e quindi la probabilità di avere  $F=1$  è ovviamente unitaria.

Invece, nel caso in cui sia  $p<1$  con  $\theta\neq\pi/4$  e  $|\lambda_n\rangle=|B_{00}\rangle \forall n$ , ne segue che non è possibile sapere quando il canale lascia inalterata la parte dello stato  $|B_{00}\rangle$  in esso trasmessa e quindi in questo caso la procedura di concentrazione dell'entanglement deve essere utilizzata.

Comunque, in conclusione, qualora Alice e Bob condividano due stati parzialmente entangled, affinché si riesca, con una probabilità prossima ad 1, ad effettuare il teletrasporto quantistico con  $F=1$ , è necessario che Alice crei lo stato  $|B_{00}\rangle$  e che il canale quantistico rumoroso sia realizzato in modo tale che  $p$  sia prossimo ad 1.

E' poi possibile generalizzare la procedura di concentrazione dell'entanglement appena mostrata.

Esiste infatti un protocollo che permette di concentrare  $n$  stati parzialmente entangled del tipo  $|\eta\rangle$  in  $m<n$  stati massimamente entangled, con una probabilità di fallimento che può essere resa piccola a piacere aumentando il valore di  $n$ .

Si può dimostrare che questo protocollo è asintoticamente efficiente, nel senso che, per  $n$  grande, il numero di qubit singoli massimamente entangled a cui esso dà origine va come  $m=nS(\rho)-O(\log_2 n)$ , dove  $S(\rho)$  rappresenta l'entropia di von Neumann di  $\rho=\rho_A=\rho_B$ , ovvero dei due operatori densità ridotti rispettivamente della parte appartenente ad Alice e della parte appartenente a Bob dello stato  $|\eta\rangle$ .

Definendo l'*entanglement distillabile* come il limite del rapporto  $m/n$ , per  $m$  ed  $n$  tendenti entrambe a  $+\infty$ , ovvero come la quantità di correlazione che può essere estratta dallo stato  $|\eta\rangle$ , si osserva che:

$$\lim_{(m;n)\rightarrow(+\infty;+\infty)} \frac{m}{n} = \lim_{n\rightarrow+\infty} \frac{nS(\rho) - O(\log_2 n)}{n} = S(\rho) = E_{|\eta\rangle} \quad (2.9)$$

La (2.9) rappresenta la giustificazione della formula precedentemente utilizzata per definire l'entanglement  $E$ .

### 3 Realizzazione sperimentale del teletrasporto quantistico

Sebbene si sia verificato un veloce progresso nella descrizione teorica dell'elaborazione dell'informazione quantistica, le difficoltà nel maneggiare i sistemi quantistici non hanno permesso un uguale sviluppo nella realizzazione sperimentale delle nuove proposte.

Questo lento progresso sperimentale è espresso dal fatto che, fino a poco tempo fa, la principale tecnica per ottenere degli stati entangled era quella ottica, ovvero quella che produce tali stati correlando coppie di fotoni e nella quale la proprietà teletrasportata è rappresentata dalla polarizzazione dei fotoni [2].

Questa tecnica però è affetta dal problema di non riuscire sempre a proiettare la coppia di fotoni entangled in uno qualsiasi degli stati di Bell (infatti, più precisamente, essa è in grado di proiettare la coppia di fotoni in almeno due degli stati di Bell).

Si è quindi passati a sviluppare delle tecniche alternative, che ovviassero a questo inconveniente.

Solo molto recentemente è stata realizzata una di queste tecniche, che fa uso di atomi [10], come particelle da correlare tramite l'entanglement.

Inoltre è da segnalare la possibilità [10] di creare stati entangled condivisi da più particelle contemporaneamente (i cosiddetti *stati entangled multi-ripartiti*: vedere il paragrafo 5.1), possibilità non disponibile in passato lavorando con i fotoni, i quali infatti possono trovarsi in stati entangled solamente in coppia (nei cosiddetti *stati entangled bi-ripartiti*).

La PRIMA verifica sperimentale a livello storico del teletrasporto quantistico è stata realizzata attraverso la tecnica ottica.

Di conseguenza, prima di analizzare nel dettaglio questa tecnica, è necessario ricordare che, interpretando un fotone come particella, esso possiede uno spin che può esistere solamente in due stati differenti, mentre interpretandolo come onda, esso possiede due stati di polarizzazione, che sono correlati ai due stati di spin della precedente interpretazione.

Un singolo fotone può per esempio essere polarizzato orizzontalmente o verticalmente, il che è indicato dagli stati  $|\leftrightarrow\rangle$  oppure  $|\updownarrow\rangle$ : questi sono due esempi di polarizzazione lineare.

Un fotone può perfino essere polarizzato nella generica sovrapposizione  $|\psi\rangle = \alpha|\leftrightarrow\rangle + \beta|\updownarrow\rangle$  di questi due stati.

Gli stati  $|\leftrightarrow\rangle$  e  $|\updownarrow\rangle$ , in un discorso più generale, sono sostituiti dagli stati computazionali  $|0\rangle$  ed  $|1\rangle$ .

Possiamo ora passare all'analisi dell'esperimento vero e proprio, il cui schema viene mostrato di seguito [2]:

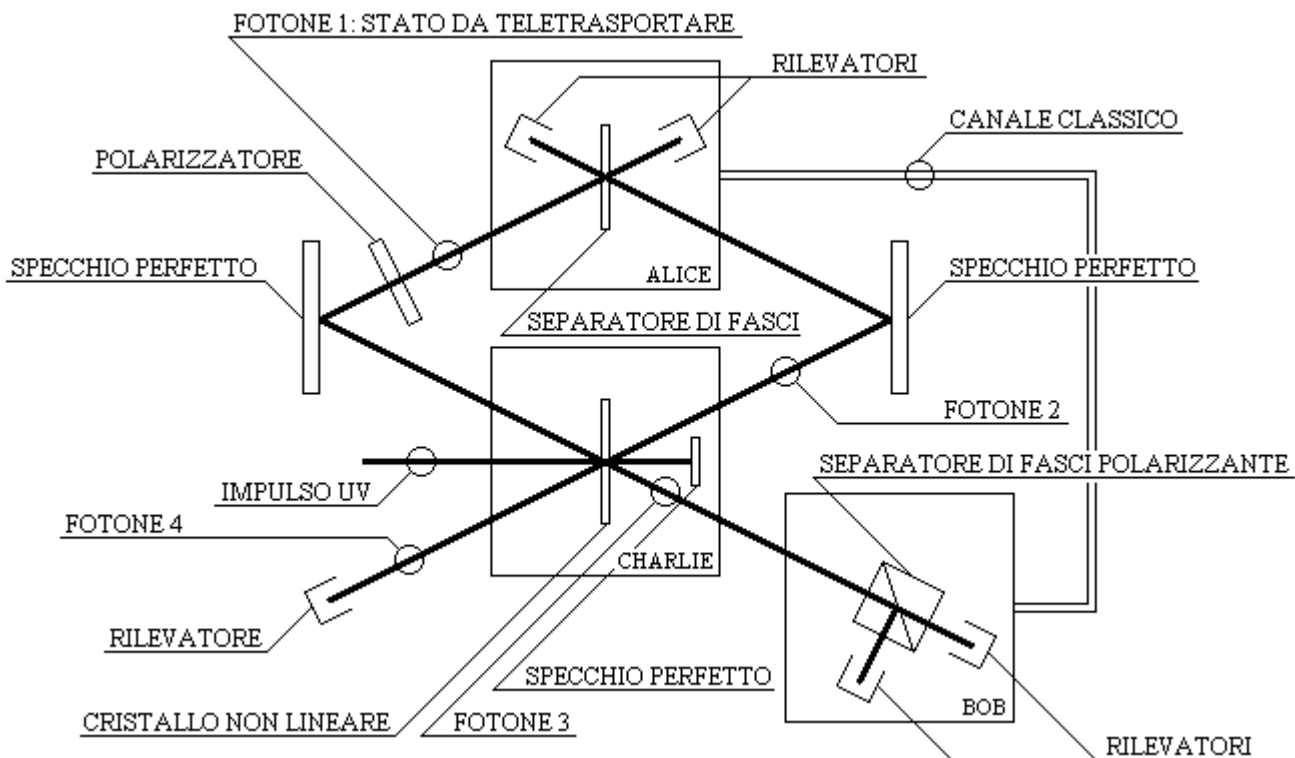


Figura 3

Nel blocco “Charlie” viene prodotta una coppia di fotoni entangled, attraverso il processo della cosiddetta *parametric down-conversion di tipo II*.

Questo processo consiste nel bersagliare un cristallo non lineare con un impulso ultravioletto, il quale può creare una coppia di fotoni, più precisamente i fotoni 2 e 3, durante questo passaggio.

Qualora questi due fotoni vengano creati, le loro polarizzazioni si troveranno nello stato di Bell  $|B_{11}\rangle$  ed il fotone 2 verrà inviato verso Alice, mentre il fotone 3 verso Bob.

Lo stato entangled che si è così formato tra questi due fotoni ricopre il ruolo dello stato  $|B_{00}\rangle$  analizzato nel paragrafo 1.1.1, ovvero dello stato entangled condiviso tra Alice e Bob e che rende possibile il teletrasporto quantistico.

Anche se l’impulso UV è riuscito a creare i fotoni 2 e 3, esso non viene assorbito completamente dal cristallo e quindi ne uscirà dalla parte opposta.

Qui l’impulso troverà uno specchio, in grado di rifletterlo, in modo da fargli attraversare nuovamente il cristallo.

In questo secondo passaggio, l’impulso potrà creare ancora una coppia di fotoni, che nella figura 3 sono stati indicati come fotoni 1 e 4.

In realtà, allo stesso modo dei fotoni 2 e 3, anche i fotoni 1 e 4 saranno entangled tra loro, ma ciò non importa, dato che la cosa veramente utile è che l’entanglement esista tra i fotoni 2 e 3.

E’ possibile infine sapere se l’impulso UV ha avuto successo nel creare la seconda coppia, semplicemente grazie ad una eventuale segnalazione derivante dal rilevatore del fotone 4.

Prima di giungere al blocco “Alice”, il fotone 1 viene polarizzato secondo una direzione di oscillazione prestabilita.

In tal modo è possibile affermare che il fotone 1, quando entrerà nel blocco “Alice”, avrà una polarizzazione coincidente con quella imposta dal polarizzatore.

Questa polarizzazione è nota allo sperimentatore che l’ha regolata, ma non è nota ad Alice.

Pertanto non stiamo analizzando il caso del teletrasporto quantistico di uno stato noto, che è già stato discusso nel paragrafo 1.1.2, dal punto di vista teorico.

In altri termini, in questo apparato sperimentale, il polarizzatore non ha alcun modo di comunicare al blocco “Alice” quale sia la sua polarizzazione.

In tal modo il blocco “Alice” non potrà effettuare la misura proiettiva rispetto alla base formata dallo stato del polarizzatore e dallo stato ad esso ortogonale, semplicemente poiché questo blocco ignora quale sia lo stato del polarizzatore.

Stiamo quindi trattando il caso del teletrasporto quantistico di uno stato sconosciuto.

Il blocco “Alice” cerca invece di rappresentare quello che nel paragrafo 1.1.1 era stato indicato come il blocco della misurazione nella base di Bell, riuscendovi in parte, in quanto in realtà il blocco “Alice” riesce ad effettuare solamente una misurazione incompleta nella base di Bell.

Infatti, del blocco di misurazione nella base di Bell esso rappresenta solamente la parte di proiezione rispetto allo stato  $|B_{11}\rangle$ .

Questa affermazione è giustificata dal fatto che il blocco “Alice” dello schema di figura 3 riesce ad effettuare il teletrasporto dello stato del fotone 1 solamente nel caso in cui la misura (incompleta) nella base di Bell da esso

effettuata dia come risultato lo stato  $|B_{11}\rangle$ , cioè solamente nel caso in cui, dopo tale misura, i fotoni 1 e 2 si trovino nello stato  $|B_{11}\rangle$ .

Infatti, in tale situazione, a causa della condivisione tra i fotoni 1 e 2 dello stato  $|B_{11}\rangle$ , il fotone 1 sarà anti-correlato (vedere il paragrafo 5.1) al fotone 2, che a sua volta è anti-correlato al fotone 3.

Ne segue quindi, per la doppia negazione, che gli stati dei fotoni 1 e 3 devono essere uguali, e quindi che il teletrasporto è in tal caso avvenuto.

La differenza tra il blocco della misurazione nella base di Bell ed il blocco “Alice” è quindi rappresentato dal fatto che il primo riesce ad effettuare la proiezione rispetto a qualsiasi stato di Bell e quindi riesce ad effettuare il teletrasporto

in ogni caso, mentre il secondo riesce ad effettuare la proiezione solamente rispetto allo stato  $|B_{11}\rangle$  e quindi riesce ad effettuare il teletrasporto solamente nel caso in cui capiti tale stato.

In altri termini, il blocco della misurazione nella base di Bell riesce a teletrasportare sicuramente lo stato, cioè con probabilità pari ad 1, mentre il blocco “Alice” solamente con probabilità pari ad 1/4.

Quest’ultima affermazione è conseguenza del fatto che il blocco “Alice” riesce a creare lo stato  $|B_{11}\rangle$  tramite un separatore di fasci, ovvero tramite uno specchio mezzo argentato, in grado di riflettere o di trasmettere un fotone incidente con la stessa probabilità, pari ad 1/2.

Lo specchio utilizzato dal blocco “Alice” è mezzo argentato su entrambe i lati e quindi, dato che esso viene colpito dai fotoni 1 e 2, ne segue che possono verificarsi quattro casi differenti, aventi tutti probabilità pari ad 1/4: il fotone 1

riflesso ed il fotone 2 trasmesso, il fotone 1 trasmesso ed il fotone 2 riflesso, entrambe i fotoni riflessi ed infine entrambe i fotoni trasmessi.

Si può notare come sia impossibile, per i rilevatori posti dopo lo specchio mezzo argentato, distinguere tra loro gli ultimi due casi indicati, dato che in entrambi i rilevatori segnalano la presenza di un fotone ciascuno (invece i primi due casi sono distinguibili tra di loro, per il fatto che essi sono caratterizzati dalla doppia segnalazione di un solo rilevatore e quindi, per distinguere tra le due situazioni, basta vedere quale tra i due rilevatori ha segnalato i due fotoni).

Siccome il fotone 1 riflesso risulta indistinguibile dal fotone 2 trasmesso, mentre il fotone 1 trasmesso risulta indistinguibile dal fotone 2 riflesso, ne segue che negli ultimi due casi non è possibile stabilire quale rilevatore ha segnalato il fotone 1 e quale ha segnalato il fotone 2 (nei primi due casi invece il rilevatore che scatta avrà segnalato la presenza di entrambi i fotoni).

E' proprio questa indistinguibilità che causa la formazione dello stato  $|B_{11}\rangle$  tra i fotoni 1 e 2.

Infatti, qualora entrambi i rilevatori segnalino la presenza di un fotone, vorrà dire che i fotoni 1 e 2 si troveranno nello stato quantistico formato dalla combinazione lineare dello stato classico "fotoni 1 e 2 entrambi riflessi" con lo stato classico "fotoni 1 e 2 entrambi trasmessi".

In realtà è importante specificare che, ai fini di questa indistinguibilità, i due fotoni devono raggiungere contemporaneamente lo specchio mezzo argentato, poiché altrimenti sarebbe possibile distinguerli attraverso il loro tempo di arrivo nei due rilevatori posti nel blocco.

Comunque questi rilevatori servono per stabilire se lo stato  $|B_{11}\rangle$  si è formato oppure no tra i fotoni 1 e 2.

Infatti, se entrambi rilevano un fotone, vuol dire che lo stato  $|B_{11}\rangle$  si è formato, mentre se solo uno di essi rileva ben due fotoni, vuol dire che la procedura non ha avuto successo.

Sembrerebbe quindi che lo stato  $|B_{11}\rangle$  si possa formare con probabilità  $P=1/2$  e non con  $P=1/4$  come affermato in precedenza, dato che i casi con entrambe i fotoni riflessi od entrambi trasmessi hanno ciascuno probabilità  $1/4$  e quindi la probabilità che si verifichi uno o l'altro caso è pari ad  $1/4+1/4=1/2$ .

In realtà però si ha che  $P=1/4$ , poiché il caso complessivo nel quale entrambi i fotoni vengono riflessi od entrambi trasmessi, caso che si verifica con probabilità  $1/2$  per quanto appena detto, si suddivide a sua volta in due sotto-casi,

che si manifestano con la stessa probabilità, ma in uno solo dei quali si verifica la formazione dello stato  $|B_{11}\rangle$  tra i fotoni 1 e 2, da cui allora  $P=1/4$ , come detto.

Nel primo sotto-caso si forma, per quanto riguarda le ampiezze di probabilità dello stato quantistico, interferenza distruttiva tra l'ampiezza dei due fotoni riflessi e quella dei due fotoni trasmessi, in modo tale che entrambi i rilevatori non segnalino la presenza di alcun fotone: in questo caso lo stato  $|B_{11}\rangle$  non si forma.

Nel secondo sotto-caso tra le ampiezze di probabilità si forma invece interferenza costruttiva, in modo tale che

entrambi i rilevatori segnalino la presenza di un fotone: è questa la situazione nella quale si forma lo stato  $|B_{11}\rangle$  tra i fotoni 1 e 2.

Le due situazioni di interferenza distruttiva e costruttiva si manifestano a causa del fatto che lo stato del fotone 2 è quanto-meccanicamente indefinito, poiché si trova nello stato  $|B_{11}\rangle$  che esso condivide col fotone 3, ed al fatto che lo specchio mezzo argentato sfasa di  $\pi$  radianti i fotoni da esso riflessi.

Per dimostrare quanto appena affermato bisogna ricavare lo stato complessivo  $|\mu\rangle$  dei fotoni 1, 2 e 3 dopo che i fotoni 1 e 2 hanno interagito con lo specchio mezzo argentato.

Per ricavare  $|\mu\rangle$ , si comincia con il ricordare che il fotone 1 può essere riflesso o trasmesso con pari probabilità, quindi:

$$|\mu\rangle = \frac{|1R\rangle|2;3\rangle + |1T\rangle|2;3\rangle}{\sqrt{2}} \quad (3.1)$$

La scrittura  $|2;3\rangle$  indica lo stato assunto dai fotoni 2 e 3.

Ricordando che anche il fotone 2 può essere riflesso o trasmesso con uguale probabilità dallo specchio mezzo argentato, si ottiene che:

$$|2;3\rangle = \frac{|2R;3\rangle + |2T;3\rangle}{\sqrt{2}} \quad (3.2)$$

Bisogna ora ricordare che i fotoni 2 e 3 si trovano nello stato  $|B_{11}\rangle$  anche dopo l'interazione del fotone 2 con lo specchio mezzo argentato e che tale stato è invariante rispetto ai cambiamenti di base (vedere il paragrafo 5.1), ovvero in particolare che:

$$|B_{11}\rangle = \frac{|\leftrightarrow\rangle|\uparrow\rangle - |\uparrow\rangle|\leftrightarrow\rangle}{\sqrt{2}} = \frac{|\psi\rangle|\varphi\rangle - |\varphi\rangle|\psi\rangle}{\sqrt{2}} \quad (3.3)$$

dove  $|\psi\rangle$  rappresenta lo stato da teletrasportare, ovvero lo stato del fotone 1 dopo che questo è uscito dal polarizzatore (vedere la figura 3), mentre  $|\varphi\rangle$  rappresenta lo stato tale che la coppia  $\{|\psi\rangle;|\varphi\rangle\}$  costituisca una base che goda della relazione di completezza. Quindi deve essere che:

$$|2R;3\rangle = \frac{|2R\psi\rangle|3\varphi\rangle - |2R\varphi\rangle|3\psi\rangle}{\sqrt{2}} \quad |2T;3\rangle = \frac{|2T\psi\rangle|3\varphi\rangle - |2T\varphi\rangle|3\psi\rangle}{\sqrt{2}} \quad (3.4)$$

dove per esempio la scrittura  $|2R\psi\rangle$  sta ad indicare che il fotone 2 è riflesso e si trova nello stato  $|\psi\rangle$ .

Inserendo tutti questi risultati nella formula (3.1) dello stato  $|\mu\rangle$  e raccogliendo i termini formati, si ottiene infine che:

$$\begin{aligned} |\mu\rangle = & \frac{1}{2\sqrt{2}} (|1R\psi\rangle|2T\psi\rangle|3\varphi\rangle - |1R\psi\rangle|2T\varphi\rangle|3\psi\rangle) + \frac{1}{2\sqrt{2}} (|1T\psi\rangle|2R\psi\rangle|3\varphi\rangle - |1T\psi\rangle|2R\varphi\rangle|3\psi\rangle) + \\ & + \frac{1}{2\sqrt{2}} (|1R\psi\rangle|2R\psi\rangle|3\varphi\rangle + |1T\psi\rangle|2T\psi\rangle|3\varphi\rangle) - \frac{1}{2\sqrt{2}} (|1R\psi\rangle|2R\varphi\rangle|3\psi\rangle + |1T\psi\rangle|2T\varphi\rangle|3\psi\rangle) \end{aligned} \quad (3.5)$$

Questa formula evidenzia come  $|\mu\rangle$  sia costituito da quattro stati (quelli raccolti nelle parentesi tonde), ognuno dei quali può essere distinto dai rilevatori posti dopo lo specchio mezzo argentato.

Il primo di questi quattro stati rappresenta la situazione nella quale il fotone 1 è riflesso ed il fotone 2 è trasmesso.

Come si può osservare, questo stato non presenta traccia di entanglement tra i fotoni 1 e 2, dato che in questo caso lo stato del fotone 1 può essere raccolto e quindi separato, ovvero reso indipendente e quindi scorrelato, dallo stato dei fotoni 2 e 3 e quindi in particolare dallo stato del fotone 2.

Il secondo dei quattro stati rappresenta invece la situazione nella quale il fotone 1 è trasmesso ed il fotone 2 è riflesso: anche in questo caso i fotoni 1 e 2 sono scorrelati.

Il terzo caso rappresenta invece una delle due situazioni nelle quali entrambi i fotoni sono riflessi od entrambi sono trasmessi, più precisamente la situazione di interferenza distruttiva.

Infatti bisogna ricordare che, per i rilevatori, lo stato “fotoni 1 e 2 entrambi riflessi” è indistinguibile dallo stato “fotoni 1 e 2 entrambi trasmessi”, e che lo specchio mezzo argentato sfasa di  $\pi$  radianti i fotoni che esso riflette.

Di conseguenza lo stato “fotone 1 riflesso/trasmesso” verrà cancellato, per opposizione di fase, dallo stato “fotone 2 trasmesso/riflesso”, da cui appunto l'interferenza distruttiva.

Per imporre questa cancellazione nella formula (3.5) dello stato  $|\mu\rangle$ , deve essere che:

$$|1R\psi\rangle|2R\psi\rangle = -|1T\psi\rangle|2T\psi\rangle \quad (3.6)$$

in modo tale quindi che il terzo termine dello stato  $|\mu\rangle$  si cancelli, grazie anche al fatto che lo stato del fotone 3 è in tal caso separabile dallo stato dei fotoni 1 e 2.

Quest'ultima formula contiene proprio le informazioni di indistinguibilità e sfasamento descritte prima.

Infine, il quarto termine dello stato  $|\mu\rangle$  rappresenta la seconda delle situazioni nelle quali entrambe i fotoni sono riflessi od entrambe trasmessi, ovvero la situazione di interferenza costruttiva: è questa la situazione d'interesse, ovvero quella che manifesta la formazione dello stato  $|B_{11}\rangle$  tra i fotoni 1 e 2.

Infatti, sostituendo la seguente relazione:

$$|1R\psi\rangle|2R\varphi\rangle = -|1T\varphi\rangle|2T\psi\rangle \quad (3.7)$$



che è analoga (e cioè contenente sempre le informazioni di indistinguibilità e sfasamento) alla (3.6), nel quarto termine dello stato  $|\mu\rangle$ , ed osservando che lo stato del fotone 3 può essere separato dallo stato dei fotoni 1 e 2, si ottiene che lo stato che in tal caso si viene a formare tra i fotoni 1 e 2 è il seguente:

$$\frac{|1T\psi\rangle|2T\phi\rangle - |1T\phi\rangle|2T\psi\rangle}{\sqrt{2}} = \frac{|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle}{\sqrt{2}} = |B_{11}\rangle \quad (3.8)$$

Pertanto in questo caso si è formato lo stato  $|B_{11}\rangle$  tra i fotoni 1 e 2.

Come si può osservare, ciò che ha qui impedito la formazione di interferenza distruttiva è il fatto che lo stato di polarizzazione del fotone 1 è sempre ortogonale a quello del fotone 2, ovvero il fatto che le loro polarizzazioni sono sempre diverse, il che impedisce la semplificazione dei due termini, mentre nel caso della terza parte dello stato  $|\mu\rangle$  si aveva che le due polarizzazioni erano sempre uguali e quindi si semplificavano, da cui appunto l'interferenza distruttiva in quel caso.

Come è già stato detto, la condivisione dello stato  $|B_{11}\rangle$  tra i fotoni 1 e 2 e tra i fotoni 2 e 3 comporta, a causa della doppia anti-correlazione, l'uguaglianza tra gli stati dei fotoni 1 e 3.

Questo può essere visto direttamente nel quarto termine della (3.5), dove appunto i fotoni 1, 2 e 3 compaiono rispettivamente negli stati  $|\psi\rangle$ ,  $|\phi\rangle$  e  $|\psi\rangle$ .

Concludiamo ora l'analisi dello schema di figura 3 del teletrasporto sperimentale, osservando che qualora lo stato  $|B_{11}\rangle$  tra i fotoni 1 e 2 si sia formato (il che, ricordiamo, è segnalato dai due rilevatori posti dopo lo specchio mezzo argentato), il blocco "Alice" trasmette un bit al blocco "Bob", tramite il canale di informazione classica.

Per esempio, è possibile imporre che il bit che il blocco "Alice" trasmette al blocco "Bob" sia sempre 0, ad eccezione di quando entrambi i rilevatori segnalano la presenza di un fotone.

In tal modo il blocco "Bob" sa quando lo stato del fotone 3 che esso possiede è teoricamente uguale a quello del fotone 1, ovvero sa quando il teletrasporto è avvenuto.

E' evidente come in tale sistema sia sufficiente la trasmissione di un solo bit, contro i due necessari nello schema teorico del teletrasporto quantistico di uno stato sconosciuto, dato che la tecnica sperimentale descritta è in grado di distinguere solamente tra le situazioni " $|B_{11}\rangle$  creato" e " $|B_{11}\rangle$  non creato" (tra i fotoni 1 e 2).

E comunque la funzione di quest'unico bit è differente da quella dei due bit dello schema teorico di figura 1.1, dato che questi due servono per distinguere tra loro i quattro stati di Bell, mentre il singolo bit serve per distinguere lo stato di Bell  $|B_{11}\rangle$  dagli stati non entangled che si possono formare nel blocco "Alice".

Per verificare sperimentalmente che il teletrasporto sia avvenuto, è sufficiente che il blocco "Bob" controlli, una volta ricevuto il segnale di conferma attraverso il canale classico, che la polarizzazione del fotone 3 sia uguale a quella del polarizzatore dal quale esce il fotone 1.

Per controllare la polarizzazione del fotone 3, il blocco "Bob" utilizza un separatore di fasci polarizzante, ovvero un dispositivo che riflette o trasmette un fotone a seconda della sua polarizzazione.

Quindi, basta che questo dispositivo venga regolato con la stessa polarizzazione del fotone 1, dopo che questo è uscito dal polarizzatore discusso in precedenza.

Per esempio, è possibile imporre che i fotoni che possiedono tale polarizzazione vengano riflessi dal separatore: in tal modo un eventuale segnale proveniente dal rilevatore del raggio riflesso svelerà che il teletrasporto è avvenuto.

Un eventuale raggio trasmesso avrà invece polarizzazione ortogonale a quella del raggio riflesso.

## 4 Applicazioni del teletrasporto quantistico

Il primo settore di applicazione al quale si potrebbe pensare è certamente quello del teletrasporto di persone ed oggetti di grandi dimensioni.

Non esistono ostacoli teorici nei confronti di questa applicazione, ma ciononostante essa probabilmente non resterà altro che un'idea fantasiosa.

E questo semplicemente per il fatto che la quantità di informazione da gestire in un simile teletrasporto è enorme (dell'ordine almeno del numero di Avogadro) e quindi il processo diventerebbe eccessivamente costoso.

Sarebbe quindi più conveniente, dal punto di vista economico, trasportare direttamente la persona o l'oggetto coinvolti.

Di seguito vengono invece riportati dei settori di applicazione reali del teletrasporto quantistico.

## 4.1 Memorie quantistiche

Nella sezione 3 è stato riportato l'esperimento del teletrasporto quantistico realizzato attraverso delle coppie di fotoni entangled ed è stata menzionata la possibilità di creare l'entanglement anche tra atomi.

Ma il teletrasporto non è ristretto solamente a questi sistemi omogenei, cioè a sistemi nei quali le particelle correlate sono dello stesso tipo (come appunto per esempio i casi fotone-fotone ed atomo-atomo).

Infatti è possibile realizzare l'entanglement anche tra coppie eterogenee, cioè correlare fotoni con atomi, o fononi con ioni, e così via [2].

In questo modo il teletrasporto permette di trasferire lo stato di particelle di vita breve in qualche sistema più stabile.

Questo apre quindi la possibilità delle memorie quantistiche, dove l'informazione di fotoni incidenti viene immagazzinata, tramite teletrasporto, su ioni intrappolati, accuratamente schermati dall'ambiente esterno.

## 4.2 Protezione delle trasmissioni dati dal rumore quantistico

La procedura completa del teletrasporto quantistico mostrata nella figura 2.2, ovvero quella facente uso della concentrazione dell'entanglement, può essere utilizzata per realizzare una trasmissione dell'informazione quantistica che sia protetta dagli errori causati dal rumore del canale quantistico di comunicazione [4].

Infatti, anziché utilizzare il canale di comunicazione quantistica affetto da rumore a disposizione per trasmettere direttamente da Alice e Bob i qubit di informazione, è possibile sfruttarlo per instaurare un entanglement parziale tra Alice e Bob stessi.

Questo entanglement parziale verrà poi concentrato, in modo che i due interlocutori giungano a condividere almeno uno stato  $|B_{00}\rangle$ .

In questo modo Alice potrà trasmettere i qubit di informazione a Bob tramite teletrasporto con fedeltà pari ad 1 (ovviamente nel caso di porte quantistiche e trasmissione classica perfette), evitando quindi di trasmetterli nel canale quantistico affetto da rumore (si è quindi trasferito il problema della trasmissione da un canale quantistico, con rumore, ad uno classico, che deve essere privo di disturbi).

In questo modo l'informazione quantistica, essendo teletrasportata, non risentirà del rumore del canale quantistico e quindi la trasmissione sarà complessivamente protetta dagli errori causati dal rumore stesso.

Quanto appena detto non aggiunge niente di nuovo al discorso fatto nel paragrafo 2.3 circa la procedura di concentrazione dell'entanglement, bensì rappresenta semplicemente una reinterpretazione dello schema come protocollo di protezione dagli errori di trasmissione.

Una particolare sotto-applicazione di questa capacità di trasmissione protetta è l'uso del teletrasporto per creare collegamenti affidabili tra computer quantistici od addirittura per creare microprocessori quantistici a rete neurale.

## 4.3 Porte quantistiche più affidabili

Come è stato detto nel paragrafo 2.1, il problema principale delle porte quantistiche è quello di poterne realizzare di affidabili.

E' stato anche detto che, per raggiungere questo obiettivo, è necessario scegliere, nella tecnica costruttiva, un compromesso tra isolamento e capacità di interazione con l'ambiente esterno ed utilizzare dei metodi di codifica dell'informazione.

Nel presente paragrafo viene specificato che l'idea che permette di utilizzare la codifica dell'informazione nella costruzione di porte affidabili, è quella di elaborare direttamente gli stati codificati, in modo tale che la loro decodifica non sia mai richiesta nei passaggi intermedi, ma solamente al termine dell'elaborazione [4].

Comunque il rumore non degrada solamente le funzioni logiche, ma anche la procedura di preparazione degli stati, la misurazione delle uscite e perfino la trasmissione dell'informazione lungo i fili quantistici.

Per combattere gli effetti del rumore viene allora sostituito ciascun qubit del circuito originale con un blocco codificato (come è stato detto, tramite un codice di correzione degli errori, come per esempio il codice di Steane a sette

qubit, che appartiene ad una particolare categoria di codici definiti *stabilizzatori*) di qubit ed inoltre ciascuna porta del circuito originale deve essere sostituita con una cosiddetta *porta codificata*, cioè con una porta che agisca direttamente sugli stati codificati.

Effettuando periodicamente la correzione degli errori sugli stati codificati è possibile prevenire la loro accumulazione. Tale accumulazione è infatti dannosa poiché non permette la ricostruzione corretta (tramite decodifica) dell'informazione originale.

Comunque queste correzioni periodiche non sono sufficienti a prevenire l'accumulazione degli errori, anche se effettuate dopo ciascuna porta codificata.

Le ragioni di questa affermazione sono due.

La prima è rappresentata dal fatto che, nel caso di porte a più ingressi ed a più uscite, un errore che si verifichi ad uno degli ingressi potrebbe propagarsi su più uscite.

Le porte codificate devono allora essere progettate in modo da propagare l'errore al minor numero possibile di uscite. La seconda ragione è rappresentata dal fatto che la correzione degli errori stessa può introdurre degli errori nei qubit codificati.

Questo problema ha soluzione analoga al precedente, cioè quella di realizzare delle procedure di correzione che, in caso di errore, non ne comportino una moltiplicazione eccessiva con la propagazione.

Si definisce in generale la tolleranza di una procedura nei confronti degli errori come la proprietà che, se un solo componente della procedura fallisce, allora questo fallimento causa al massimo un errore in ciascun blocco codificato di qubit in uscita dalla procedura.

In questa definizione, per "componente" s'intende ciascuna delle operazioni elementari utilizzate nella porta codificata, che possono includere funzioni logiche, misurazioni, fili quantistici e preparazioni di stati, tutti con rumore. La precedente definizione di tolleranza nei confronti degli errori può essere poi attribuita alle funzioni logiche, alle misurazioni, ai fili quantistici ed alle preparazioni di stati, ottenendo così le definizioni di funzioni logiche tolleranti, di misurazioni tolleranti, eccetera.

Esiste poi un importante risultato, definito *teorema della soglia*, che dimostra come sia possibile ottenere, tramite una serie di codifiche concatenate, un circuito che simuli (attraverso un numero  $N$  di porte pari a  $GM$ , dove  $M$  rappresenta il numero di porte del circuito originale, mentre  $G$  rappresenta una funzione polinomiale con argomento  $\log_2 M$ ) una funzione logica qualsiasi con una probabilità di errore piccola a piacere, nella condizione però che ciascun componente delle porte del circuito di simulazione abbia una probabilità di errore minore di una apposita costante tipica della funzione logica da simulare.

Come riportato nel paragrafo 5.3, le porte  $H$ , fase, CNOT e  $\pi/8$  formano un set universale (in alternativa si può considerare il set universale formato da  $H$ , fase, CNOT e Toffoli).

Grazie a tale proprietà di universalità, essendo poi note delle tecniche per realizzare queste quattro porte in modo affidabile, è possibile creare qualsiasi porta quantistica in modo affidabile.

Un metodo per realizzare in modo affidabile le quattro porte del set universale è attraverso delle appropriate sequenze di porte codificate, facenti uso di codici stabilizzatori, e di misurazioni (per quanto riguarda il set alternativo che fa uso della porta di Toffoli, bisogna specificare che la realizzazione in modo affidabile, sempre con questa tecnica, di tale porta si basa su uno schema analogo a quello della porta  $\pi/8$  tollerante, ma più elaborato).

Purtroppo però, utilizzando questa tecnica, le porte fase e  $\pi/8$  (oppure, in alternativa, la porta di Toffoli) risultano progettate tramite degli schemi ad hoc e quindi non facilmente generalizzabili.

Un metodo alternativo per realizzare tali porte in modo affidabile, e che si presta ad una facile generalizzazione, è rappresentato dall'uso del teletrasporto quantistico [11].

Per comprendere come sia possibile generalizzare la procedura del teletrasporto che verrà spiegata, è necessario osservare prima come sia possibile raccogliere diverse porte logiche (non è ancora noto se tutte) in gruppi  $C_k$ , con  $k$  numero intero e maggiore od uguale a 1, dove  $C_1 \equiv G_n$ , con  $G_n$  che rappresenta il gruppo di Pauli (vedere il paragrafo 5.3) ed  $n$  il numero di qubit sui quali lavorano le porte appartenenti a tale gruppo, mentre, per ogni  $k$  intero maggiore od uguale a 2, questi gruppi sono definiti come  $C_k = \{U | UC_1 U^\dagger \subseteq C_{k-1}\}$ .

Un gruppo particolare è  $C_2$ , definito *gruppo di Clifford*.

Alla luce di questa definizione di gruppo  $C_k$ , si dimostra che le porte fase e  $\pi/8$  (oppure, in alternativa, la porta di Toffoli), cioè quelle realizzate ad hoc, sono contenute nel gruppo  $C_3$ .

E' questa l'osservazione che permetterà di generalizzare, tramite teletrasporto, la costruzione di tali porte.

Si comincia ora con il dimostrare come sia possibile utilizzare il teletrasporto nella simulazione di una porta quantistica ad un qubit, per poi passare alla generalizzazione di questa tecnica.

La capacità di utilizzare in tal modo il teletrasporto è garantita dalla possibilità di trasferire la funzione logica dalla porta quantistica allo stato entangled che compare nel teletrasporto, nel senso di seguito spiegato.

Per cominciare, prendiamo in considerazione lo schema del teletrasporto di figura 1.1, e sostituiamo lo stato  $|B_{00}\rangle$  con lo stato  $(I_2 \otimes U)|B_{00}\rangle$ , dove  $U$  è un operatore quantistico ad un qubit (che sia però diverso dall'operatore  $I_2$ , poiché questo caso sarebbe banale), che rappresenta la porta quantistica da simulare (ovviamente  $U$  deve essere un operatore unitario: vedere il paragrafo 5.3).

A causa di questa sostituzione, lo stato ricostruito da Bob non sarà più  $|\psi\rangle$ .

Per ogni operatore  $U$  è possibile modificare ulteriormente la procedura del teletrasporto di figura 1.1 in modo che lo stato ricostruito da Bob sia  $U|\psi\rangle$ .

Si comincia infatti con l'osservare che, per la (1.6), si ha che  $(B \otimes I_2)(|\psi\rangle|B_{00}\rangle) = |M_1\rangle|M_2\rangle(X^{M_2}Z^{M_1}|\psi\rangle)$ ,  $\forall |\psi\rangle$  (indipendentemente dall'uscita  $|M_1\rangle|M_2\rangle$  di  $B$ ), e quindi  $(B \otimes U)(|\psi\rangle|B_{00}\rangle) = |M_1\rangle|M_2\rangle[U(X^{M_2}Z^{M_1}|\psi\rangle)]$ .

Affinché Bob possa ricostruire lo stato  $U|\psi\rangle$ , è sufficiente che l'operatore  $U$  goda della proprietà per la quale esiste un operatore  $G_{M_1M_2}$  invertibile tale che  $U(X^{M_2}Z^{M_1}) = G_{M_1M_2}U$ .

Infatti in tal caso basterebbe che Bob applicasse, al posto dell'operatore  $Z^{M_1}X^{M_2}$  espresso dalla (1.7), l'operatore  $G_{M_1M_2}^{-1}$ , il che gli permetterebbe di ricostruire lo stato  $U|\psi\rangle$ , dato che:

$$\begin{aligned} G_{M_1M_2}^{-1} \left[ (B \otimes U)(|\psi\rangle|B_{00}\rangle) \right] &= G_{M_1M_2}^{-1} \left\{ |M_1\rangle|M_2\rangle \left[ U(X^{M_2}Z^{M_1}|\psi\rangle) \right] \right\} = |M_1\rangle|M_2\rangle \left\{ G_{M_1M_2}^{-1} \left[ G_{M_1M_2} U|\psi\rangle \right] \right\} = \\ &= |M_1\rangle|M_2\rangle \left[ (G_{M_1M_2}^{-1} G_{M_1M_2}) U|\psi\rangle \right] = |M_1\rangle|M_2\rangle (U|\psi\rangle) \end{aligned} \quad (4.1)$$

In realtà ogni operatore gode di questa proprietà, dato che basta porre  $G_{M_1M_2} = U(X^{M_2}Z^{M_1})U^\dagger$ .

Però solamente per certi operatori  $U$  ad un qubit è possibile realizzare la procedura di teletrasporto appena descritta utilizzando una porta  $G_{M_1M_2}^{-1}$  appartenente al gruppo  $G_1$ .

Infatti, per la definizione data precedentemente di gruppo  $C_k$ , ed osservando che  $(X^{M_2}Z^{M_1})^{-1} = (Z^{M_1})^{-1}(X^{M_2})^{-1} = Z^{M_1}X^{M_2} \in G_1$ , si ha che  $G_{M_1M_2}^{-1} = [U(X^{M_2}Z^{M_1})U^\dagger]^{-1} = (U^\dagger)^{-1}(X^{M_2}Z^{M_1})^{-1}U^{-1} = U(Z^{M_1}X^{M_2})U^\dagger \in G_1 \Leftrightarrow U \in C_2$  (in questi passaggi è stato utilizzato il fatto che  $U$  è un operatore unitario, ovvero il fatto che  $U^\dagger = U^{-1}$ ).

Quindi solamente per  $U \in C_2$  si ha che  $G_{M_1M_2}^{-1} \in G_1$ , ovvero che la procedura di teletrasporto modificata può essere realizzata attraverso sole porte appartenenti al gruppo  $G_1$  (escludendo ovviamente il blocco della misurazione nella

base di Bell e l'operatore  $U$  applicato al qubit basso dello stato  $|B_{00}\rangle$ , del quale si discuterà più avanti).

Supponiamo invece di voler utilizzare questa tecnica per simulare il comportamento di un operatore  $U$  ad un qubit appartenente per esempio al gruppo  $C_3$  (come la porta  $\pi/8$ ).

In tal caso, sempre per la definizione data di gruppo  $C_k$  e per il fatto che  $(X^{M_2}Z^{M_1})^{-1} \in G_1$ , si ottiene che

$G_{M_1M_2}^{-1} \in C_2$ , e siccome le porte appartenenti al gruppo  $C_2$  non possono essere espresse in termini di porte appartenenti al gruppo  $G_1$ , ne segue che ogni  $U$  appartenente al gruppo  $C_3$  non rientra direttamente nell'insieme di operatori studiato (ovvero nell'insieme degli operatori per i quali la procedura di simulazione tramite teletrasporto può essere effettuata utilizzando solamente operatori appartenenti al gruppo  $G_1$ , anche se in realtà è possibile farli rientrare in questo insieme tramite un procedimento ricorsivo, come verrà spiegato più avanti).

Di seguito viene mostrato un esempio della procedura di teletrasporto modificata, nel caso in cui  $U=H$ , poiché  $H \in C_2$ :

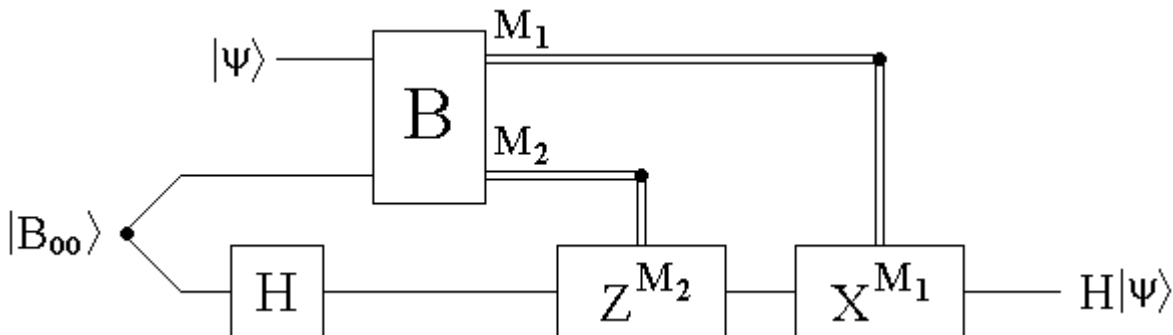


Figura 4.1

Come si può osservare, lo schema è identico a quello di figura 1.1, solamente che compare  $(I_2 \otimes H)|B_{00}\rangle$  al posto di  $|B_{00}\rangle$  (il cui motivo è già stato spiegato) e le due porte X e Z sono scambiate. Questo scambio è giustificato semplicemente dal fatto che:

$$G_{M_1 M_2}^{-1} = [H(X^{M_2} Z^{M_1})H^\dagger]^{-1} = (H^\dagger)^{-1} [(Z^{M_1})^{-1} (X^{M_2})^{-1}] H^{-1} = H(Z^{M_1} X^{M_2})H = X^{M_1} Z^{M_2} \quad (4.2)$$

avendo utilizzato il fatto che l'operatore H è unitario.

In questo modo Bob riesce a ricostruire lo stato  $H|\psi\rangle$ , utilizzando solamente le porte X e Z, che sono porte appartenenti al gruppo  $G_1$ .

E' possibile estendere poi la tecnica mostrata al caso di operatori che appartengono sempre al gruppo  $C_2$ , ma che operino su un maggior numero di qubit contemporaneamente. Nell'esempio seguente viene riportato il caso della porta CNOT:

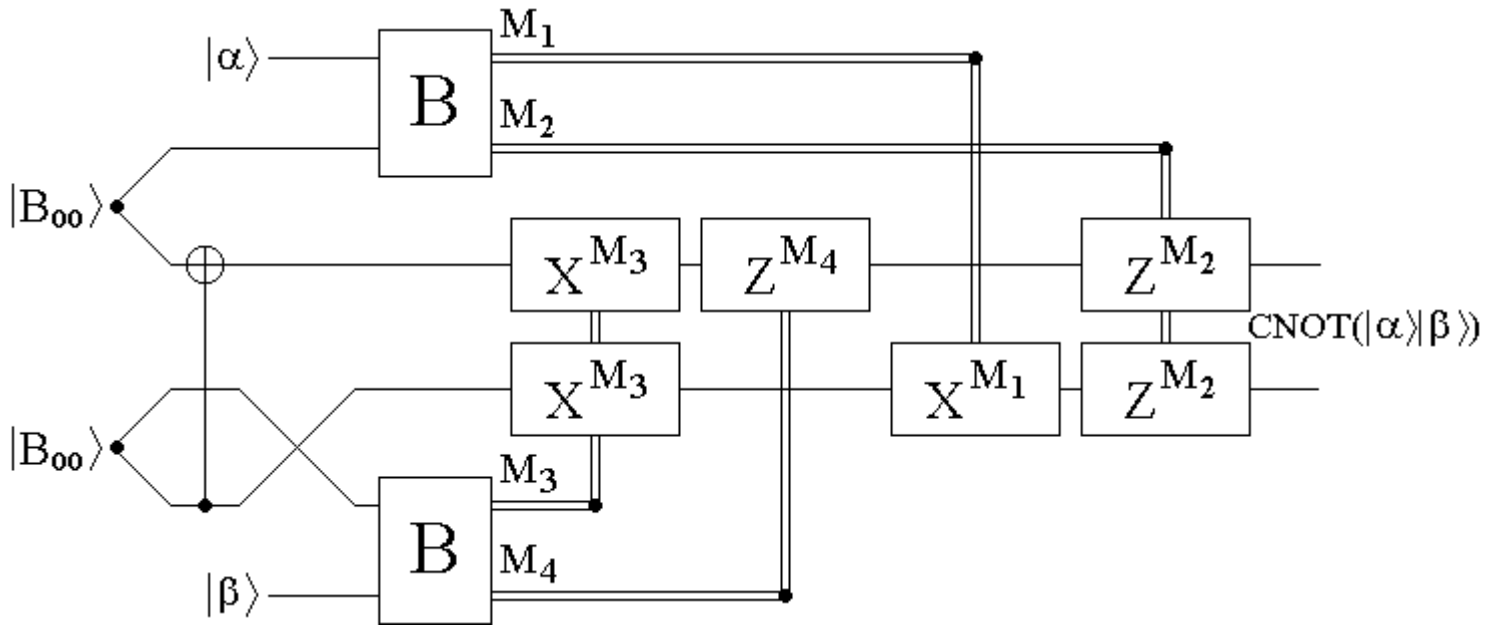


Figura 4.2

Si osserva che questa volta, invece di applicare l'operatore  $I_2 \otimes H$  allo stato  $|B_{00}\rangle$ , viene applicato l'operatore

$I_2 \otimes I_2 \otimes \text{CNOT}$  allo stato  $|B_{00}\rangle|B_{00}\rangle$ , in modo che il qubit alto (cioè rappresentato dalla linea posta più in alto nello schema: questo metodo di individuare in modo grafico i qubit di uno stato entangled potrebbe dare origine a delle ambiguità se non si fissa una convenzione, ma purtroppo è l'unico possibile, dato che le parti di uno stato entangled non sono quanto-meccanicamente definite) di ciascuno stato  $|B_{00}\rangle$  entri in una porta  $I_2$  (cioè, per meglio dire, non subisce alcuna operazione), mentre i due qubit bassi entrino nella porta CNOT.

Comunque è da ricordare che, per gli operatori H e CNOT, in quanto appartenenti al gruppo  $C_2$ , esistono già delle tecniche che permettono facilmente di realizzarli in modo affidabile senza far uso del teletrasporto.

I motivi per i quali sono stati mostrati gli schemi delle porte H e CNOT sono allora diversi.

Infatti questi schemi permettono di rendere più facile la generalizzazione che verrà di seguito spiegata per la tecnica di simulazione tramite teletrasporto ed inoltre mostrano come il teletrasporto unito a tutti gli operatori ad un qubit rimanenti (X, Y, Z,  $\pi/8$ , eccetera) formi un set universale alternativo a quelli indicati in precedenza (e nel paragrafo 5.3).

Infatti le porte H e CNOT possono essere realizzate tramite il teletrasporto ed operatori appartenenti al gruppo  $G_1$ , ed assieme a tutti gli operatori ad un qubit rimanenti formano un set universale: pertanto tutte le porte quantistiche possono essere realizzate tramite questo nuovo set.

Torniamo ora al problema iniziale.

Precedentemente sono stati mostrati due esempi concreti di come questa tecnica possa essere applicata a delle porte appartenenti ai gruppi  $C_2$  ed operanti su un numero qualsiasi di qubit.

Mostriamo ora come essa possa essere generalizzata, tramite un'estensione ad operatori  $U$  (sempre unitari ovviamente) appartenenti a  $C_k$ , dove  $k$  rappresenta un intero qualsiasi maggiore od uguale a 2, operanti anch'essi su un numero qualsiasi di qubit.

Questa generalizzazione consiste semplicemente nel mostrare come la procedura modificata del teletrasporto utilizzata in precedenza per le porte appartenenti al gruppo  $C_2$  possa essere utilizzata per simulare il comportamento di porte appartenenti al gruppo generico  $C_k$ , con  $k \geq 2$ , utilizzando operatori appartenenti al gruppo  $C_{k-1}$ .

Consideriamo, in generale, un operatore  $U$  qualsiasi, purché unitario, appartenente al gruppo  $C_k$  (con  $k \geq 2$ ) e che agisca su un numero  $n$  qualsiasi di qubit.

Poiché esso opera su  $n$  qubit, estendendo il risultato trovato con la porta CNOT, è possibile concludere che questa volta il numero di stati  $|B_{00}\rangle$  occorrenti è  $n$  (stati che possono essere raggruppati in un unico stato complessivo

$|B_{00}^n\rangle = [(|00\rangle + |11\rangle)/\sqrt{2}]^{\otimes n}$  e che lo stato d'ingresso al sistema, che viene indicato con  $|\psi\rangle$  (dove  $|\psi\rangle = |\alpha\rangle|\beta\rangle$  nel caso della CNOT), debba essere uno stato ad  $n$  qubit.

Sempre estendendo il risultato trovato con la CNOT, si riarrangiano le parti degli  $n$  stati  $|B_{00}\rangle$  in modo che, prima delle misure nella base di Bell, i qubit alti non subiscano alcuna operazione, mentre quelli bassi finiscano nella porta  $U$ . Nello schema di figura 4.2 della porta CNOT si sarebbero anche potuti raccogliere i due operatori  $B$  in un unico operatore  $B$  complessivo e raccogliere le quattro uscite  $M_1, M_2, M_3$  ed  $M_4$  dei due operatori  $B$  in due sole uscite dell'operatore  $B$  complessivo, più precisamente riunire  $M_1$  ed  $M_3$  in una sola delle due uscite di  $B$  complessivo, ed  $M_2$  ed  $M_4$  nell'altra (in altri termini, vengono raggruppate le uscite analoghe dei due operatori  $B$ ).

Sempre in tale schema, si sarebbero potuti inoltre raccogliere gli operatori  $X$  e  $Z$  in un'unica rete complessiva, appartenente al gruppo  $G_2$ , che costituisce la generalizzazione dell'operatore  $G_{M_1 M_2}^{-1} \in G_1$  e comandata dalle linee  $M_1, M_2, M_3$  ed  $M_4$ .

Questo è quello che viene fatto nel caso ora analizzato della porta  $U$  generica, ponendo inoltre che tale rete complessiva (cioè la generalizzazione del complesso degli operatori  $X$  e  $Z$  visto nel caso della CNOT) abbia funzione

logica  $G_{xy}^{-1}$ , con  $G_{xy} = U F_{xy} U^\dagger$ , dove  $F_{xy}$  è un operatore appartenente a  $G_n$ , dipendente dall'uscita  $|x\rangle|y\rangle$  dell'operatore  $B$  complessivo (dove  $x$  ed  $y$  rappresentano i raggruppamenti delle uscite analoghe dei singoli operatori  $B$ ), e tale che  $(B \otimes I_n)(|\psi\rangle|B_{00}^n\rangle) = |x\rangle|y\rangle(F_{xy}|\psi\rangle)$ ,  $\forall |\psi\rangle$  (indipendentemente dall'uscita  $|x\rangle|y\rangle$  di  $B$ ).

L'operatore  $F_{xy}$  rappresenta la generalizzazione dell'operatore  $X^{M_2} Z^{M_1}$  considerato in precedenza nel caso di operatore  $U$  ad un bit ed appartenente al gruppo  $C_2$ .

Si osserva ora, tramite gli stessi passaggi riportati in precedenza nel caso di operatore  $U$  ad un qubit ed appartenente al gruppo  $C_2$ , che la funzione logica  $G_{xy}^{-1}$ , per come è stata definita, permette a Bob di ottenere in uscita lo stato  $U|\psi\rangle$ .

Come è già stato detto, questa generalizzazione mostra come la procedura modificata del teletrasporto possa essere utilizzata per simulare il comportamento di porte appartenenti al gruppo generico  $C_k$ , con  $k \geq 2$ , tramite operatori appartenenti al gruppo  $C_{k-1}$ , dato che, per  $U \in C_k$ , si ottiene che  $G_{xy}^{-1} = (U F_{xy} U^\dagger)^{-1} = (U^\dagger)^{-1} F_{xy}^{-1} U^{-1} = U F_{xy}^{-1} U^\dagger \in C_{k-1}$ , dato anche che  $F_{xy} \in G_n \Rightarrow F_{xy}^{-1} \in G_n$ .

In modo ricorsivo, questa procedura può essere utilizzata per simulare il comportamento di porte appartenenti al gruppo  $C_{k-1}$ , tramite operatori appartenenti al gruppo  $C_{k-2}$ , e così via, fino a giungere agli operatori appartenenti al gruppo  $G_n$ .

In questo modo, il comportamento delle porte appartenenti al gruppo  $C_k$  generico può essere simulato, attraverso il teletrasporto quantistico, utilizzando solamente operatori appartenenti al gruppo  $G_n$ .

Il motivo per il quale si voleva giungere ad ottenere questo risultato è rappresentato dal fatto che le porte appartenenti al gruppo  $G_n$  possono essere facilmente realizzate in modo affidabile attraverso delle appropriate sequenze di porte codificate, facenti uso di codici stabilizzatori.

Siccome poi è possibile realizzare in modo affidabile anche la misurazione nella base di Bell, la propagazione lungo i fili quantistici e la preparazione degli stati, che sono le ultime operazioni richieste per realizzare la procedura del teletrasporto analizzata, ne segue che tramite questa procedura è possibile realizzare in modo affidabile le porte appartenenti al generico gruppo  $C_k$ .

Comunque, qualora si volesse implementare una data funzione logica in un sistema, potrebbe non essere conveniente utilizzare direttamente questa tecnica, a causa della elevata complessità circuitale risultante nel caso di funzioni logiche appartenenti a gruppi di ordine elevato.

Inoltre non è detto che tutte le porte possano essere simulate col teletrasporto, dato che non è detto che l'unione di tutti gli insiemi  $C_k$ , cioè per  $k$  che va da 1 fino a  $+\infty$ , includa tutte le porte quantistiche possibili: infatti il preciso set di porte che forma ciascun gruppo  $C_k$  è ancora oggetto di studio.

Pertanto nel primo caso potrebbe essere più conveniente, mentre nel secondo sarebbe l'unica soluzione, realizzare con questa tecnica le porte di un qualche set universale e che appartengano a gruppi  $C_k$  di ordine basso, e poi esprimere la funzione logica da implementare in termini delle porte di questo set universale.

Per esempio la tecnica del teletrasporto permette di simulare facilmente ed in modo affidabile le porte appartenenti al gruppo  $C_3$  e quindi in particolare le porte fase e  $\pi/8$  (oppure, in alternativa, la porta di Toffoli), che assieme alle porte H e CNOT formano, come già detto in precedenza, un set universale.

E comunque si ricorda che era già possibile ottenere in modo affidabile le porte appartenenti al gruppo  $C_3$  senza l'uso del teletrasporto, anche se in modo più complesso, dato che si trattava di utilizzare degli schemi ad hoc.

Si osserva comunque che per simulare le porte appartenenti a gruppi di ordine maggiore od uguale a 3 non è necessario procedere in maniera iterativa fino a giungere ad una rete  $G_{xy}^{-1} \in C_1$ .

E' infatti sufficiente fermarsi al caso  $G_{xy}^{-1} \in C_2$ , dato che anche le porte appartenenti al gruppo  $C_2$  possono facilmente essere realizzate in modo affidabile.

Ad ogni modo il teletrasporto presenta come vantaggio quello di permettere una facile generalizzazione dello schema attraverso il quale le porte  $C_3$  e quelle di ordine superiore vengono realizzate in modo affidabile ed inoltre un secondo vantaggio, derivante dal trasferimento della funzione logica dalla porta allo stato entangled.

E' stato infatti dimostrato precedentemente che è possibile ottenere un sistema di teletrasporto che si comporti esattamente come una determinata porta quantistica (se la funzione logica  $U$  non appartiene a qualche gruppo  $C_k$ ,

allora basta realizzarla tramite un'opportuna combinazione delle porte logiche di un qualche set universale che godano di questa proprietà), senza avere a disposizione la porta quantistica stessa: basta solamente alterare lo stato entangled con la funzione logica di quella porta.

In questo senso la funzione logica è stata trasferita dalla porta quantistica allo stato entangled.

Questo sembrerebbe non essere un grande vantaggio, poiché se la funzione logica è difficile da implementare in modo affidabile direttamente in una porta logica, non sembra esserci ragione per la quale la funzione debba essere più facile da implementare nello stato entangled.

Nonostante l'apparenza, si dimostra che l'implementazione sullo stato entangled può essere ottenuta in modo affidabile, perfino utilizzando porte inaffidabili.

Questo per il fatto che una tale implementazione è da realizzare solamente su degli stati specifici, cioè solamente sui qubit bassi degli stati entangled, e per il fatto che l'implementazione su stati specifici risulta più facile rispetto a quella su stati sconosciuti, come sono quelli in ingresso ad una porta quantistica.

In altri termini, con questo trasferimento della funzione logica  $U$ , essa deve essere implementata su un numero finito di stati noti (che sono appunto le varie combinazioni dei qubit bassi degli stati entangled), mentre, qualora si decidesse di realizzare direttamente la porta quantistica, la sua funzione logica dovrebbe essere implementata sull'infinità di stati possibili al suo ingresso.

## 4.4 Testare la validità della meccanica quantistica

La tecnica di teletrasporto di Bennett *et al.* [1] è importante anche dal punto di vista concettuale, in quanto costituisce una delle incredibili conseguenze della meccanica quantistica.

Infatti la verifica a livello sperimentale delle previsioni teoriche derivanti dall'uso di questa tecnica rappresenta, assieme alla disuguaglianza di Bell, una prova a favore della meccanica quantistica, nel dibattito contro la teoria delle variabili locali nascoste, circa il problema dell'interpretazione fisica della realtà.

Infatti, riuscire a teletrasportare dell'informazione tramite una quantità di bit inferiore a quella prevista dal più efficiente dei protocolli di teletrasporto classico [3] può essere considerato come una prova dell'esistenza dell'entanglement e quindi del fenomeno della non-località, che è escluso nella teoria delle variabili locali nascoste.

## 5 Appendice

In questa sezione vengono riportate le conoscenze necessarie per la comprensione della maggior parte dei concetti esposti nelle sezioni precedenti.

Innanzitutto bisogna osservare che nei paragrafi 1.1.1 (più precisamente, nella dimostrazione che il teletrasporto non implica una velocità superluminare dell'informazione) e 2.3 (cioè nel calcolo della fedeltà del teletrasporto e dell'entanglement E) viene utilizzata una formulazione alternativa della meccanica quantistica, realizzata attraverso un importante strumento definito *operatore densità* oppure *matrice densità* [4].

Questa formulazione alternativa è comunque matematicamente equivalente a quella dei vettori di stato, ma fornisce un linguaggio molto più conveniente in alcuni dei problemi affrontati.

Questi problemi possono essere risolti anche utilizzando la formulazione dei vettori di stato, ma in modo più complesso.

La matrice densità permetterà quindi di definire, nel corso di questa stessa sezione, alcune grandezze di grande importanza utilizzate nelle sezioni precedenti, come l'entropia di von Neumann (vedere il paragrafo 5.2) e la fedeltà con la quale avviene il teletrasporto (vedere il paragrafo 5.4).

Comunque, trattandosi di una riformulazione alternativa della meccanica quantistica, la teoria relativa alla matrice densità viene data per scontata anche in questa sezione, cioè considerata come prerogativa di un corso di introduzione alla meccanica quantistica, e quindi non viene trattata.

Analogamente non vengono trattati nemmeno tutti gli strumenti di calcolo che sono di supporto a tale riformulazione, come il concetto di traccia parziale [4], anch'esso utilizzato nelle sezioni 1.1.1 e 2.3 (seppur implicitamente in quest'ultima).

Si può ora passare ad esaminare i prerequisiti rimanenti.

### 5.1 Qubit e stati entangled

Dato che in questo lavoro viene affrontato il problema dell'elaborazione dell'informazione quantistica, è necessario innanzitutto definire il concetto di *informazione quantistica*.

Per raggiungere questo obiettivo è però necessario definire prima il concetto di bit quantistico.

Come nell'ambito della computazione classica e dell'informazione classica (*teoria dell'informazione di Shannon*) il *bit* rappresenta il concetto fondamentale [4][7], a livello quantistico la corrispondente grandezza è rappresentata appunto dal *bit quantistico*, detto anche *qubit* [4], che costituisce una generalizzazione di quello classico.

Come il bit classico può assumere solamente lo stato 0 od 1, il qubit, se misurato, può assumere solamente, utilizzando la notazione di Dirac, lo stato  $|0\rangle$  oppure lo stato  $|1\rangle$ .

Però, l'importante differenza tra i due casi classico e quantistico, è che il qubit, prima di essere misurato, può assumere anche degli stati di sovrapposizione, cioè di combinazione lineare, tra gli stati  $|0\rangle$  ed  $|1\rangle$ .

In altri termini, la forma generale di un qubit è la seguente:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \quad (5.1)$$

dove  $\theta$  e  $\phi$  sono due costanti reali.

Gli stati  $|0\rangle$  ed  $|1\rangle$  costituiscono una base ortonormale per lo spazio di Hilbert di tutti i possibili qubit singoli (cioè aventi la forma appena mostrata), definita base computazionale.

Comunque in realtà la coppia  $\{|0\rangle;|1\rangle\}$  rappresenta, in tutto e per tutto, solo una delle infinite scelte di base possibili per un qubit singolo, in quanto è possibile (almeno in principio, anche se ciò non significa che possa essere realizzato facilmente) effettuare una misurazione del qubit anche rispetto ad una base diversa da quella computazionale.

Nel teletrasporto quantistico sono utilizzati dei particolari qubit doppi, ovvero dei qubit condivisi da due sottosistemi formanti un unico sistema composto, noti con il nome di *stati di Bell* o *stati EPR* (Einstein, Podolsky, Rosen) o *coppie EPR*, che costituiscono una base ortonormale per lo spazio di Hilbert di tutti i possibili qubit doppi, e di seguito mostrati:

$$|B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad |B_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad |B_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad |B_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (5.2)$$



dove si è utilizzata la convenzione  $|xy\rangle \equiv |x\rangle \otimes |y\rangle$ , con  $x, y \in \{0;1\}$ .

Lo stato di Bell  $|B_{11}\rangle$  presenta la caratteristica di essere invariante sotto rotazione della base, ovvero i coefficienti della combinazione lineare che lo definisce rimangono gli stessi indipendentemente dalla base rispetto alla quale  $|B_{11}\rangle$  viene rappresentato, una proprietà utilizzata nel paragrafo 1.1.2 e nella sezione 3.

Per dimostrarla, prendiamo in considerazione due stati quantistici  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  e  $|\varphi\rangle = \chi|0\rangle + \delta|1\rangle$ .

Affinché  $\{|\psi\rangle; |\varphi\rangle\}$  costituisca una base ortonormale dello spazio generato dalla coppia  $\{|0\rangle; |1\rangle\}$ , e che soddisfi la relazione di completezza, deve essere verificato che  $|\alpha|^2 + |\chi|^2 = 1$ ,  $|\beta|^2 + |\delta|^2 = 1$  ed  $\alpha^* \beta + \chi^* \delta = 0$ .

Se poniamo  $\alpha = \cos(\theta/2)$  e  $\beta = e^{i\phi} \sin(\theta/2)$ , allora queste tre relazioni sono contemporaneamente soddisfatte da  $\chi = -\sin(\theta/2)$  e  $\delta = e^{i\phi} \cos(\theta/2)$ .

A questo punto basta osservare che, utilizzando la proprietà di completezza della base  $\{|\psi\rangle; |\varphi\rangle\}$ , si ottiene:

$$\begin{aligned}
 |B_{11}\rangle &= (I_2 \otimes I_2) |B_{11}\rangle = [ (|\psi\rangle\langle\psi| + |\varphi\rangle\langle\varphi|) \otimes I_2 ] \frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} [ (|\psi\rangle\langle\psi| + |\varphi\rangle\langle\varphi|) |0\rangle I_2 |1\rangle + \\
 &- (|\psi\rangle\langle\psi| + |\varphi\rangle\langle\varphi|) |1\rangle I_2 |0\rangle ] = \frac{1}{\sqrt{2}} [ (\alpha|\psi\rangle + \chi|\varphi\rangle) |1\rangle - (\beta^*|\psi\rangle + \delta^*|\varphi\rangle) |0\rangle ] = \\
 &= \frac{1}{\sqrt{2}} [ |\psi\rangle(-\beta^*|0\rangle + \alpha|1\rangle) + |\varphi\rangle(-\delta^*|0\rangle + \chi|1\rangle) ] = \frac{1}{\sqrt{2}} [ |\psi\rangle(-e^{-i\phi} \sin(\theta/2)|0\rangle + \cos(\theta/2)|1\rangle) + \\
 &+ |\varphi\rangle(-e^{-i\phi} \cos(\theta/2)|0\rangle - \sin(\theta/2)|1\rangle) ] = \frac{e^{-i\phi}}{\sqrt{2}} [ |\psi\rangle(-\sin(\theta/2)|0\rangle + e^{i\phi} \cos(\theta/2)|1\rangle) + \\
 &- |\varphi\rangle(\cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle) ] = \frac{1}{\sqrt{2}} (|\psi\rangle\langle\varphi| - |\varphi\rangle\langle\psi|)
 \end{aligned} \tag{5.3}$$

avendo sfruttato il fatto che il fattore di fase  $e^{-i\phi}$  non è fisicamente osservabile.

Si può notare che questo risultato vale per ogni valore dei parametri  $\theta$  e  $\phi$  e di conseguenza esprime l'invarianza dello stato  $|B_{11}\rangle$  rispetto alla generica rotazione della base rispetto alla quale esso viene rappresentato.

Invece gli altri stati di Bell non presentano questa caratteristica.

Tutti e quattro gli stati di Bell presentano invece la proprietà di non essere rappresentabili come prodotto tensoriale di due singoli qubit.

Si dice pertanto che gli stati di Bell *non sono separabili* e che le loro parti (ovvero i qubit associati ai due sottosistemi, formanti il sistema composto, che condividono lo stato di Bell) sono *quanto-meccanicamente indefinite*.

Tutti gli stati che presentano questa proprietà vengono definiti *stati entangled*.

Gli stati di Bell sono degli esempi di stati entangled *bi-ripartiti*, ovvero condivisi tra due sottosistemi.

Esistono anche esempi di stati entangled *multi-ripartiti*, cioè condivisi da più di due sottosistemi contemporaneamente, come per esempio gli stati seguenti [11]:

$$\begin{aligned}
 |\Upsilon\rangle &= (|000\rangle + |111\rangle) / 2 \\
 |\chi\rangle &= [ (|00\rangle + |11\rangle) |00\rangle + (|01\rangle + |10\rangle) |11\rangle ] / 2
 \end{aligned} \tag{5.4}$$

che sono rispettivamente tri e quadri-ripartiti e che quindi presentano rispettivamente tre e quattro parti quanto-meccanicamente indefinite.

Una conseguenza di questa proprietà è la cosiddetta *non-località*, cioè la capacità che una misurazione effettuata da un osservatore sulla sua parte dello stato entangled influenzi il risultato della misurazione effettuata da un secondo osservatore sulla propria parte dello stesso stato entangled, condiviso tra i due osservatori.

Un esempio concreto di non-località è rappresentato dal fenomeno dell'anti-correlazione che si verifica nello stato di Bell  $|B_{11}\rangle$ .

Se viene effettuata una misurazione dell'operatore vettoriale di Pauli  $\sigma = (\sigma_x, \sigma_y, \sigma_z)$  sulle due parti dello stato  $|B_{11}\rangle$ , lungo l'asse  $\mathbf{v}$  (ovvero se viene misurata l'osservabile  $\mathbf{v} \cdot \sigma$ ), i risultati possono essere solamente +1 oppure -1 per

ciascuna parte dello stato di Bell, ma si dimostra [4] che, per qualunque scelta di  $v$ , i segni dei risultati delle due misurazioni sono sempre opposti tra di loro.

Questo mostra quindi come il risultato della misura effettuata sul primo qubit influenzi il risultato della misura effettuata sul secondo qubit, per di più in modo indipendente dalla distanza alla quale sono posti i due osservatori: è quindi un esempio di non-località.

In questo senso, stati entangled bi-ripartiti correlano due osservatori, mentre stati entangled multi-ripartiti correlano più di due osservatori contemporaneamente.

E' la proprietà di non-località il motivo per il quale gli stati entangled giocano un ruolo cruciale nell'ambito della computazione quantistica e dell'informazione quantistica, più precisamente nell'ambito del teletrasporto quantistico e della codifica superdensa [4].

Inoltre è sempre questa proprietà che permette agli stati entangled di violare la disuguaglianza di Bell e di dimostrare quindi che almeno l'ipotesi di località nel teorema EPR non è corretta (anche questo risultato è estremamente significativo, in quanto impartisce l'importante lezione che la realtà fisica non è quella che appare ai nostri occhi). Sembra incredibile che una misurazione su una parte di uno stato entangled possa influenzare istantaneamente lo stato di un'altra sua parte, che può essere arbitrariamente lontana.

Talmente incredibile che addirittura Einstein rinnegava questo fenomeno di non-località, come dimostra il fatto che nel teorema EPR la località era posta come ipotesi e quindi assunta come fatto vero.

Ma ciononostante questa proprietà è stata ormai dimostrata da numerosi esperimenti, che hanno verificato che l'entanglement sopravvive su distanze dell'ordine di almeno 10 Km.

## 5.2 Entropia di Shannon, entropia di von Neumann e ridondanza

E' ora finalmente possibile passare a definire il concetto di informazione quantistica.

Si prenda in considerazione un qubit singolo  $|\psi\rangle$ : l'informazione quantistica ad esso associata è rappresentata dalla conoscenza della costanti  $\theta$  e  $\phi$  che compaiono nella combinazione lineare che lo definisce (vedere l'espressione (5.1)).

Pertanto disporre di un qubit di informazione quantistica equivale a possedere un qubit noto, ovvero uno stato quantistico che presenta delle costanti  $\theta$  e  $\phi$  dal valore conosciuto.

Comunque, siccome queste costanti sono reali, è necessaria una quantità infinita di informazione classica per descriverle.

Di conseguenza è possibile affermare che possedere un qubit di informazione quantistica equivale a possedere  $2 \cdot \infty$  bit di informazione classica.

Un risultato fondamentale nell'ambito della teoria dell'informazione quantistica, ed in particolare del teletrasporto (vedere i paragrafi (2.1) e (2.3)), è la capacità di quantificare l'informazione quantistica media emessa da una sorgente. Per definire questa grandezza cominciamo con l'analizzare il concetto corrispondente a livello classico, per poi estenderlo all'ambito quantistico.

La teoria dell'informazione classica è nota come *teoria dell'informazione di Shannon*, nella quale si assume che la conoscenza di una certa sequenza di bit classici fornisca una determinata quantità di informazione classica.

Questa informazione classica può essere quantificata, come di seguito spiegato.

Si cominci con il considerare un sistema che possa trovarsi in  $M$  stati differenti, equiprobabili e statisticamente indipendenti.

Conoscere in quale tra questi stati esso si trovi, richiede una quantità di informazione classica  $Q$  (misurata in bit ed indipendente dallo stato) definita come [7]:

$$Q \equiv \log_2 M \quad (5.5)$$

In generale, se gli  $M$  stati del sistema non sono equiprobabili, ma sono comunque statisticamente indipendenti, la quantità di informazione classica  $Q_i$ , con  $i \in \{1; 2; \dots; M\}$ , associata a ciascuno stato "  $i$  ", e cioè la quantità di informazione classica che si riceve nel sapere che il sistema si trova in quello stato "  $i$  " particolare, è funzione della probabilità  $p_i$  che ha il sistema di trovarsi proprio in quello stato "  $i$  ", secondo la seguente definizione:

$$Q_i \equiv \log_2 \frac{1}{p_i} \quad (5.6)$$

Siccome  $p_i$  varia da stato a stato, allora anche  $Q_i$  sarà variabile.

Si definisce allora in tal caso una quantità di informazione classica media (la media è quella pesata sulle probabilità  $p_j$ ) per stato, denominata *entropia* [4][7]:

$$H \equiv -\sum_{i=1}^M p_i \log_2 p_i \quad (5.7)$$

Questa, più precisamente, è denominata *entropia di Shannon*, e si misura in bit/stato. In questa formula si assume per convenzione che  $0 \log_2 0 = 0$ .

Intuitivamente questa convenzione è giustificata dal fatto che sembra ragionevole supporre che uno stato che non potrà mai essere occupato (cioè avente  $p=0$ ) non debba contribuire a determinare il valore dell'entropia del sistema. Più formalmente, invece, questa convenzione è giustificata dal fatto che  $\lim_{x \rightarrow 0} (x \log_2 x) = 0$ .

Si può dimostrare che, per un sistema di  $M$  stati statisticamente indipendenti, il massimo dell'entropia classica si ottiene in condizioni di equiprobabilità, cioè che:

$$H_{MAX} = H(p_1 = p_2 = \dots = p_M = 1/M) = \log_2 M \quad (5.8)$$

Quindi, se gli  $M$  stati del sistema non sono equiprobabili, si avrà  $H < H_{MAX}$  e quindi la capacità informativa del sistema (visto come sorgente di informazione) risulta minore rispetto al caso di equiprobabilità.

Si dice quindi che, nel caso di  $H < H_{MAX}$ , il sistema presenta un certo grado di ridondanza  $R_H$ , di seguito definita [7]:

$$R_H \equiv 1 - \frac{H}{H_{MAX}} \quad (5.9)$$

Quindi avere  $R_H < 1$ , vuol dire non ricevere la massima informazione classica dal sistema.

A livello quantistico, estendendo la definizione di entropia di Shannon, si introduce la cosiddetta *entropia di von Neumann* [4], che rappresenta l'entropia quantistica, ovvero la quantità di informazione quantistica media, di un sistema quantistico descritto da una matrice densità  $\rho$  (e cioè di un sistema che è descritto da un ensemble di stati puri statisticamente indipendenti  $\{p_j; |\psi_j\rangle\}$  tale che  $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$ , dove  $\sum_j p_j = 1$ ), avente autovalori  $\lambda_i$ :

$$S \equiv -\text{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i \quad (5.10)$$

Se si lavora poi in uno spazio  $M$ -dimensionale, si ottiene che:

$$S_{MAX} = S(\lambda_1 = \lambda_2 = \dots = \lambda_M = 1/M) = \log_2 M \quad (5.11)$$

In modo analogo al caso classico, si definisce ora la ridondanza nel caso quantistico, indicata con il simbolo  $R_S$ :

$$R_S \equiv 1 - \frac{S}{S_{MAX}} \quad (5.12)$$

L'entropia di von Neumann è molto importante nell'ambito della concentrazione dell'entanglement (vedere il paragrafo (2.3)).

Anche il concetto di ridondanza è molto importante, in quanto permette di comprendere l'idea che sta alla base della correzione, classica o quantistica, degli errori (vedere i paragrafi (2.1) e (2.2)).

### 5.3 Porte quantistiche X, Y, Z, H e CNOT

Un altro prerequisito necessario nello studio del teletrasporto quantistico è il concetto di *porta quantistica* [4].

Questa non è altro che l'estensione al caso quantistico delle porte logiche note dalla teoria classica e che lavorano con l'algebra booleana, utilizzate ampiamente nel campo dell'elettronica digitale.

Le porte quantistiche lavorano però sui qubit.

Quindi, dati uno o più qubit in ingresso a queste porte quantistiche, esse forniscono in uscita uno o più qubit, dipendenti, tramite qualche funzione logica, dagli stati quantistici d'ingresso.

Di seguito vengono riportate le porte utilizzate nel teletrasporto quantistico.

Cominciamo con il cosiddetto *inverter*, ovvero la *porta NOT*, una porta ad un solo ingresso e ad una sola uscita, che rappresenta l'estensione quantistica dell'inverter classico, e che solitamente è indicata come *porta X*:

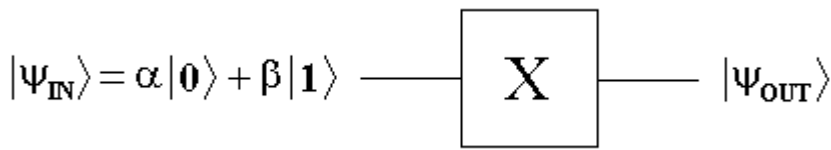


Figura 5.1

dove lo schema va letto, per convenzione, da sinistra a destra e ricordando che le linee in ingresso ed in uscita dal blocco rappresentano i fili del circuito quantistico, che non corrispondono però necessariamente a dei fili reali: possono corrispondere invece a dei passaggi di tempo o a delle particelle che si muovono da un punto ad un altro nello spazio.

La tavola della verità della NOT classica riporta le operazioni  $0 \rightarrow 1$  ed  $1 \rightarrow 0$ , ovvero la porta NOT classica è in grado di intercambiare gli stati 0 ed 1.

La NOT quantistica è anch'essa in grado, per analogia, di intercambiare gli stati  $|0\rangle$  ed  $|1\rangle$ , ma la tavola della verità classica non ci dice cosa succede alle loro combinazioni lineari, situazione comunque possibile nel caso quantistico. Per evitare paradossi come viaggi nel tempo, o comunicazioni superluminali, o violazioni della seconda legge della termodinamica, si dimostra che la porta NOT quantistica, ovvero l'operatore  $X$  che la descrive, deve avere un comportamento lineare.

Quindi essa deve agire come di seguito mostrato:

$$|\psi_{OUT}\rangle = X|\psi_{IN}\rangle = X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle \quad (5.13)$$

Visto che l'operatore  $X$  agisce in modo lineare, esso può essere rappresentato in forma matriciale, nel modo seguente, rispetto alla base  $\{|0\rangle;|1\rangle\}$ :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (5.14)$$

Come si può osservare, la matrice  $X$  non è altro che la matrice  $\sigma_x$  di Pauli, rappresentata nella base degli autostati della matrice di Pauli  $\sigma_z$ .

Si osserva inoltre che siccome sia lo stato d'ingresso che quello d'uscita della porta devono avere norma pari ad 1 ai fini dell'interpretazione probabilistica, vuol dire che l'operatore che descrive questa porta deve essere in grado di conservare la norma.

Dall'analisi matematica è noto che gli operatori che possiedono questa proprietà sono tutti e soli gli operatori  $U$  tali che  $UU^\dagger = I$ , che sono definiti *operatori unitari*.

Per essi si ha quindi che  $U^{-1} = U^\dagger$ , e siccome  $U^\dagger$  esiste sempre, vuol dire che questi operatori sono sicuramente invertibili (o reversibili), ed inoltre anche il loro inverso è un operatore unitario.

Comunque il requisito di unitarietà è l'unica condizione che deve essere soddisfatta da una porta quantistica.

Un'altra porta utilizzata nel teletrasporto quantistico è la cosiddetta *porta Z*, anch'essa ad un solo ingresso e ad una sola uscita, la cui rappresentazione matriciale nella base  $\{|0\rangle;|1\rangle\}$  è la seguente:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (5.15)$$

Questa porta presenta quindi la caratteristica di lasciare inalterato lo stato  $|0\rangle$ , e di cambiare lo stato  $|1\rangle$  nello stato  $-|1\rangle$ .

Si osserva inoltre che la matrice  $Z$  non è altro che la matrice  $\sigma_z$  di Pauli, rappresentata nella base dei suoi autostati.

Nel teletrasporto quantistico, anche se in alcuni testi non è esplicitato, viene utilizzata anche la cosiddetta *porta Y*, anch'essa ad un solo ingresso e ad una sola uscita, la cui rappresentazione matriciale nella base  $\{|0\rangle;|1\rangle\}$  è la seguente:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (5.16)$$

La sua funzione è quella di trasformare lo stato  $|0\rangle$  nello stato  $i|1\rangle$ , e lo stato  $|1\rangle$  nello stato  $-i|0\rangle$ .

Il motivo per il quale questa porta non viene sempre menzionata in modo esplicito nel teletrasporto quantistico, è che la matrice  $Y$  può essere espressa tramite il prodotto matriciale di  $X$  con  $Z$ , ovvero  $-iY=XZ$ .

In tal modo è sufficiente menzionare solamente le porte  $X$  e  $Z$ .

Si osserva poi che la matrice  $Y$  non è altro che la matrice  $\sigma_Y$  di Pauli, rappresentata nella base degli autostati della matrice di Pauli  $\sigma_Z$ .

Le porte  $I$ ,  $X$ ,  $Y$  e  $Z$  vengono anche chiamate *porte di Pauli* e permettono di definire il cosiddetto *gruppo di Pauli*  $G_n$  su  $n$  qubit, cioè costituito da operatori che operano su  $n$  qubit.

Nel caso particolare di  $n=1$ , il gruppo di Pauli è definito come  $G_1 = \{\pm I; \pm iI; \pm X; \pm iX; \pm Y; \pm iY; \pm Z; \pm iZ\}$ , dove  $i$  rappresenta sempre l'unità immaginaria.

Questo set di matrici forma un gruppo sotto l'operazione di prodotto matriciale.

In generale, invece, il gruppo di Pauli  $G_n$  è definito come l'insieme di tutti i prodotti tensoriali  $n$ -esimi delle porte di Pauli, ed ancora moltiplicati per i fattori  $\pm 1, \pm i$ .

Esiste un'ultima porta quantistica ad un solo ingresso e ad una sola uscita utile, anche se non necessaria, nella comprensione del teletrasporto quantistico (e comunque trattata anche nel paragrafo 4.3), che è la cosiddetta *porta di Hadamard*, indicata attraverso l'operatore  $H$ , la cui rappresentazione matriciale nella base  $\{|0\rangle;|1\rangle\}$  è di seguito mostrata:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (5.17)$$

La sua funzione è quella di trasformare lo stato  $|0\rangle$  nello stato  $(|0\rangle+|1\rangle)/\sqrt{2}$ , e lo stato  $|1\rangle$  nello stato  $(|0\rangle-|1\rangle)/\sqrt{2}$ .

L'ultima delle porte quantistiche prese in considerazione è la cosiddetta *porta controlled-NOT* (abbreviata in CNOT), che è a due ingressi, il control qubit ed il target qubit, e a due uscite:

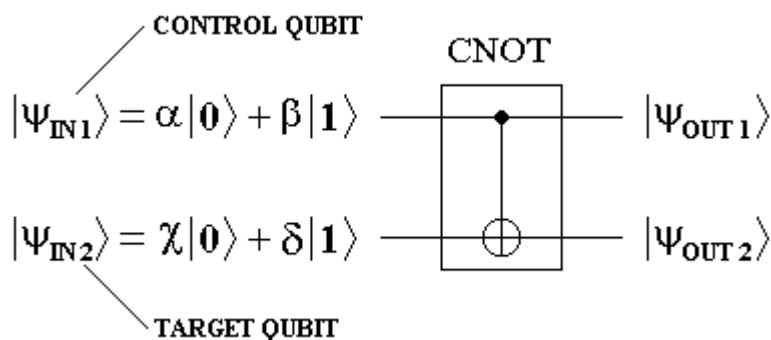


Figura 5.2

La CNOT, sugli stati di base, agisce nel seguente modo:  $|00\rangle \rightarrow |00\rangle$ ;  $|01\rangle \rightarrow |01\rangle$ ;  $|10\rangle \rightarrow |11\rangle$ ;  $|11\rangle \rightarrow |10\rangle$ .

In altri termini, la prima uscita è sempre uguale al valore del control qubit, mentre la seconda è uguale al valore del target qubit solo quando il control qubit si trova nello stato zero, mentre in caso contrario la seconda uscita si trova nella negazione dello stato del target qubit.

Nel caso invece in cui sia il control qubit che il target qubit si trovino in uno stato di combinazione lineare, basta estendere il comportamento della CNOT appena visto nel caso degli stati di base, ipotizzando che questa porta si comporti in modo lineare rispetto ad entrambi i qubit d'ingresso:

$$\begin{aligned}
|\psi_{OUT}\rangle &= CNOT(|\psi_{IN1}\rangle; |\psi_{IN2}\rangle) = CNOT(|\psi_{IN1}\rangle \otimes |\psi_{IN2}\rangle) = CNOT\left[\left(\alpha|0\rangle + \beta|1\rangle\right)\left(\chi|0\rangle + \delta|1\rangle\right)\right] = \\
&= CNOT(\alpha\chi|00\rangle + \alpha\delta|01\rangle + \beta\chi|10\rangle + \beta\delta|11\rangle) = \alpha\chi CNOT|00\rangle + \alpha\delta CNOT|01\rangle + \beta\chi CNOT|10\rangle + \\
&+ \beta\delta CNOT|11\rangle = \alpha\chi|00\rangle + \alpha\delta|01\rangle + \beta\chi|11\rangle + \beta\delta|10\rangle
\end{aligned} \tag{5.18}$$

La rappresentazione matriciale della CNOT nella base  $\{|00\rangle; |01\rangle; |10\rangle; |11\rangle\}$  è la seguente:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{5.19}$$

Anche la porta CNOT, come la porta H, è utile ma non necessaria nella comprensione del teletrasporto quantistico (e comunque viene trattata anche nel paragrafo 4.3).

L'importanza delle porte H e CNOT nelle applicazioni del teletrasporto è dovuta al fatto che esse sono parte dei cosiddetti *set universali*, ovvero di quegli insiemi formati da un numero finito di operatori aventi la caratteristica che ciascuna porta quantistica a più ingressi ed a più uscite possa essere riprodotta da una opportuna combinazione finita di porte appartenenti a questo insieme.

E' importante osservare che non esiste un unico set universale.

Un esempio è rappresentato dall'insieme costituito da tutte le porte ad un qubit, e quindi anche H, e dalla porta CNOT.

Un set universale alternativo è invece costituito dalla porta H, dalla cosiddetta *porta fase* (cioè l'operatore  $\text{diag}(1, 1, 1, i)$ ), dalla porta CNOT ed infine dalla cosiddetta *porta  $\pi/8$*  (la cui funzione è quella di incrementare di  $\pi/4$  radianti l'angolo  $\phi$  che compare nell'espressione (5.1) del generico qubit singolo).

Inoltre, in quest'ultimo set, l'operatore  $\pi/8$  può essere sostituito dalla cosiddetta *porta di Toffoli* [4] (cioè dalla porta controlled-controlled-NOT) ottenendo un altro set universale.

## 5.4 Fedeltà classica e quantistica

Nell'ambito della teoria classica dell'informazione, la fedeltà rappresenta una grandezza in grado di quantificare la distanza, cioè la differenza, tra due distribuzioni di probabilità [4].

Supponiamo cioè di avere due sistemi distinti, che condividano lo stesso insieme di stati "i", con  $i \in \{1; 2; \dots; M\}$ .

Questo significa che ciascuno degli stati di questo insieme può essere assunto sia dal primo che dal secondo sistema. Però ipotizziamo che ciascuno di questi stati abbia una probabilità differente di verificarsi nel primo sistema, rispetto al secondo.

Si ottengono in tal modo due distribuzioni di probabilità, in generale differenti, una per ciascuno dei due sistemi, che indichiamo con  $\{p_i\}$  e  $\{q_i\}$ .

Si definisce quindi, attraverso la seguente espressione, la fedeltà delle due distribuzioni di probabilità  $\{p_i\}$  e  $\{q_i\}$ , come una misura della distanza tra le due distribuzioni stesse:

$$F(\{p_i\}; \{q_i\}) \equiv \sum_{i=1}^M \sqrt{p_i q_i} \tag{5.20}$$

Sebbene la fedeltà venga utilizzata per misure di distanza, essa non è una metrica, dato per esempio che, quando  $\{p_i\} = \{q_i\}$ , si ottiene che  $F(\{p_i\}; \{q_i\}) = \sum_i p_i = 1$ , mentre una metrica, applicata a due grandezze uguali, deve dare zero come risultato.

Comunque la fedeltà non è l'unica misura di distanza possibile.

Passiamo ora a definire l'estensione quantistica della fedeltà.

Dati due stati quantistici aventi matrici densità  $\rho$  e  $\sigma$  rispettivamente, la loro fedeltà è definita nel modo seguente:

$$F(\rho; \sigma) \equiv \text{tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}} \quad (5.21)$$

dove bisogna ricordare che, dato un generico operatore lineare  $A$  di autovalori  $a$  ed autostati  $|a\rangle$ , e quindi tale che

$A = \sum_a a |a\rangle\langle a|$ , allora la grandezza  $f(A)$ , con  $f$  funzione generica, è definita come  $f(A) = \sum_a f(a) |a\rangle\langle a|$ .

Si osserva che  $F \in [0; 1]$  e che, in particolare,  $F=1$  quando  $\rho=\sigma$ , mentre  $F=0$  quando  $\rho$  e  $\sigma$  sono due stati tra loro ortogonali.

La fedeltà è molto utile nel determinare quanto lo stato quantistico da teletrasportare di Alice risulterà simile allo stato ricostruito da Bob (vedere il paragrafo 2.3), il che fornisce quindi una misura quantitativa del grado di affidabilità raggiunto nell'operazione.

## Bibliografia

- [1] Bennett, C. H. *et al.*, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* 70, 1895-1899 (1993).
- [2] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger, Experimental quantum teleportation. *Nature*, Vol. 390, 575-579, 11 December (1997).
- [3] N. J. Cerf, N. Gisin, and S. Massar, Classical Teleportation of a Quantum Bit. *Phys. Rev. Lett.*, Vol. 84, N. 11, 2521-2524, 13 March (2000).
- [4] Michael A. Nielsen & Isaac L. Chuang, Quantum Computation and Quantum Information. Cambridge, UNIVERSITY PRESS.
- [5] M. Steiner, quant-ph/9902014.
- [6] G. Brassard, R. Cleve, and A. Tapp, *Phys. Rev. Lett.* 83, 1874 (1999).
- [7] A. CECCONELLI, A. TOMASSINI, LE TELECOMUNICAZIONI, TECNICHE DI TRASMISSIONE E SISTEMI DI TELECOMUNICAZIONI-MISURE. CALDERINI.
- [8] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, Benjamin Schumacher, Concentrating Partial Entanglement by Local Operations. ArXiv:quant-ph/9511030 v1 21 Nov 1995.
- [9] Michael Lacroix, ENTANGLEMENT AS A RESOURCE. 96066769 C&O 639.
- [10] M. A. Nielsen, E. Knill & R. Laflamme, Complete quantum teleportation using nuclear magnetic resonance. *Nature*, Vol. 396, 52-55, 5 November (1998).
- [11] Daniel Gottesman & Isaac L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, Vol. 402, 390-393, 25 November (1999).