

# Comunicazioni ottiche quantistiche

Danjel Qyteza  
Relatore Prof. R. Corvaja

26 aprile 2010

# Sommario

Lo scopo sostanziale di questa tesina consiste nell'introdurre le comunicazioni quantistiche e nel constatare la differenza di prestazioni in termini di probabilità di errore, fra i sistemi quantistici binari ed i rispettivi sistemi ottici "classici". Si analizzano inoltre le possibili realizzazioni di ricevitori quantistici binari.

Nel primo capitolo seguirà una breve introduzione sulla teoria della meccanica quantistica e sugli sviluppi ed applicazioni in genere.

Nel secondo capitolo verrà presentato un'analisi dei sistemi ottici con le modulazioni OOK e 2-PSK.

Nel terzo capitolo si darà un'introduzione agli elementi della meccanica quantistica e si studierà un sistema quantistico con modulazione OOK e 2-PSK. Ci sarà anche un confronto con i rispettivi sistemi ottici classici.

Nel quarto capitolo si analizzeranno due ricevitori quantistici, quali il ricevitore di Kennedy e di Dolinar.

Nel ultimo capitolo seguiranno, infine, le conclusioni.

# Indice

<b>1</b>	<b>Introduzione</b>	<b>3</b>
<b>2</b>	<b>Comunicazioni ottiche classiche</b>	<b>4</b>
2.1	Sistemi classici . . . . .	4
2.2	Sistemi ottici con modulazione OOK . . . . .	5
2.3	Sistemi ottici con modulazione 2-PSK . . . . .	6
2.3.1	Ricevitore superomodina . . . . .	6
2.3.2	Ricevitore omodina . . . . .	7
<b>3</b>	<b>Comunicazioni ottiche quantistiche</b>	<b>9</b>
3.1	Elementi di meccanica quantistica . . . . .	9
3.1.1	Dal bit al qubit . . . . .	11
3.1.2	Rappresentazione quantistica della radiazione emessa da un laser . . . . .	12
3.2	Formulazione della decisione quantistica . . . . .	12
3.2.1	Misure proiettive . . . . .	13
3.2.2	Misure generalizzate (POVM) . . . . .	13
3.2.3	Sistema quantistico e ottimizzazione del ricevitore binario . . . . .	14
3.3	Sistema quantistico con modulazione OOK . . . . .	18
3.4	Sistema quantistico con modulazione 2PSK . . . . .	20
<b>4</b>	<b>Realizzazione di ricevitori quantistici</b>	<b>22</b>
4.1	Il ricevitore di Kennedy . . . . .	22
4.2	Il ricevitore di Dolinar . . . . .	23
<b>5</b>	<b>Conclusioni</b>	<b>25</b>
	<b>Bibliografia</b>	<b>26</b>

# Capitolo 1

## Introduzione

La teoria della meccanica quantistica ha alle spalle oltre cento anni di vita e non è mai stata smentita dalla relativa verifica pratica. Con essa si apre uno scenario che fa prevedere vaste applicazioni nell'area dell'ingegneria dell'informazione ed in particolare nelle *telecomunicazioni quantistiche* (QTLC).

Nei sistemi QTLC si considerano sempre sistemi che operano alle frequenze ottiche (per cui si parla di comunicazioni ottiche quantistiche) in quanto alle frequenze radio i fenomeni quantistici non risultano apprezzabili. I sistemi ottici quantistici presentano un netto guadagno di prestazioni rispetto ai sistemi ottici classici, in particolare in termini di probabilità di errore. Un altro vantaggio molto importante consiste nel fatto che l'informazione quantistica non può essere "doppiata" e quindi non può essere intercettata senza che il destinatario ne venga automaticamente a conoscenza (*no cloning theorem*).

Con la tecnologia attuale la teoria delle comunicazioni quantistiche è di difficile implementazione, in particolare il problema si concentra nella possibilità di realizzare il ricevitore quantistico. La realizzazione di un buon ricevitore quantistico teorizzato dai lavori pionieristici di Helstrom costituisce l'ultimo passaggio per la successiva implementazione pratica di un sistema di comunicazione quantistica. Esistono molti tipi di ricevitore quantistico, alcuni di essi raggiungono l'ottimalità, costituita dal cosiddetto limite di Helstrom, altri si avvicinano ad essa e per questo vengono detti sub-ottimali. I ricevitori quantistici più studiati e praticamente implementati sono il ricevitore di Kennedy e il ricevitore di Dolinar.

## Capitolo 2

# Comunicazioni ottiche classiche

### 2.1 Sistemi classici

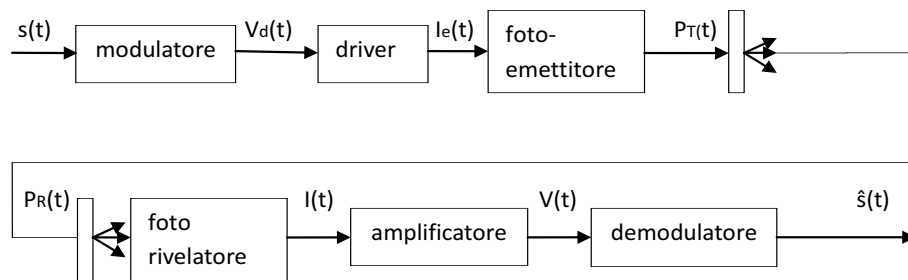


Figura 2.1: Sistema di trasmissione su fibra ottica.

Per sistemi classici si intendono i sistemi di trasmissione ottica basati su una modulazione generica, dove il messaggio di informazione è affidato a una grandezza ottica per cui essi prevedono una conversione elettro-ottica ed una successiva conversione ottico-elettrica e la rivelazione non tiene conto delle caratteristiche quantistiche (modello di Glauber) della grandezza ottica. In tali sistemi, una modulazione M-aria è specificata da  $M$  forme d'onda complesse

$$\gamma_{\alpha_1}(t), \gamma_{\alpha_2}(t), \dots, \gamma_{\alpha_M}(t) \quad (2.1)$$

di durata limitata nell'intervallo  $[0, T]$  con la regola che se  $a \in \mathcal{A}$  è il simbolo della sorgente, il modulatore forma un segnale con involuppo complesso

$$c(t) = \gamma_a(t) \quad 0 \leq t < T.$$

Con la successione di simboli  $a_n$  l'espressione completa dell'involuppo complesso diventa

$$c(t) = \sum_{n=-\infty}^{+\infty} \gamma_{a_n}(t - nT)$$

dalla quale si ottiene il segnale modulato dato da

$$v(t) = \Re[c(t)e^{i2\pi ft}]$$

dove  $f$  è la frequenza della portante.

## 2.2 Sistemi ottici con modulazione OOK

Nelle modulazioni On-off keying (OOK) si associa al simbolo  $a=0$  una potenza nulla ed al simbolo  $a=1$  una potenza positiva che raccoglie in un periodo di cifra un numero medio di fotoni  $N_R(1) = 2N_R$ , dove  $N_R$  è il numero medio di fotoni per bit. Il ricevitore a conteggio di fotoni utilizza il criterio di decisione per determinare il simbolo stimato  $\hat{a}$

$$\hat{a} = \begin{cases} 0 & \text{se } n = 0 \\ 1 & \text{se } n \geq 1 \end{cases} \quad (2.2)$$

dove  $n$  è il numero di fotoni conteggiati in un periodo di cifra. Si ha che con la trasmissione del simbolo  $a = 0$  il numero di arrivi è nullo,  $n = 0$ , e si ha sempre una decisione corretta, pertanto

$$P_e(0) = 0. \quad (2.3)$$

Con il simbolo  $a = 1$  il numero di arrivi  $n$  è una variabile aleatoria di Poisson con media  $N_R(1)$  e quindi con distribuzione di massa (condizionata)

$$p_n(k|1) = e^{-N_R(1)} \frac{N_R(1)^k}{k!}, \quad k, 0, 1, \dots$$

Si ha errore quando  $n = 0$  e questo accade con probabilità

$$P_e(1) = e^{-N_R(1)} = e^{-2N_R} \quad (2.4)$$

Assumendo i simboli equiprobabili quindi ( $q_0 = q_1 = \frac{1}{2}$ ) si ottiene infine

$$P_e = \frac{1}{2}P_e(0) + \frac{1}{2}P_e(1) = \frac{1}{2}e^{-2N_R} \quad (2.5)$$

Questa probabilità rappresenta il limite quantico poichè dà la minima probabilità di errore che si può avere con una modulazione *OOK* utilizzando un contatore di fotoni, questo perchè il criterio di decisione adottato (2.2) è ottimale. Considerando il legame tra la probabilità di errore e il numero di fotoni per bit troviamo che fissando una  $P_e = 10^{-9}$  si ottiene la sensibilità del ricevitore ideale (*limite quantico*):

si ha  $N_{R_{min}} = 10$  fotoni per bit.

## 2.3 Sistemi ottici con modulazione 2-PSK

Un'onda monocromatica a frequenza  $f$  è rappresentabile mediante un segnale sinusoidale

$$x_0(t) = X_0 \cos(2\pi ft + \phi_0) \quad (2.6)$$

dove  $X_0$  è una tensione opportunamente normalizzata in modo che la corrispondente potenza risulti

$$P = X_0^2.$$

Nella modulazione 2-PSK la portante (2.6) viene modulata nella forma

$$x_R(t) = X_0 \cos(2\pi ft + a_0\pi), \quad 0 < t < T \quad (2.7)$$

dove la potenza è costante  $P = X_0^2$  indipendentemente dal simbolo  $a_0$ .

### 2.3.1 Ricevitore superomodina

Si ipotizza di avere in ricezione un oscillatore locale che produca una radiazione  $x_L(t)$  con la stessa ampiezza, frequenza e fase del segnale trasmesso, cioè

$$x_L(t) = X_L \cos(2\pi ft) \quad \text{con} \quad X_L = X_0. \quad (2.8)$$

Aggiungendo questa portante locale al segnale modulato si ottiene

$$x(t) = X_0 \cos(2\pi ft + a_0\pi) + X_0 \cos(2\pi ft) = \begin{cases} 2X_0 \cos(2\pi ft) & a_n = 0 \\ 0 & a_n = 1. \end{cases} \quad (2.9)$$

Si suppone di avere a disposizione un contatore ideale di fotoni. Negli intervalli di cifra in cui viene trasmesso  $a_n = 0$  entra la potenza  $(2X_0)^2 = 4P_R$ , mentre entra potenza nulla quando  $a_n = 1$ . Quindi il numero medio di fotoni in un periodo di cifra risulta rispettivamente

$$N_x(0) = \frac{4P_R T}{hf}, \quad N_x(1) = 0 \quad (2.10)$$

dove  $h = 6.63 \cdot 10^{-34} \text{ Js}$  è la costante di Planck. Si prende la decisione in base al numero di arrivi  $n$  secondo la regola

$$\begin{cases} n = 0 \longrightarrow \hat{a} = 1 \\ n \geq 1 \longrightarrow \hat{a} = 0 \end{cases}$$

In modo analogo alla (2.5) si ottiene la probabilità di errore

$$P_e = \frac{1}{2} P_e(0) = \frac{1}{2} e^{-N_x(0)} \quad (2.11)$$

Si nota che il numero medio di fotoni per bit in ricezione prima dell'aggiunta della portante è  $N_R = P_R T / (hf)$ , che risulta essere un quarto di  $N_x(0)$ , tale che (2.11) diventa

$$P_e = \frac{1}{2} e^{-4N_R}. \quad (2.12)$$

Si ha perciò un miglioramento rispetto alla modulazione *OOK*, di un fattore due e la sensibilità limite diventa

$$N_{R_{min}} \simeq 5 \text{ fotoni/bit}$$

che rappresenta il limite superquantico. Il miglioramento sta nel fatto che la potenza introdotta dall'oscillatore locale crea una situazione più favorevole ad una decisione corretta.

### 2.3.2 Ricevitore omodina

Il risultato ottenuto con il ricevitore superomodina è poco realistico per il fatto che la portante introdotta dall'oscillatore locale abbia la stessa ampiezza del segnale ricevuto. Nella ricezione omodina si considera che la portante introdotta abbia un'ampiezza  $X_L$  molto maggiore di quella del segnale ricevuto. Si ha il segnale

$$x(t) = X_0 \cos(2\pi ft + a_0\pi) + X_L \cos(2\pi ft) \quad (2.13)$$

con

$$X_L \gg X_0. \quad (2.14)$$

Dalla scomposizione  $\cos(2\pi ft + a_n\pi) = \cos(\pi a_n) \cos(2\pi ft)$  la potenza risulta

$$P_x(t) = (X_0 \cos(\pi a_n) + X_L)^2 = X_0^2 + X_L^2 + 2X_0X_L \cos(\pi a_n). \quad (2.15)$$

Applicando questa potenza ad un contatore di fotoni si ottiene un numero di arrivi  $n$  in un periodo di cifra, che può essere scomposto nella forma

$$n = \bar{n}(a_0) + u$$

dove  $\bar{n}(a_0) = E[N|a_0]$  è il segnale utile e la fluttuazione  $u$  è il rumore granulare. Il numero medio di fotoni  $E[N|a_0]$  risulta uguale alla intensità fotonica  $P_x(t)/hf$  integrata su  $(0, T)$ , si ha

$$\bar{n}(a_0) = E[N|a_0] = K(X_0^2 + X_L^2 + 2X_0X_L \cos(\pi a_n)) \quad (2.16)$$

con  $K = T/hf$ , quindi si può scrivere

$$\bar{n}(a_0) = V_0 + A_0 \cos(\pi a_0) = V_0 \pm A_0 \quad (2.17)$$

dove  $V_0 = K(X_0^2 + X_L^2)$  è un termine di polarizzazione mentre  $\pm A = \pm 2KX_0X_L$  è la parte che dipende dai simboli:  $+A_0(-A_0)$  quando  $a_0 = 0(a_0 = 1)$ . La varianza risulta

$$\sigma_n^2(a_0) = E[n|a_0] = K(X_0^2 + X_L^2 + 2X_0X_L \cos(\pi a_0)) \simeq KX_L^2 = N_L \quad (2.18)$$



dove dall'ipotesi  $X_L \gg X_0$  si deduce il penultimo passaggio. Infine la decisione sul simbolo trasmesso  $a_0$  va presa in base al campione

$$n = V_0 + A_0 \cos(\pi a_0) + u$$

dove il rumore  $u$  può essere considerato gaussiano con varianza praticamente costante dato dalla (2.18). Ponendo la soglia dell'elemento di decisione a  $V_0$  si ottiene

$$P_e = Q\left(\frac{A_0}{\sigma_n}\right)$$

. Tenendo conto infine che la funzione  $Q(x)$  per grandi argomenti è ottimamente approssimata dalla  $Q(x) \cong e^{-x^2/2}$ , si ottiene

$$P_e = e^{-2N_R} \tag{2.19}$$

trovando così il limite quantico ( $N_R = 10$  fotoni per bit per garantire una probabilità di errore  $P_e = 10^{-9}$ ), anziché il limite superquantico.

## Capitolo 3

# Comunicazioni ottiche quantistiche

### 3.1 Elementi di meccanica quantistica

La teoria delle QTLC si sviluppa negli spazi di Hilbert sui numeri complessi. Ad ogni sistema fisico chiuso va associato uno spazio di Hilbert  $\mathcal{H}$  di dimensioni opportune sul corpo dei numeri complessi  $\mathbb{C}$ , detto spazio degli stati. In ogni istante della sua evoluzione il sistema è completamente specificato da uno stato  $|\psi\rangle$  dato da un vettore unitario di  $\mathcal{H}$ . La descrizione di uno spazio di Hilbert è del tutto astratta in quanto non si danno indicazioni su come associarlo ad un sistema fisico, l'unica specificazione è di tipo matematico e cioè che  $|\psi\rangle$  deve essere unitario, verificare quindi la condizione di normalizzazione  $\langle\psi|\psi\rangle = 1$ .

Lo stato di uno spazio  $\mathcal{H}$  si interpreta come un vettore colonna di dimensione anche infinita, e viene scritto come visto, con il simbolo

$$|\psi\rangle \tag{3.1}$$

secondo la notazione di Dirac e viene detto *ket*. Il suo coniugato trasposto  $|\psi\rangle^*$  va interpretato come vettore riga e si indica con

$$\langle\psi| = |\psi\rangle^* \tag{3.2}$$

e viene detto *bra*. Il prodotto interno tra due vettori  $|x\rangle$  e  $|y\rangle$  si indica nella forma

$$\langle x|y\rangle.$$

Ai fini della decisione quantistica occorre dare alcune utili definizioni.

#### Operatori lineari

Un operatore lineare  $\mathbf{A}$  è definito come una funzione

$$\mathbf{A} : \mathcal{H} \rightarrow \mathcal{H}.$$

Se  $|x\rangle \in \mathcal{H}$ , l'operatore  $\mathbf{A}$  restituisce il vettore

$$|y\rangle = \mathbf{A}|x\rangle \quad \text{con } |y\rangle \in \mathcal{H}$$

L'operatore  $\mathbf{A}$  è lineare se vale

$$\mathbf{A}(a_1|x1\rangle + a_2|x2\rangle) = a_1\mathbf{A}|x1\rangle + a_2\mathbf{A}|x2\rangle$$

per ogni  $|x1\rangle, |x2\rangle \in \mathcal{H}$  e  $a_1, a_2 \in \mathbb{C}$ .

È possibile associare ad ogni operatore lineare  $\mathbf{A}$  una matrice quadrata di dimensioni  $n \times n$  se lo spazio di Hilbert ha dimensione  $n$ , oppure di dimensioni infinite se  $\mathcal{H}$  ha dimensioni infinite.

### Autovalori, autovettori e la traccia di un operatore

Un autovalore  $\lambda$  di un dato operatore  $\mathbf{A}$  è un numero complesso tale per cui esista un vettore  $|x_0\rangle \in \mathcal{H}$  diverso da zero, che soddisfa

$$\mathbf{A}|x_0\rangle = \lambda|x_0\rangle \quad |x_0\rangle \neq 0$$

dove il vettore  $|x_0\rangle$  è detto autovettore corrispondente all'autovalore  $\lambda$ .

La traccia di un operatore  $\mathbf{A}$  è data dalla somma degli elementi diagonali della sua rappresentazione matriciale

$$Tr(\mathbf{A}) = \sum_i \langle b_i | \mathbf{A} | b_i \rangle. \quad (3.3)$$

dove i  $b_i$  sono gli elementi di una base ortonormale di  $\mathcal{H}$ .

Vale la seguente identità

$$\langle u | \mathbf{A} | u \rangle = Tr(\mathbf{A} | u \rangle \langle u |) \quad (3.4)$$

dove  $|u\rangle$  è un vettore arbitrario e  $|u\rangle\langle u|$  è l'operatore dato dal prodotto esterno.

### Prodotto esterno e operatori elementari

Il prodotto esterno tra due vettori  $|x\rangle$  e  $|y\rangle$  si indica come

$$|x\rangle\langle y|$$

. Mentre il prodotto interno fra  $|x\rangle$  e  $|y\rangle$  restituisce un numero complesso, il prodotto esterno è un operatore. Attraverso il prodotto esterno possiamo rappresentare gli operatori elementari come

$$\mathbf{C} = |c_1\rangle\langle c_2|$$

al quale applicando un ket arbitrario  $|x\rangle \in \mathcal{H}$  si ottiene

$$\mathbf{C}|x\rangle = (|c_1\rangle\langle c_2|)|x\rangle = (\langle c_2|x\rangle)|c_1\rangle, \quad \text{per ogni } |x\rangle \in \mathcal{H}$$

ottenendo così un vettore proporzionale a  $|c_1\rangle$  con costante di proporzionalità data dal numero complesso  $k = \langle c_2|x\rangle$ . Una classe importante di operatori elementari si ottengono come

$$\mathbf{B} = |b\rangle\langle b|$$

che trasforma un ket arbitrario  $|x\rangle$  in un ket proporzionale a  $|b\rangle$ . Se  $|b\rangle$  è unitario allora  $|b\rangle\langle b|$  risulta essere un proiettore.

### Proiettori ortogonali

Un proiettore  $\mathbf{P} : \mathcal{H} \rightarrow \mathcal{H}$  è un operatore hermitiano idempotente, cioè vale

$$\mathbf{P}^* = \mathbf{P}, \quad \mathbf{P}^2 = \mathbf{P}$$

e quindi  $\mathbf{P}^n = \mathbf{P}$  per ogni  $n \geq 2$ . Si ha per esempio che  $\mathbf{P}|s\rangle = |s\rangle$  e si dice che il sottospazio  $\mathcal{P}$  è invariante rispetto all'operatore  $\mathbf{P}$ . Si definisce *spettro dell'operatore*  $\mathbf{A}$  e si indica con  $\sigma(\mathbf{A})$  l'insieme di tutti gli autovalori dell'operatore stesso. Lo spettro di  $\mathbf{P}$  è sempre  $\sigma(\mathbf{P}) = \{0, 1\}$ .

### Scomposizione spettrale

Sia  $\mathbf{A}$  un operatore hermitiano sullo spazio di Hilbert  $\mathcal{H}$  e siano  $\{\lambda_i\}, i = 1, 2, \dots, k$  gli autovalori distinti di  $\mathbf{A}$ . Allora  $\mathbf{A}$  può essere univocamente scomposto nella forma

$$\mathbf{A} = \sum_{i=1}^k \lambda_i \mathbf{P}_i \tag{3.5}$$

dove i  $\{\mathbf{P}_i\}$  formano un sistema completo di proiettori ortogonali.

#### 3.1.1 Dal bit al qubit

Il bit costituisce la nozione fondamentale della teoria classica dell'informazione. Il suo stato è descritto da due possibili valori 0 e 1. Come il bit classico anche il qubit ha come stati possibili  $|0\rangle$  e  $|1\rangle$  ma a differenza del bit il qubit può essere anche in un qualunque stato combinazione lineare degli stati  $|0\rangle$  e  $|1\rangle$ :

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{3.6}$$

dove  $a$  e  $b$  sono numeri complessi. Il qubit viene inquadrato in uno spazio di Hilbert bidimensionale la cui base è formata da due vettori ortonormali qui indicati come  $|0\rangle$  e  $|1\rangle$ : sappiamo solo che se lo misuriamo abbiamo la probabilità  $|a|^2$  e  $|b|^2$  di trovarlo in uno dei due stati  $|0\rangle$  e  $|1\rangle$ . I numeri  $a$  e  $b$  devono verificare la condizione di normalizzazione

$$|a|^2 + |b|^2 = 1.$$

### 3.1.2 Rappresentazione quantistica della radiazione emessa da un laser

Nei sistemi QTLC l'informazione viene affidata alla radiazione monocromatica coerente prodotta da un laser (stati coerenti), la cui rappresentazione quantistica è dovuta a Glauber. Gli stati coerenti sono inquadrati in uno spazio di Hilbert di dimensioni infinite mediante una base ortonormale  $\{|n\rangle, n = 0, 1, 2, \dots\}$  dove gli stati  $n$  vengono chiamati autostati numero perché rappresentano il numero di fotoni contenuto nello stato  $|n\rangle$ . Secondo la rappresentazione di Glauber il generico stato coerente  $|\alpha\rangle$  è dato dalla combinazione lineare di autostati numero secondo l'espressione

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (3.7)$$

dove  $\alpha$  è un'ampiezza complessa che caratterizza il modo  $|\alpha\rangle$  e ha il significato

$$|\alpha|^2 = \text{numero medio di fotoni dello stato } |\alpha\rangle. \quad (3.8)$$

Secondo la (3.7) ad ogni punto  $\alpha$  del piano complesso viene associato uno stato coerente, il cui significato fisico è dato dalla (3.8). L'insieme degli stati secondo la rappresentazione di Glauber viene indicato con

$$\mathcal{G} = \{|\alpha\rangle, \alpha \in \mathbb{C}\}. \quad (3.9)$$

## 3.2 Formulazione della decisione quantistica

Lo stato di un sistema quantistico  $\mathcal{H}$  può essere definito e si scrive  $s = |\psi\rangle$  oppure può assumere un certo numero di valori  $|\psi_1\rangle, |\psi_2\rangle, \dots$  in un insieme  $\mathcal{S}$  supposto numerabile, con probabilità  $p_1, p_2, \dots$ , quindi con

$$p_i \geq 0 \quad e \quad \sum_i p_i = 1.$$

I due casi si possono interpretare come modello probabilistico in cui  $s = |\psi\rangle$  è l'evento certo oppure lo stato  $s$ , può essere visto come una variabile aleatoria discreta con probabilità  $P[s = |\psi_i\rangle] = p_i$ . Per descrivere un sistema il cui stato può assumere un certo numero di valori si definisce un operatore densità

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|.$$

L'operatore densità diventa

$$\rho = \sum_i |\psi_i\rangle \langle \psi_i|$$

per descrivere un sistema che si trova in uno stato certo. L'operatore densità ha le seguenti proprietà:

- 1)  $\rho$  è un operatore hermitiano,
- 2)  $\rho \geq 0$ , è un operatore semidefinito positivo,
- 3)  $Tr(\rho) = 1$ , ha traccia unitaria,
- 4)  $Tr(\rho^2) \leq 1$  e  $Tr(\rho^2) = 1$  se e solo se il sistema si trova in uno stato puro.

### 3.2.1 Misure proiettive

Una misura su un sistema quantistico  $\mathcal{H}$  si ottiene applicando un insieme ortogonale completo di proiettori  $\{\mathbf{\Pi}_i, i \in \mathcal{M}\}$  e l'alfabeto  $\mathcal{M}$  fornisce i possibili risultati della misura. Supposto che l'istante prima il sistema si trovi nello stato  $|\psi\rangle$ , la probabilità che la misura dia il risultato  $m = i \in \mathcal{M}$  è data da

$$P[m = i|\psi] = \langle \psi | \mathbf{\Pi}_i | \psi \rangle \quad (3.10)$$

che espresso mediante l'operatore densità con  $\rho = |\psi\rangle\langle\psi|$  si ottiene

$$P[m = i|\psi] = Tr(\rho \mathbf{\Pi}_i), \quad i \in \mathcal{M}. \quad (3.11)$$

### 3.2.2 Misure generalizzate (POVM)

Le misure quantistiche generalizzate vengono effettuate mediante operatori hermitiani che non sono necessariamente proiettori, quindi non è essenziale che siano ortogonali, e sono dette POVM (positive operator-valued measures). Dato un insieme,  $\{Q_i, i \in \mathcal{M}\}$  di operatori, per essere POVM, devono soddisfare le seguenti caratteristiche:

- 1)  $Q_i$  sono operatori hermitiani,  $Q_i^* = Q_i$ ,
- 2)  $Q_i$  sono semidefiniti positivi,  $Q_i \geq 0$ ,
- 3) formano un sistema completo:  $\sum_i Q_i = I_{\mathcal{H}}$ .

Gli operatori POVM costituiscono una classe più vasta di operatori poiché non devono verificare l'idempotenza e l'ortogonalità e le proprietà elencate assicurano la probabilità secondo (3.11).

La formula (3.11) si può generalizzare per il calcolo delle probabilità ai sistemi che si trovano in una miscela di stati descritti dal operatore  $\rho$ , cioè

$$P[m = i|\rho] = Tr(\rho Q_i). \quad (3.12)$$

### Grado di sovrapposizione degli stati coerenti

Il grado di sovrapposizione di due stati coerenti distinti  $|\alpha\rangle$  e  $|\beta\rangle$  risulta partendo dalla (3.7)

$$\begin{aligned} \langle \alpha | \beta \rangle &= e^{-\frac{1}{2}(|\alpha|^2 + |\beta|^2)} \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \frac{(\alpha^*)^n \beta^n}{\sqrt{n!m!}} \langle m | n \rangle \\ &= e^{-\frac{1}{2}(|\alpha|^2 + |\beta|^2)} \sum_{m=0}^{\infty} \frac{(\alpha^* \beta)^m}{\sqrt{m!}} \\ &= e^{-\frac{1}{2}(|\alpha|^2 + |\beta|^2)} e^{\alpha^* \beta}. \end{aligned} \quad (3.13)$$

Quindi si ha infine

$$\langle \alpha | \beta \rangle = e^{-\frac{1}{2}(|\alpha|^2 + |\beta|^2) - 2\alpha^* \beta}. \quad (3.14)$$

Si osserva che due stati distinti *non sono mai ortogonali*.

### Sovrapposizione degli stati

Si introduce il grado di sovrapposizione (quadratico) tra due stati coerenti distinti  $|\alpha\rangle$  e  $|\beta\rangle$ , data dalla geometria del prodotto interno con

$$\Gamma^2 = |\langle \alpha | \beta \rangle|^2 = e^{-|\alpha - \beta|^2} \quad |\alpha\rangle, |\beta\rangle \in \mathcal{G}. \quad (3.15)$$

Si può notare che ponendo  $\alpha = 0$  nella (3.15) si ottiene

$$|\alpha\rangle_{\alpha=0} = |n\rangle_{n=0}$$

ovvero si ottiene lo stato  $|0\rangle$  della base (ground state).

### 3.2.3 Sistema quantistico e ottimizzazione del ricevitore binario

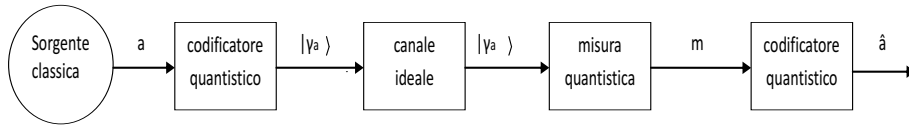


Figura 3.1: Sistema quantistico di trasmissione numerica.

La sorgente classica emette un simbolo fra  $M$  simboli possibili,  $a \in \mathcal{A} = \{\alpha_1, \dots, \alpha_M\}$  con probabilità a priori  $q_\alpha = P[a = \alpha]$ ,  $a \in \mathcal{A}$ . Il codificatore quantistico “prepara” il sistema quantistico  $\mathcal{H}_T$  in uno degli stati

$$|\gamma_{\alpha_1}\rangle, |\gamma_{\alpha_2}\rangle, \dots, |\gamma_{\alpha_M}\rangle.$$

Agli stati corrispondono gli operatori densità

$$\rho_{\alpha_1}, \rho_{\alpha_2}, \dots, \rho_{\alpha_M} \quad \text{con} \quad \rho_\alpha = |\gamma_\alpha\rangle\langle\gamma_\alpha|$$

con probabilità a priori  $q_\alpha \geq 0$ , dove  $\sum_{\alpha=0}^M q_\alpha = 1$ . Sia  $\{\mathbf{Q}_\alpha, \alpha \in \mathcal{A}\}$  l’insieme degli operatori di misura POVM dove le probabilità di transizione del canale quantistico sono

$$p_c(\hat{\alpha}|\alpha) = \text{Tr}(\rho_\alpha \mathbf{Q}_\alpha), \quad \hat{\alpha}, \alpha \in \mathcal{A}. \quad (3.16)$$

La probabilità di decisione corretta diventa

$$P_c = \sum_{\alpha \in \mathcal{A}} q_\alpha \text{Tr}(\rho_\alpha \mathbf{Q}_\alpha) \quad (3.17)$$

e in particolare se il sistema in ricezione è in uno stato certo (assenza di rumore), con  $\rho = |\gamma_\alpha\rangle\langle\gamma_\alpha|$  si ha

$$P_c = \sum_{\alpha \in \mathcal{A}} q_\alpha \langle\gamma_\alpha|\mathbf{Q}_\alpha|\gamma_\alpha\rangle. \quad (3.18)$$

Si può notare dalla (3.17) che la probabilità di corretta decisione si può massimizzare determinando gli operatori per ottenere

$$\max \sum_{\alpha \in \mathcal{A}} q_\alpha \langle\gamma_\alpha|\mathbf{Q}_\alpha|\gamma_\alpha\rangle \quad (3.19)$$

quando gli stati sono certi, oppure per ottenere

$$\max \sum_{\alpha \in \mathcal{A}} q_\alpha \text{Tr}(\rho_\alpha \mathbf{Q}_\alpha) \quad (3.20)$$

quando gli stati del sistema sono specificati dall'operatore densità.

Si possono applicare le considerazioni precedenti ad un sistema binario con simboli  $a \in \{0, 1\}$ . Il modulatore pone il sistema in uno dei due stati  $|\gamma_1\rangle, |\gamma_2\rangle \in \mathcal{H}$ . Si suppone l'alfabeto  $\mathcal{M}$  della misura coincidente con l'alfabeto della sorgente  $\mathcal{A} = \mathcal{M} = \{0, 1\}$ . Per la misura scegliamo due operatori di misura POVM:

$$\mathbf{Q}_0, \quad \mathbf{Q}_1, \quad \text{con} \quad \mathbf{Q}_0 + \mathbf{Q}_1 = \mathbf{I}$$

e poichè  $\mathbf{Q}_0 + \mathbf{Q}_1 = \mathbf{I}$  si può considerare solo un operatore, ad esempio  $\mathbf{Q}_1$ .

Supposto che il sistema è specificato da due operatori di densità  $\rho_0$  e  $\rho_1$ , si calcola la probabilità di decisione corretta utilizzando la (3.17), che dà

$$\begin{aligned} P_c &= q_0 \text{Tr}(\rho_0 \mathbf{Q}_0) + q_1 \text{Tr}(\rho_1 \mathbf{Q}_1) \\ &= q_0 \text{Tr}(\rho_0 \mathbf{I}) + \text{Tr}[(q_1 \rho_1 - q_0 \rho_0) \mathbf{Q}_1] \\ &= q_0 + \text{Tr}[(q_1 \rho_1 - q_0 \rho_0) \mathbf{Q}_1] \end{aligned} \quad (3.21)$$

dove nell'ultimo passaggio si è tenuto presente che la traccia di un operatore densità è sempre unitaria. Con i simboli equiprobabili ( $q_0 = q_1 = \frac{1}{2}$ ) si ha

$$P_c = \frac{1}{2} + \frac{1}{2} \text{Tr}[(\rho_1 - \rho_0) \mathbf{Q}_1].$$

Dalla (3.21), si ha che per minimizzare la probabilità di errore, occorre trovare l'operatore di misura  $\mathbf{Q}_1$  tale che

$$\max \text{Tr}[(q_1 \rho_1 - q_0 \rho_0) \mathbf{Q}_1] \quad q_0 + q_1 = 1.$$



Per fare questo si fa la scomposizione spettrale dell'operatore hermitiano

$$\mathbf{D} = q_1 \boldsymbol{\rho}_1 - q_0 \boldsymbol{\rho}_0 = \sum_k \eta_k |\eta_k\rangle \langle \eta_k| \quad (3.22)$$

dove  $\eta_k$  è il generico autovalore (reale) e  $|\eta_k\rangle$  il corrispondente autovettore (gli  $\eta_k$  si suppongono distinti e quindi i corrispondenti autovettori sono ortonormali). Risulta che

$$\begin{aligned} \text{Tr}[(q_1 \boldsymbol{\rho}_1 - q_0 \boldsymbol{\rho}_0) \mathbf{Q}_1] &= \sum_k \eta_k \text{Tr}[|\eta_k\rangle \langle \eta_k| \mathbf{Q}_1] \\ &= \sum_k \eta_k \langle \eta_k | \mathbf{Q}_1 | \eta_k \rangle \end{aligned} \quad (3.23)$$

dove nell'ultimo passaggio si è utilizzata l'identità (3.3). La quantità  $\epsilon_k = \langle \eta_k | \mathbf{Q}_1 | \eta_k \rangle$  rappresenta la probabilità della misura ottenuta con l'operatore di misura  $\mathbf{Q}_1$  quando il sistema è nello stato  $|\eta_k\rangle$ , quindi  $0 \leq \epsilon_k \leq 1$ . Per ottenere il massimo dall'espressione (3.23) bisogna scegliere, se possibile, i termini con  $\eta_k \geq 0$  e  $\epsilon_k = 1$ . Tale scelta è possibile scegliendo l'operatore di misura  $\mathbf{Q}_1$  in questo modo

$$\mathbf{Q}_1 = \sum_{\eta_k > 0} |\eta_k\rangle \langle \eta_k| \quad (3.24)$$

poichè così si ottiene  $\epsilon_k = \langle \eta_k | \mathbf{Q}_1 | \eta_k \rangle = 1$  ed il massimo ricercato risulta

$$\text{Tr}[(q_1 \boldsymbol{\rho}_1 - q_0 \boldsymbol{\rho}_0) \mathbf{Q}_1] = \sum_{\eta_k > 0} |\eta_k\rangle \langle \eta_k|$$

ovvero dato dalla somma degli autovalori positivi. Con questa scelta la probabilità di corretta decisione risulta

$$P_c = q_0 + \sum_{\eta_k > 0} \eta_k. \quad (3.25)$$

La (3.25) rappresenta il limite di Helstrom per il sistema quantistico binario.

In generale trovare la probabilità di corretta decisione dato un sistema di  $M \geq 2$  di operatori di misura POVM diventa molto difficile poichè bisogna massimizzare la  $P_c$  "su" tutti gli  $M$  operatori. Si ricorre allora a formulazioni differenti, nelle quali si cerca di trattare un numero minore di variabili e restrizioni per il calcolo della probabilità di corretta decisione, vedi [6].

### Limite di Helstrom del ricevitore binario con stati certi

Supposto che il sistema quantistico in ricezione si trovi in uno dei due stati puri  $|\gamma_0\rangle$  e  $|\gamma_1\rangle$ , e sia perciò descritto dagli operatori densità

$$\boldsymbol{\rho}_0 = |\gamma_0\rangle \langle \gamma_0| \quad \boldsymbol{\rho}_1 = |\gamma_1\rangle \langle \gamma_1|$$

Si procede come precedentemente con lo sviluppo spettrale dell'operatore hermitiano

$$\mathbf{D} = q_1 \boldsymbol{\rho}_1 - q_0 \boldsymbol{\rho}_0 = q_1 |\gamma_1\rangle \langle \gamma_1| - q_0 |\gamma_0\rangle \langle \gamma_0|. \quad (3.26)$$

Allora la scomposizione spettrale di  $\mathbf{D}$  è limitata a due termini (due autovalori diversi da zero) e per trovarla si osserva che i due autovettori  $|\eta_0\rangle$  e  $|\eta_1\rangle$  di  $\mathbf{D}$  devono appartenere al sottospazio  $\mathcal{D}$  e quindi sono combinazioni lineari dei due stati

$$|\eta_0\rangle = a_0 |\gamma_0\rangle + b_0 |\gamma_1\rangle \quad |\eta_1\rangle = a_1 |\gamma_0\rangle + b_1 |\gamma_1\rangle \quad (3.27)$$

dove i coefficienti  $a_i$  e  $b_i$  si ottengono applicando la definizione di autovettore, cioè

$$\mathbf{D}|\eta_0\rangle = \eta_0 |\eta_0\rangle \quad \mathbf{D}|\eta_1\rangle = \eta_1 |\eta_1\rangle. \quad (3.28)$$

Sostituendo (3.26) e (3.27), tenendo presente che  $\langle \gamma_0 | \gamma_0 \rangle = \langle \gamma_1 | \gamma_1 \rangle = 1$  e ponendo  $X = \langle \gamma_0 | \gamma_1 \rangle$  si ottiene

$$q_1(a_i X + b_i) |\gamma_1\rangle - q_0(a_i + b_i X^*) |\gamma_0\rangle = \eta_i(a_i |\gamma_0\rangle + b_i |\gamma_1\rangle), \quad i = 0, 1, \dots \quad (3.29)$$

Per la supposta indipendenza, nella (3.29) i coefficienti di  $|\gamma_0\rangle$  e  $|\gamma_1\rangle$  devono essere uguali

$$q_1(a_i X + b_i) = \eta_i b_i, \quad q_0(a_i + b_i X^*) = \eta_i a_i$$

che risolvendo rispetto a  $\eta_i$  si trova l'equazione

$$\eta_i^2 - \eta_i(q_1 - q_0) - q_0 q_1(1 - |X|^2) = 0$$

le cui soluzioni sono  $\eta_1 \geq 0$  e  $\eta_0 \leq 0$ , quindi si ha soltanto un autovalore positivo. Pertanto applicando la (3.25) si ha

$$P_c = \frac{1}{2}(1 + \sqrt{1 - 4q_0 q_1 \Gamma^2}) \quad (3.30)$$

dove  $\Gamma^2 = |X|^2 = |\langle \gamma_0 | \gamma_1 \rangle|^2$  rappresenta il grado sovrapposizione (quadratico) tra i due stati. Infine la probabilità di errore che rappresenta il limite di Helstrom diventa

$$P_e = \frac{1}{2}(1 - \sqrt{1 - 4q_0 q_1 \Gamma^2}) \quad (3.31)$$

## Il teorema di Kennedy

Il teorema di Kennedy si riferisce ad un sistema in cui si hanno  $M$  stati certi.

*TEOREMA 3.1* In un sistema  $M$ -ario specificato da  $M$  stati certi  $|\gamma_1\rangle, \dots, |\gamma_M\rangle$ , i proiettori ottimali (che minimizzano la probabilità di errore) sono sempre elementari, cioè hanno la forma

$$\mathbf{Q}_i = |\mu_i\rangle \langle \mu_i|, \quad i = 1, 2, \dots, M \quad (3.32)$$

dove i vettori di misura  $|\mu_i\rangle$  devono essere ortonormali.

In base al teorema, la ricerca della decisione ottimale si semplifica poiché è limitata alla ricerca di  $M$  vettori di misura

$$|\mu_1\rangle, |\mu_2\rangle, \dots, |\mu_M\rangle$$

dai quali si costruiscono i proiettori ottimali mediante la (3.32).

Si ha quindi una semplificazione in quanto bisogna ricercare  $M$  vettori anziché  $M$  matrici.

### 3.3 Sistema quantistico con modulazione OOK

Per realizzare un sistema QTLC binario il trasmettitore (laser) viene posto in due stati coerenti distinti  $|\gamma_0\rangle$  e  $|\gamma_1\rangle \in \mathcal{G}$  la cui geometria è completamente specificata dal prodotto interno  $\langle\gamma_0|\gamma_1\rangle$  che con gli stati di Glauber è data dalla (3.14). Nella modulazione OOK la costellazione è composta dagli stati

$$|\gamma_0\rangle = |0\rangle, |\gamma_1\rangle = |\beta\rangle \in \mathcal{G}$$

dove  $|0\rangle$  è il ground state e lo stato  $|\beta\rangle$  è determinato dal numero  $\beta$  che si può considerare reale e positivo, vedi figura 3.2. La sovrapposizione quadratica dei due stati risulta  $|\langle 0|\beta\rangle|^2 = e^{-\beta^2}$ . Il numero medio di fotoni associato al simbolo  $a = 0$  è  $N_R(0) = 0$  e quello associato al simbolo  $a = 1$  è  $N_R(1) = \beta^2$ . Risulta che il numero medio di fotoni per bit è

$$N_R = \frac{1}{2}N_R(0) + \frac{1}{2}N_R(1) = \frac{1}{2}N_R(1)$$

dove la sovrapposizione quadratica dei due stati può essere scritta nella forma

$$\Gamma^2 = e^{-2N_R}.$$

Dalla (3.31), considerando simboli equiprobabili quindi le probabilità a priori pari a  $q_0 = q_1 = \frac{1}{2}$ , la probabilità di corretta decisione del sistema quantistico OOK risulta

$$P_c = \frac{1}{2} \left[ 1 + \sqrt{1 - e^{-2N_R}} \right] \quad (3.33)$$

di conseguenza si ha una probabilità di errore  $P_e = 1 - P_c$  che è

$$P_e = \frac{1}{2} \left[ 1 - \sqrt{1 - e^{-2N_R}} \right] \quad (3.34)$$

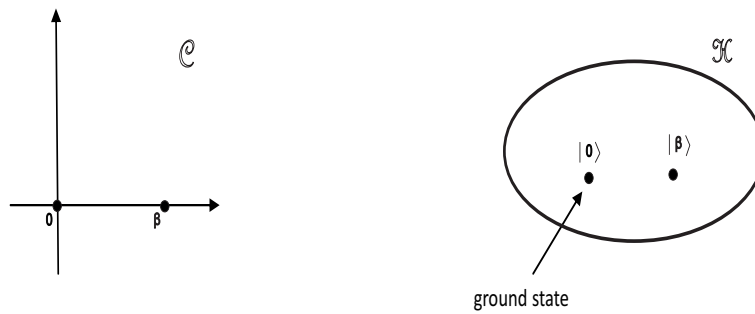


Figura 3.2: Costellazioni di simboli e di stati nella modulazione OOK.

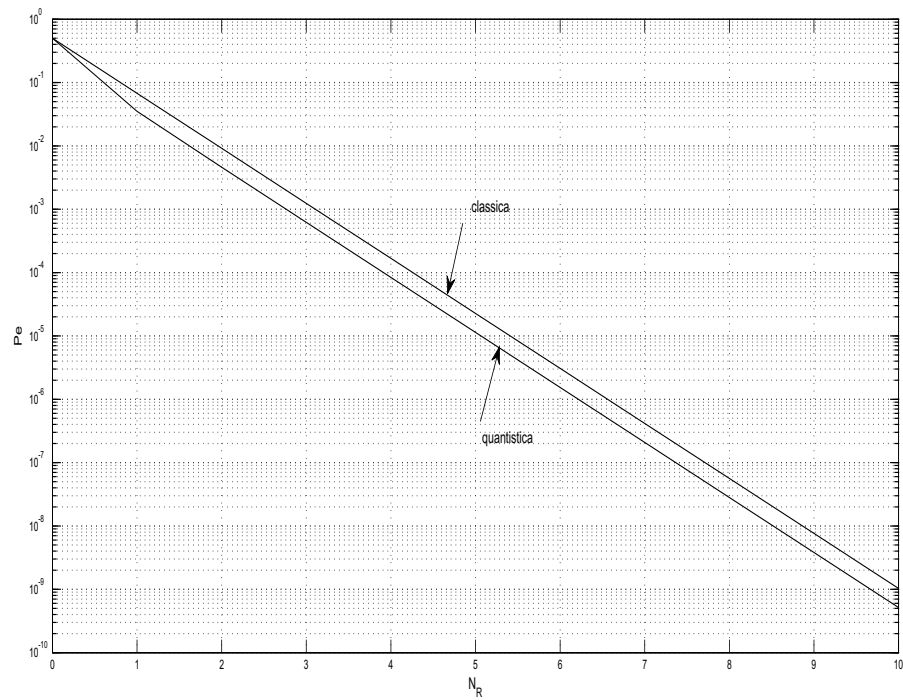


Figura 3.3: Confronto fra modulazione OOK quantistica e classica.

Il comportamento asintotico della (3.34) risulta (ottenuto con l'approssimazione  $1 - \sqrt{1-x} \simeq \frac{1}{2}x$  per  $x$  piccolo )

$$P_e = \frac{1}{4}e^{-2N_R} \quad N_R \gg 1$$

ovvero la metà del caso classico dato dalla (2.5). Fissando una  $P_e = 10^{-9}$  risulta  $N_R = 9.6$  fotoni per bit. Il confronto fra la  $P_e$  del ricevitore classico, data dalla (2.5), e la  $P_e$  del ricevitore quantistico, data dalla (3.34), è riportato in figura 3.3 in funzione del numero medio di fotoni per bit  $N_R$ .

### 3.4 Sistema quantistico con modulazione 2PSK

Nel sistema quantistico 2PSK al simbolo  $a = 0$  (fase  $\varphi = 0$ ) viene associato uno stato coerente  $|\beta\rangle$  con un dato  $\beta$  e al simbolo  $a = 1$  (fase  $\varphi = \pi$ ) lo stato coerente  $|\!-\beta\rangle$  (figura 3.4)

$$|\gamma_0\rangle = |\beta\rangle, \quad |\gamma_1\rangle = |\!-\beta\rangle \in \mathcal{G}$$

Dalla associazione fatta si ottiene che il numero medio di fotoni associato ai due stati risulta uguale

$$N_R(0) = N_R(1) = |\beta|^2 = N_R$$

mentre il grado di sovrapposizione quadratico dei due stati diventa

$$\Gamma^2 = e^{-|\beta - (-\beta)|^2} = e^{-4|\beta|^2} = e^{-4N_R} \quad (3.35)$$

che partendo sempre dalla 3.31 dà una probabilità di errore

$$P_e = \frac{1}{2} \left[ 1 - \sqrt{1 - e^{-4N_R}} \right]. \quad (3.36)$$

Il confronto fra la  $P_e$  del ricevitore classico, data dalla (2.12), e la  $P_e$  del ricevitore quantistico, data dalla (3.36), è riportato in figura 3.5 in funzione del numero medio di fotoni per bit  $N_R$ . In particolare nel ricevitore classico si ha

$$P_e = 10^{-9} \quad \text{con} \quad N_R = 5 \text{ fotoni per bit}$$

mentre con il ricevitore quantistico si ha

$$P_e = 10^{-9} \quad \text{con} \quad N_R = 4.8 \text{ fotoni per bit.}$$

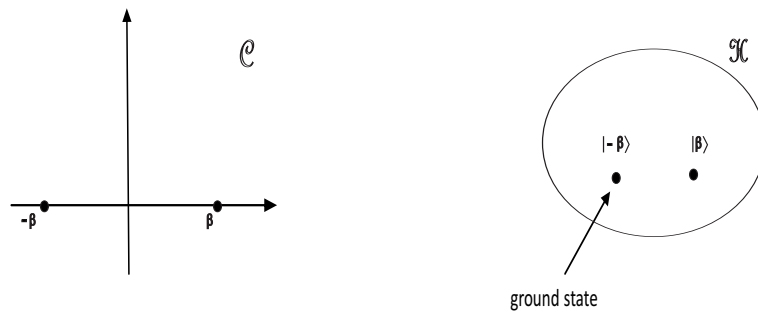


Figura 3.4: Costellazioni di simboli e di stati nella modulazione 2PSK.

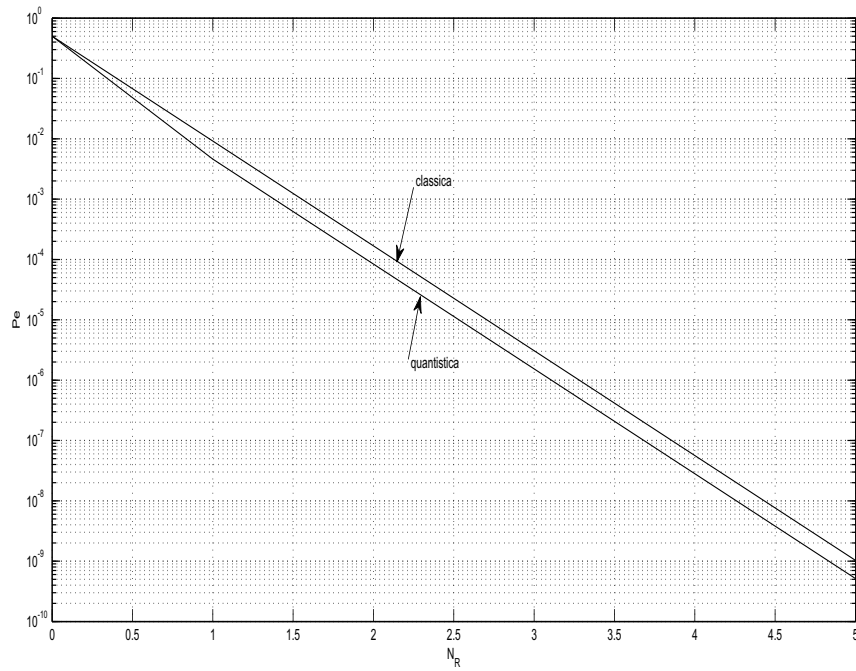


Figura 3.5: Confronto fra modulazione 2PSK quantistica e classica.

## Capitolo 4

# Realizzazione di ricevitori quantistici

Se supponiamo di avere a disposizione un *buon* trasmettitore, conoscendo inoltre le caratteristiche del canale ed operando al massimo del rate di trasmissione possibile, è stato dimostrato che esiste un ricevitore in grado di minimizzare gli errori di comunicazione. Questo tipo di ricevitore prende il nome di *ricevitore quantistico*. Esso è stato studiato prima da Helstrom, a partire dagli anni settanta, e da Kennedy e Dolinar successivamente. I ricevitori più studiati e praticamente implementati sono i ricevitori per comunicazioni quantistiche binarie quali il ricevitore di Kennedy e il ricevitore di Dolinar.

### 4.1 Il ricevitore di Kennedy

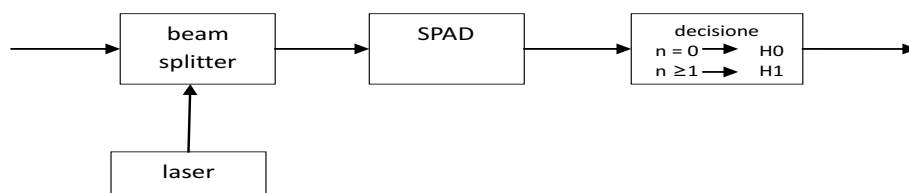


Figura 4.1: Schema di principio del ricevitore di Kennedy.

Il ricevitore di Kennedy necessita in sostanza di tre elementi:

- un Beam Splitter (BS);
- un oscillatore locale (laser) identico a quello usato in trasmissione;

- un contatore di singoli fotoni (SPAD);

Tale ricevitore si basa sul principio di sommare allo stato quantico in ricezione lo stato creato da un laser locale identico a quello in trasmissione attraverso il Beam Splitter. Si può intuire che sommando allo stato coerente in arrivo lo stato coerente locale si ottengono due possibili risultati:

1- i due stati sono in fase allora l'ampiezza dello stato risultante sarà doppio di quello in ricezione.

2- i due stati sono in contro fase, lo stato risultante sarà lo stato di base  $|0\rangle$  (ground state), ovvero lo stato è formato da un numero di fotoni nullo.

Il conteggio dei fotoni si ottiene mediante l'utilizzo di uno SPAD (Single-Photon Avalanche Diode), sensibile al singolo fotone. All'uscita dello SPAD occorre operare una scelta sul segnale ricevuto in base al numero di fotoni contati dallo SPAD in un periodo  $T$ . Indicando con  $N_R$  il numero di fotoni all'interno di ogni periodo di simbolo, la regola di decisione è

$$\begin{aligned} \text{Se } N_R \geq 1 & \text{ è stato trasmesso lo stato } |\gamma_1\rangle \\ \text{Se } N_R = 0 & \text{ è stato trasmesso lo stato } |\gamma_0\rangle \end{aligned} \quad (4.1)$$

Data la regola di decisione e realizzando una trasmissione quantistica BPSK si ottiene la probabilità d'errore per il ricevitore di Kennedy che è pari a

$$P_e = \frac{1}{2}e^{-4N_R} \quad (4.2)$$

Il ricevitore di Kennedy si dice sub-ottimale poichè la probabilità di errore si avvicina molto al limite di Helstrom.

## 4.2 Il ricevitore di Dolinar

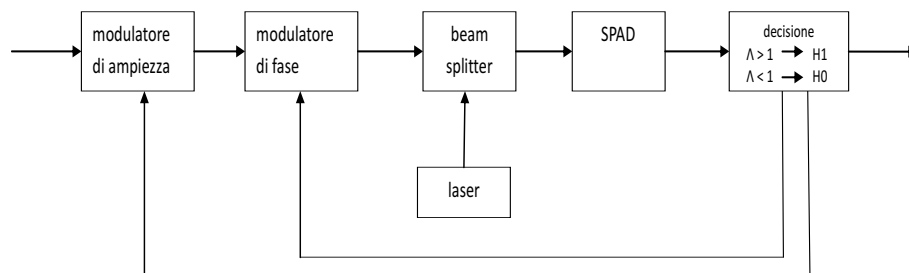


Figura 4.2: Schema di principio del ricevitore di Dolinar.

Il ricevitore di Dolinar rappresenta un ricevitore ottimale in quanto raggiunge il limite di Helstrom. Esso è però più difficile da implementare rispetto



al ricevitore di Kennedy in quanto presenta una retroazione. La retroazione deve avvenire in tempo reale, all'interno del periodo di simbolo con cui si trasmettono i simboli  $|\gamma_0\rangle$  e  $|\gamma_1\rangle$ . Il ricevitore opera una somma tra il segnale in arrivo dal canale e un segnale del tipo

$$U(t) = u(t)e^{-i(\omega t + \phi)} \quad (4.3)$$

in modo che lo SPAD conteggia i fotoni con una media istantanea

$$\Phi(t) = |\gamma(t) + u(t)|^2 \quad (4.4)$$

dove  $u(t)$  rappresenta il "displacement" dell'ampiezza. Se  $\gamma(t) = 0$  il canale è nello stato  $|\gamma_0\rangle$  ed è descritto dall'operatore  $\rho_0$ , e  $\gamma(t) = \gamma_1(t)$  quando il canale si trova nello stato  $|\gamma_1\rangle$  descritto dall'operatore  $\rho_1$ .

L'arrivo di fotoni provenienti dal canale è inquadrato come un processo aleatorio di Poisson e il periodo di simbolo  $T$  è suddiviso negli intervalli  $\{t_1, t_2, \dots, t_n\}$  che rappresentano i tempi di interarrivo dei fotoni.

Il criterio di decisione fra i due stati  $|\gamma_0\rangle$  e  $|\gamma_1\rangle$  avviene scegliendo in base al rapporto

$$\Lambda = \frac{p[\rho_1|t_1, t_2, \dots, t_n, u(t)]}{p[\rho_0|t_1, t_2, \dots, t_n, u(t)]} \quad (4.5)$$

dove le probabilità condizionate  $p[\rho_i|t_1, t_2, \dots, t_n, u(t)]$  riflettono la probabilità di  $\rho_1$  e  $\rho_0$  sotto la condizione che gli  $n$  arrivi di fotoni avvengano nei precisi istanti  $\{t_1, t_2, \dots, t_n\}$  e data la  $u(t)$ . Se  $\Lambda > 1$  allora si decide che è stato inviato  $|\gamma_1\rangle$ , in caso contrario è stato trasmesso  $|\gamma_0\rangle$ . Si può concludere dicendo che monitorando il flusso esatto di fotoni ed effettuando una retroazione in tempo reale, si assicura il comportamento ottimale del ricevitore di Dolinar permettendogli di raggiungere il limite di Helstrom

$$\begin{aligned} P_e &= \frac{1}{2}(1 - \sqrt{1 - 4q_0q_1|\langle\gamma_0|\gamma_1\rangle|^2}) \\ &= \frac{1}{2}(1 - \sqrt{1 - e^{-4N_R}}) \\ &= \frac{1}{4}e^{-4N_R} \text{ per } N_R \gg 0. \end{aligned} \quad (4.6)$$

## Capitolo 5

# Conclusioni

Ad oggi con la tecnologia attuale, la teoria delle comunicazioni quantistiche è di difficile implementazione pratica. La comunicazione quantistica si scontra principalmente con due problemi pratici, ovvero rilevare con grande efficienza singoli sistemi quantistici, in particolare, singoli fotoni e in secondo luogo è difficile operare in sistemi quantistici senza andare ad alterare la proprietà di coerenza degli stati stessi. Tuttavia si è arrivati ad implementare con successo il ricevitore di Kennedy. È stato realizzato anche il ricevitore di Dolinar che però non raggiunge ancora le prestazioni predette dalla teoria. Un miglioramento di prestazioni di quest'ultimo si può avere con l'introduzione dell'elettronica veloce in modo tale da poter realizzare la retroazione in tempo reale.

# Bibliografia

- [1] Gianfranco Cariolaro, *Comunicazioni quantistiche*. Progetto, Marzo 2008;
- [2] G. Cariolaro, C. De Angelis, N. Laurenti, *Comunicazioni Ottiche* Progetto, Settembre 2006;
- [3] Gianfranco Cariolaro, *Trasmissione numerica*. Progetto, 1991;
- [4] G. Brida, M. Genovese, M. Gramegna, A. Meda, S. Olivares, M.G.A. Paris, F. Piacentini, E. Predazzi, P. Traina, *A review on recent results on on/off reconstruction of optical states*. Optical Society of America, pag. 42-50, arXiv:8010.5472v2, 5 Nov 2008;
- [5] Robert L. Cook, Paul J. Martin & M. Geremia, *Optical coherent state discrimination using a closed-loop quantum measurement*. Nature vol.446, 12 April 2007;
- [6] A. Assalini, G. Cariolaro, G. Pierobon, *Efficient optimal minimum error discrimination of symmetric quantum states*. Department of Information Engineering, arXiv:1001.1385v1, January 2010;
- [7] J.M. Geremia, *Distinguishing between optical coherent states with imperfect detection*. Physics and Control & Dynamical Systems, arXiv:quant-ph/0407205v1, February 2008;