

OPTIMAL RECEIVER DESIGN FOR QUANTUM COMMUNICATION

by

Rahul Kumar Bhadani

A Thesis Submitted to the Faculty of the

JAMES C. WYANT COLLEGE OF OPTICAL SCIENCES

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science

In the Graduate College

THE UNIVERSITY OF ARIZONA

Summer 2021

THE UNIVERSITY OF ARIZONA  
GRADUATE COLLEGE

As members of the Master's Committee, we certify that we have read the thesis prepared by **Rahul Kumar Bhadani**, titled *Optimization in Quantum Information Theory* and recommend that it be accepted as fulfilling the thesis requirement for the Master's Degree.

*Ivan Djordjevic*

\_\_\_\_\_  
Professor Ivan B. Djordjevic

Date: 08/19/2021

*Khanh Kieu*

\_\_\_\_\_  
Professor Khanh Q. Kieu

Date: 8/19/2021


*Yuzuru Takashima*

\_\_\_\_\_  
Professor Yuzuru Takashima

Date: 08/19/2021

\_\_\_\_\_  
Date: \_\_\_\_\_

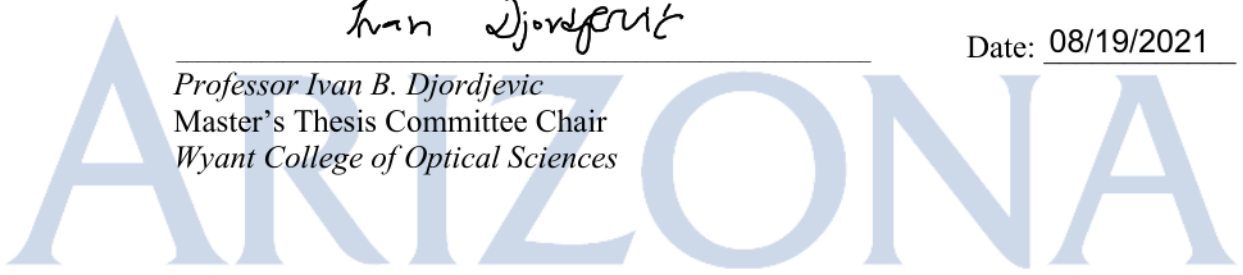
Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to the Graduate College.

I hereby certify that I have read this thesis prepared under my direction and recommend that it be accepted as fulfilling the Master's requirement. 

*Ivan Djordjevic*

\_\_\_\_\_  
Professor Ivan B. Djordjevic  
Master's Thesis Committee Chair  
Wyant College of Optical Sciences

Date: 08/19/2021



ॐॐॐ

---

Copyright © Rahul Kumar Bhadani, 2021

---

## ACKNOWLEDGEMENT

---

I am grateful to work with Dr. Ivan B. Djordjevic. This thesis is the result of advising, mentorship and continuous support through in-person as well as remote interaction with Dr. Djordjevic. I also thank Dr. Jonathan Sprinkle for unwavering support through funding, and advising. I also like to thank Dr. Saikat Guha for stimulating interest in Quantum Information Theory. Further, I thank OCSL lab members for weekly helpful discussion and critical thinking. Finally, I couldn't imagine presenting this thesis without the support of my parents and brothers.

# CONTENTS

---

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	LAYOUT OF THE THESIS . . . . .	1
<b>2</b>	<b>BACKGROUND AND LITERATURE REVIEW</b>	<b>3</b>
2.1	THE CONCEPT OF ‘INFORMATION’ . . . . .	3
2.1.1	Information Theory for photon detection . . . . .	3
2.1.2	Poisson point process . . . . .	6
2.2	BRA- AND KET-NOTATIONS . . . . .	8
2.2.1	Usage of bracket in quantum mechanics . . . . .	9
2.2.2	Measurements in Quantum System . . . . .	10
2.2.3	Projective measurements (Von Neumann measurements) . . . . .	10
2.3	LASER PULSES AND DETECTION OF PHOTON . . . . .	12
2.3.1	State of Quantum System . . . . .	13
2.4	COHERENT STATE (IDEAL SINGLE MODE LASER) . . . . .	14
2.4.1	Ideal photon detection of square pulse . . . . .	15
2.5	DISCRIMINATION OF STATES . . . . .	17
2.6	BEAMSPLITTER AND MIXING OPERATION . . . . .	18
2.7	SQUEEZED-STATES . . . . .	19
2.8	ENTANGLED STATE . . . . .	21
2.9	SPONTANEOUS PARAMETRIC DOWNCONVERSION . . . . .	23
2.10	A REVIEW OF EXISTING RECEIVER DESIGNS EMPLOYING COHERENT STATES	24
2.10.1	Kennedy’s Receiver . . . . .	25
2.10.2	Unambiguous State Discrimination Receiver (USD) . . . . .	27

2.10.3 Dolinar Receiver . . . . .	28
<b>3 RECEIVER DESIGN FOR PHASE-SHIFT KEYING COHERENT STATES</b>	<b>31</b>
3.1 INTRODUCTION . . . . .	31
3.2 PHASE-SHIFT KEYED COHERENT STATES, NOISE MODELS, AND DETECTOR IMPERFECTIONS . . . . .	33
3.3 DISPLACEMENT RECEIVERS WITH PHOTON-COUNTING AND ON-OFF PHOTODETECTOR FOR BPSK . . . . .	34
3.3.1 Detector Imperfections . . . . .	37
3.4 DISPLACEMENT RECEIVER DESIGN FOR QPSK . . . . .	40
3.4.1 Izumi-Sasaki Design without Feedforward . . . . .	41
3.5 CONCLUSION . . . . .	50
<b>4 OPTIMAL SQUEEZING OPERATION FOR DISPLACEMENT RECEIVER</b>	<b>51</b>
4.1 INTRODUCTION . . . . .	51
4.2 SQUEEZING OPERATION . . . . .	52
4.2.1 Photon Statistics for Squeezed-Displaced States . . . . .	53
4.3 RECEIVER DESIGN WITH SQUEEZING OPERATION . . . . .	53
4.3.1 Receiver Design for BPSK State Discrimination . . . . .	53
4.3.2 Receiver Design for QPSK State Discrimination . . . . .	53
4.4 PERFORMANCE ASSESSMENT OF PROPOSED RECEIVER DESIGN . . . . .	56
4.4.1 Error Probability Calculation for BPSK . . . . .	56
4.4.2 Maximizing Mutual Information for BPSK . . . . .	58
4.4.3 Error Probability Calculation for QPSK State Discrimination . . . . .	59
4.4.4 Maximizing Mutual Information for QPSK . . . . .	63
4.5 DISCUSSION AND CONCLUSION . . . . .	63
<b>5 OPTIMIZED RECEIVER DESIGN FOR ENTANGLEMENT-ASSISTED COMMUNICATION USING BPSK</b>	<b>67</b>
5.1 INTRODUCTION . . . . .	67
5.2 ENTANGLEMENT ASSISTED CLASSICAL COMMUNICATION CONCEPT . . . . .	68
5.3 RECEIVER DESIGN FOR EA COMMUNICATION . . . . .	69
5.3.1 OPA based receiver with threshold detection . . . . .	71

5.3.2	Optical Phase Conjugation Receiver . . . . .	73
5.3.3	2x2 Optical Hybrid Receiver based Joint Receiver . . . . .	74
5.4	EVALUATION OF ENTANGLEMENT-ASSISTED COMMUNICATION RECEIVERS .	76
5.4.1	Error Probability Calculation . . . . .	77
5.4.2	Mutual Information Calculation . . . . .	78
5.5	DISCUSSION . . . . .	83
5.5.1	Gaussian Approximation to Negative Binomial Photon Statistics . . .	84
5.6	CONCLUDING REMARKS AND FUTURE WORKS . . . . .	84
<b>6</b>	<b>CONCLUSION</b>	<b>87</b>
	<b>APPENDICES</b>	<b>89</b>
<b>A</b>	<b>PRELIMINARIES</b>	<b>91</b>
A.1	RANDOM VARIABLES AND RANDOM PROCESSES . . . . .	91
A.2	RANDOM PROCESSES . . . . .	92
A.2.1	Definition of random processes . . . . .	92
A.2.2	Random processes describing Discrete events in continuous time and/or space . . . . .	93





# FIGURES

---

2.1	Measuring a Quantum bit . . . . .	10
2.2	A Square Pulse . . . . .	15
2.3	Mean photon number . . . . .	16
2.4	Mean photon number with oscillating phase . . . . .	17
2.5	A schematic diagram showing a beamsplitter's operation as a displacement operator. A beamsplitter acts as a displacement operator when a laser beam of a coherent state amplitude $\alpha_1$ is mixed with a strong local oscillator of amplitude $\alpha_2$ . . . . . .	18
2.6	Spontaneous Parametric Down-Conversion: A pump with frequency $\omega_a$ is passed through nonlinear crystal that converts photons into signal-idler pair conserving energy and momentum. . . . .	24
2.7	<b>Left:</b> A simple circuitry to perform displacement using beamsplitter. <b>Middle:</b> One-off pulse with $ \alpha\rangle$ and $ 0\rangle$ . <b>Right:</b> Displaced coherent states. . . . .	25
2.8	Binary Phase Shift Keying. . . . .	25
2.9	Error probability, $P_e$ of state discrimination for the Kennedy receiver with BPSK. . . . .	26
2.10	BPSK USD receiver design. . . . .	27
2.11	A schematic of Dolinar's Receiver . . . . .	29
3.1	A schematic diagram of the displacement receiver with BPSK symbols. An optimized displacement receiver uses a two-step displacement operation where one of the two coherent states of BPSK is nulled out to a vacuum state and then displaced by $\beta$ amount. . . . .	34

3.2 Transition probability matrix for BPSK. Transition probability matrix is used to describe a channel visually where a connection between each possible input and output is connected and annotated by the transition probability, mapping a particular input to an output. For example, probability of receiving output  $Y = 0$  when  $X = 0$  was transmitted is given by  $e^{-|\beta|^2}$ . . . . . 36

3.3 Transition probability matrix for BPSK with sub-efficient detector and notable dark count. Transition probability connecting possible inputs and outputs are updated to include detected efficiency and dark count. . . . . 38

3.4 BPSK channel capacity for the ideal case. We present a comparison of prior-maximized-displacement maximized mutual information with Capacity from other receiver design in units of bits transmitted per BPSK symbol (bits per mode). . . . . 39

3.5 This graph compares the  $\beta$ , optimal displacement for the Kennedy receiver, for (a) optimizing capacity (blue dotted), and (b) minimizing error probability assuming equal priors (orange dashed) . . . . . 40

3.6 QPSK signal constellation at the input. In phase-shift keying (PSK), the constellation points are positioned with equal angular spacing around a circle. QPSK, a PSK with four points, is denoted by four points on a circle, equispaced. Each point differs from its preceding point by a phase of  $\pi/4$ . . . . 41

3.7 QPSK semi-classical demodulator. In this type of receiver design, two beamsplitters are employed where decisions are made sequentially. The first output of the first beamsplitter is displaced twice and photo-detection is performed. If the decision is ambiguous, then observation is moved to the other stages. At the second stage, the second output of the first beamsplitter is fed through the first input port of the second beamsplitter, mixed with a vacuum state. The first output of the second beamsplitter is displaced twice before performing binary decision using a photodetector. The procedure is repeated at the third stage if the decision remains ambiguous. The second output of the second beamsplitter is displaced twice and finally, the photodetector provides an unambiguous decision. . . . . 42

3.8 QPSK channel capacity using Izumi-Sasaki design. We present a comparison for a case when displacement is zero and when displacement is optimum that maximizes the mutual information. We observe that the receiver achieves higher capacity for low photon numbers regime but converges for 1 to 10 photons regime. . . . . 46

3.9	QPSK channel capacity using Izumi-Sasaki design. A comparison of the channel capacity with varying transmittivity for null and optimal displacement. For a particular $\tau$ , optimal displacement provides higher channel capacity. Further, in low photon numbers regime, increasing $\tau$ increases the channel capacity, but that cannot be said in the higher photon number regime, when we should use different parameters. . . . .	47
3.10	The optimal priors that maximizes mutual information for QPSK (keeping displacement null). . . . .	48
3.11	The optimal priors that maximizes mutual information for QPSK (simultaneously maximizing the displacement). We only show one in every 50 data points for clean visualization. Discontinuities are observed in probability values as a function of the mean photon number since the optimization routine only finds local minima. As the objective function is not convex, we do not expect to get global optima. . . . .	49
3.12	The impact of dark current on the capacity of QPSK and optimality study. Higher the dark current, the lower the capacity we get. However, at the higher photon regime, the effect of dark current is negligible. . . . .	50
4.1	The probability distribution of photon number in squeezed-displaced states from Equation (2.64). . . . .	54
4.2	BPSK symbols and their displaced symbols. . . . .	55
4.3	A schematic diagram of the displacement receiver with BPSK symbols. Squeezed-displaced states are used to encode information using BPSK modulation. . . . .	55
4.4	QPSK semi-classical demodulator with squeezing on transmitter side. . . . .	56
4.5	QPSK semi-classical demodulator with squeezing on receiver side. . . . .	57
4.6	Optimal error probability for BPSK. We compare optimal error probability when BPSK is encoded using coherent states vs when it is encoded using squeezed-displaced state. We find that squeezing offers no obvious advantage. However, squeezing operation requires additional optical elements which may complicate or introduce additional errors due to imperfect implementation. . . . .	58
4.7	A comparison of optimal mutual information (capacity) for various receiver design schemes. We find that capacity is lower for the case when squeezing is used compared to the case when squeezing is not used. . . . .	59

4.8	Optimal error probability for QPSK. We compare optimal error probability when QPSK is encoded using coherent states vs when it is encoded using squeezed-displaced state. From our results, we find that squeezing offers no obvious advantage. However, squeezing operation requires additional optical elements which may complicate or introduce additional errors during implementation. In addition, we also consider non-uniform signaling when priors are not equal. In such a case, no true optimal prior is available. However, non-uniform signaling does provide a lower error probability of state discrimination. We consider two cases while minimizing error probability: (i) when priors are bounded between 0 and 1, (ii) when priors are bounded between 0.1 and 0.9. We find that for the latter case, $p_0$ converges to 0.7 while $p_1$ , $p_2$ , and $p_3$ attain the value of 0.1. . . . .	62
4.9	Optimal error probability for QPSK with squeezing operation on the receiver side. We find out that squeezing operation on receiver side improves error probability slightly as compared to one with purely coherent states. . . . .	63
4.10	Optimal mutual information for QPSK with squeezing operation on the transmitter side vs on the receiver side. We find out that squeezing operation on the receiver side improves mutual information slightly as compared to when squeezing is performing on the transmitter side. Further, we find out that as compared to the purely coherent state, mutual information is greater increased when squeezing is performed on the receiver side. We observe sub-optimal solutions for certain mean photon values which may be attributed to the optimization routine being stuck on local minimal and failing to achieve global minima. Regardless, we demonstrate that it is possible to create a receiver configuration for QPSK modulation that provides increased mutual information when squeezing is used on the receiver side. . . . .	64
5.1	An illustration showing the concept of EA communication. . . . .	69
5.2	Operating Principle of Optical Parametric Amplifier (OPA): At the receiver end, parametric amplification is applied to return-idler pair with gain $G$ . Error probability of discrimination is higher at $\hat{u}$ , hence the photon detection is made $\hat{v}$ . . . . .	71
5.3	Operating Principle of Optical Phase Conjugate (OPC) receiver: signal interacts with vacuum followed by mixing with idler using 50-50 beamsplitter and a balanced detection is applied using photodetectors. . . . .	73
5.4	Receiver configuration of a $2 \times 2$ optical hybrid based joint balanced detection receiver. . . . .	74

5.5 **Top:** Symbol-by-symbol (separable) minimum error-probability measurement on each return-idler mode pair at idler output port. We find that unequal priors have lower error probability as compared to BPSK symbols with equal prior. **Bottom:** Symbol-by-symbol (separable) minimum error-probability measurement on each return-idler mode pair at return output port of OPA receiver. As compared to measurement made at idler output port of the OPA receiver, error probability is higher at the return output port of the OPA receiver. . . . . 79

5.6 Optimal threshold for hypothesis testing at the output port of OPA as a function of number of modes. Higher threshold is required when detection is made at the return output port compared to the detection made at idler output port of OPA receiver. . . . . 80

5.7 Surface plot of  $P_E$  as a function of prior  $p_0$  and threshold mean photon number  $N_{th}$  from Equation (5.19) for photodetection at idler output port for OPA receiver. . . . . 80

5.8 Channel Capacity for BPSK state discrimination using different receiver schemes. We see that entanglement assistance offers advantage in terms of increasing capacity of the channel and beats the classical capacities such as Holevo capacity and Homodyne Capacity. We chose transmittivity of Bosonic channel as  $\eta = 0.01$  and mean background photon as  $N_B = 1.0$ . In our numerical study, classical capacity stays below 0.07 bits per channel use for mean signal photon  $N_s < 1.0$ . . . . . 82

5.9 Information rate as a function of number of modes  $M$  for EA receivers. . . . . 83

5.10 **Top:** Capacity error in the case of OPA receiver as a result of approximating negative binomial photodetection statistics to Gaussian. **Bottom:** Capacity of OPA receiver with the number of modes  $M = 10$ . We observe that with Gaussian approximation, we overestimates the shannon’s capacity of OPA receiver for EA communication while discriminating BPSK states. . . . . 85

A.1 Arrival and Counting Process . . . . . 94

---

## ABSTRACT

---

An important problem in quantum information theory is finding the best possible performance of the optical communication channel employing suitable codewords, receiver design, and constellation optimization techniques. Many receiver designs have been studied in the past to discriminate Phase-Shift Keying (PSK) quantum states that are used to encode information before transmitting over the communication channel. Among many types of quantum states, there has been significant work on the use of coherent states for encoding information. Previous work has sought to improve the communication performance in terms of various metrics such as error probability of state discrimination and capacities by employing a number of quantum states such as coherent states and squeezed-displaced states. In this thesis, we provide optimal receiver design employing coherent states and squeezed-displaced states to maximize the mutual information and lower the error probability of state discrimination. In the case of pure coherent states, we derive an alternative channel capacity of phase-shift keying coherent state with a realizable displacement receiver by maximizing mutual information over symbol priors and pre-detection displacement. We find that the capacity is higher than the capacity achieved by maximizing mutual information over symbol prior but with zero displacements. The overall scheme demonstrates designing an improved, yet easy-to-implement receiver for better communication performance by tuning it at different photon number regime. We also explore the use of squeezing operations with a displacement receiver for state discrimination. Our calculation demonstrates that we see no performance improvement in terms of the probability of error of state discrimination or mutual information using displacement receivers when optimal squeezing on the transmitter side is used. In addition, we also study the receiver design scheme for QPSK modulation where squeezing is employed at the receiver side. We find that using the squeezing operation on the receiver side provides an advantage in terms of increased mutual information for the low-photon number regime compared to when no squeezing is used.

In the later part of the thesis, we study entanglement-assisted communication using two-mode squeezing vacuum. The use of pre-shared entanglement in entanglement-assisted communication provides a superior alternative to classical communication specifically in the low brightness regime and highly noisy environment. In this thesis, we analyze the performance of a few low-complexity receivers that employ optical parametric amplifiers. In the simulation, we demonstrate that receiver designs with an entanglement-assisted scheme using phase-shift-keying modulation can outperform classical capacities. We describe a newly proposed 2x2 optical hybrid receiver for entanglement-assisted communication whose performance is roughly 10% better in terms of error probability as compared to previously proposed optical parametric amplifier-based receivers. Further, we find that using unequal priors for BPSK provides approximately three times the advantage over equal priors in terms of information rate.

---

# INTRODUCTION

---

“ Light in the form of its most fundamental unit photon has been an elixir of life since the beginning of the universe. Today light has been engineered for its utilities in communication, sensing, and computing. Its fundamental unit photon is the carrier of information, possessing numerous degrees of freedom including frequency, phase, arrival time, polarization, orbital angular momentum, linear momentum, entanglement, etc. Manipulating photons has proved to be a valuable resource for many applications ranging from communication systems to security and cryptography. ”

With the advancement in physical sciences, the ways in which we share information have tremendously changed. Along with the radio waves, light is being used in communication, sensing, and computing. Its application ranges from use in fiber optics, medical sciences, smart transportation, military, and satellite communication. However, due to its fundamental nature, an optical detector adds noise while making any measurement at the time of information extraction. This degrades the quality of the information received at other ends. Fortunately, light can be manipulated in the optical domain in such a way that detection can be made in an efficient manner so as to maximize the information received at the other end. Finding optimal ways of detection requires rigorous knowledge of estimation theory, quantum information, quantum estimation theory, optical receivers, detection theory, and optical sensing.

Since quantum theory forbids physical measurements that will allow an observer to gather enough evidence to distinguish non-orthogonal states, the operational measurements are designed to depend on statistics of measurement for distinguishing states. Broadly, there are three measures of distinguishability used: (i) error probability estimation by means of statistical overlap, (ii) the mutual information or capacity - the amount of information that we can recover that may tell us the identity of the state, (iii) the Kulback-Leibler relative information. In this thesis, we only adopt the first two measures of distinguishability for optimal receiver design.

## 1.1 LAYOUT OF THE THESIS

This thesis proposes a numerically optimized receiver design for classical communication using quantum states. The rest of the thesis is outlined as follows. In Chapter 2, we present

some background material and literature to understand the contribution of the chapters to follow. In Chapter 3, we discuss coherent state discrimination of information encoded using PSK modulation. We use coherent states to create PSK states. In terms of distinguishability as mentioned at the beginning of this Chapter, we aim to maximize mutual information for classical communication using PSK modulation. We propose an optimal receiver design based on state displacement operation and provide numerical results to support its advantage over the previously proposed design. In Chapter 4, we discuss the design of a receiver that employs squeezing operation either at the transmitter side or at the receiver side. From our numerical study, we conclude that squeezing doesn't offer any advantage in terms of reducing the error probability of state discrimination or maximizing mutual information when the squeezing operation is employed on the transmitter side. However, we see increased mutual information when squeezing is employed on the receiver side. In Chapter 5, we first review the concept of quantum entanglement and entanglement-assisted communication. Next, we present a quantum receiver design for entanglement assisted (EA) classical communication where we assess the receiver's performance in terms of error probability and mutual information for BPSK state discrimination. Our proposed EA receiver design outperforms the previously proposed receiver design for EA classical communication.

## NOTATIONS USED IN THE THESIS

$|\cdot\rangle$  represents ket-notation in the quantum-mechanical formulation which is equivalent to a vector notation in linear algebra.  $\langle\cdot|$  is the Hermitian conjugate of the vector and is usually referred to as bra-notation. Scalar product of two vectors  $|\gamma\rangle$  and  $|\psi\rangle$  is denoted by  $\langle\psi|\gamma\rangle$ . Further, ket notation  $|\alpha\rangle$  is also used to represent a coherent state of amplitude  $\alpha \in \mathbb{C}$ . We use Greek letters  $\alpha, \beta, \gamma, \psi$  to represent the amplitude of coherent states.  $j$  is used to denote an imaginary unit or a complex number  $\sqrt{-1}$ .  $\phi$  is used to represent the phase of the electromagnetic laser beam.  $X$  and  $Y$  are used to denote random variables denoting input states and detected states respectively.  $\tau$  is used for beamsplitter's transmittivity while  $\eta$  is used for photodetector's efficiency.  $N$  and its suffixed versions are used to denote the mean photo number while  $\Pi$  is used to denote a measurement operator.  $H(\cdot)$  is used to denote Shannon's entropy and  $I(\cdot, \cdot)$  is used to denote mutual information. Probabilities are denoted by  $p$  while conditional probabilities are denoted by  $p_{Y|X}$ , conditioned on  $Y$  given  $X$ .  $\otimes$  is used to denote tensor products.  $\mathcal{H}$  is Hilbert spaces. Superscript  $\dagger$  symbol is used to denote the Hermitian conjugate of a matrix.  $\langle\cdot\rangle$  is expectation operator.  $\mathbb{N}$  is a set of natural numbers,  $\mathbb{R}$  is set notation for real numbers while  $\mathbb{C}$  is a set notation for complex numbers.  $\mathbb{E}$  is used to denote average of a quantity. These notations are as per standard notation found in quantum optics and quantum communication literature (Cariolaro, 2015)(Gerry et al., 2005). Additionally, we also assume that the information is not degraded due to thermal noise or other channel noise.



---

## BACKGROUND AND LITERATURE REVIEW

---

“ Optical communication systems are now enabling us to look beyond what naked eyes are able to perceive. In the search of unknowns, the light is taking us far beyond our physical limits, something that our ancestors had only imagined. ”

### 2.1 THE CONCEPT OF ‘INFORMATION’

In this section, we introduce the mathematical theory of information and target a philosophical question of what does it mean to have information with the help of mathematics. Information is considered as a sequence of some symbols transmitted via a medium called *channel*. We motivate this by asking ourselves, what does it mean to have one bit of information. It may seem like a philosophical question, but it can be answered intuitively as well as formally using mathematical tools. A bit is considered the smallest unit of information that can be used to convey binary information that takes only two values. For example, tossing a coin with prior knowledge that two sides of the coin are different and equally likely.

But mathematically, we can consider information to be a fraction. For example, tossing a coin that has a tail on both sides (and we know it), doesn’t provide any information. In this case, we have zero bit of information. Now consider a biased coin with a 75% chance of getting head and 25% of getting tail. In this case, when tossing a coin results in the tail, we are not transmitting the whole one bit but zero bit. The reason behind this is that we already provided a priori information that coin is biased. However, now it is a lot harder to tell how much information was resulted from the outcome of coin-toss.

Formalism behind this was developed by Claude Shannon, who is considered the father of information theory (Shannon, 1953). He stated that the fundamental concept behind information theory is *entropy*, which represents the amount of uncertainty in a string of symbols, given some knowledge of the distribution of the symbols. We discuss this concept in the next section.

#### 2.1.1 INFORMATION THEORY FOR PHOTON DETECTION

Information theory is an elegant mathematical construct, dealing with the transmission of symbols, provides an understanding of uncertainty embedded in those symbols given

their distributions. As an example, consider  $\{0, 1, 2, 3\}$  are communicated in binary as  $\{0, 1, 10, 11\}$ . If all digits are equally likely, then it takes  $\frac{6}{4} = 1.5$  bits on an average to communicate one digit. We have any alternative scheme: digits 0 and 1 are equally likely but 2 and 3 are 2 times and 4 times likely, respectively. Then

$$x + x + 2x + 4x = 1 \Rightarrow x = \frac{1}{8}$$

It means 0 and 1 occur at probability of  $\frac{1}{8}$ , 2 at  $\frac{1}{4}$  and 3 at  $\frac{1}{8}$ . In order to optimize the number of bits required for transmission, we may want to encode digits with high probability with a fewer number of bits:

$$2 \leftrightarrow 0, 3 \leftrightarrow 1, 0 \leftrightarrow 10, 1 \leftrightarrow 11$$

Hence, we see that it takes

$$\frac{1}{2} \times 1 + \frac{1}{4} \times 1 + \frac{1}{8} \times 2 + \frac{1}{8} \times 2 = 1.25$$

bits to communicate a single digit. This concept is referred to as **entropy**, the average number of bits required to transmit a packet of information. In this section, we build up a mathematical aptitude for information theory to optimize information transmission and other related concepts using probability theory and a famous **Shannon's information theory**.

### 2.1.1.1 Entropy and Shannon's Information Theory

Suppose we have a variable  $X$  that takes on one of  $n$  values with different probabilities:

- ♣  $p_1, p_2, \dots, p_n$  be the probabilities of  $n$  values.
- ♣ Let  $H$  – on an average – be the measure of amount of uncertainty removed by revealing the value of the random variable.
- ♣  $H$  should satisfy the following condition:
  - ★  $H$  is continuous at every  $p_i$ .
  - ★  $H$  is maximum when  $p_i = \frac{1}{n}$ .
- ♣ If choices are broken down into successive choices, then value of the measure  $H$  i.e. the amount of uncertainty revealed is the weight sum of the value of the two new choices.

Example:

$$H\left(\frac{1}{2}, \frac{1}{3}, \frac{1}{6}\right) = H\left(\frac{1}{2}, \frac{1}{2}\right) + \left(\frac{1}{2}\right)H\left(\frac{2}{3}, \frac{1}{3}\right)$$

The only function that satisfies the conditions for  $H$  mentioned above is

$$H(X) = - \sum_{i=1}^n p_i \log_2 p_i \quad (2.1)$$

### 2.1.1.2 Definiton of Entropy

Let  $P$  be a probability measure living on some space  $(\Omega, \mathcal{F})$ , where  $\Omega$  is the set of outcomes, and  $\mathcal{F}$  is the set of events, i.e. the collection of subsets of  $\Omega$  on which  $P$  is defined.  $X$  is a discrete random variable that satisfies:

$$X : \Omega \rightarrow \mathcal{X}, \quad \mathcal{X} \in \mathbb{R} \quad (2.2)$$

where  $\mathcal{X}$  is a discrete/countable set and  $X^{-1}(x) \in \mathcal{F} \quad \forall x \in \mathcal{X}$ . Thus all random variables are assumed to be discrete in our discussion. The random variable  $X$  induces probability measure  $p_X$  on  $(\mathcal{X}, 2^{\mathcal{X}})$ , where  $2^{\mathcal{X}}$  is the set of all subsets of  $\mathcal{X}$ . For any event  $E$  that is a subset of  $\mathcal{X}$ , i.e  $E \in \mathcal{X}$ ,

$$p_x(E) := \sum_{x \in E} P(\{\omega \in \Omega : X(\omega) = x\}) \quad (2.3)$$

For simplicity, we denote  $p_X$  by  $p$  and  $\{\omega \in \Omega : X(\omega) = x\}$  by  $\{X = x\}$ . If  $f$  is a real valued function on  $\mathcal{X}$ , then expected value  $E_p(f)$  is defined as

$$E_p(f) = \sum_{x \in \mathcal{X}} p(x)f(x) \quad (2.4)$$

**Definition 2.1.** For a random variable  $X$  with values in the discrete subset  $\mathcal{X} \in \mathbb{R}$ , its entropy  $H(X)$  is defined as

$$H(X) = - \sum_{x \in \mathcal{X}: p(x) \neq 0} p(x) \log_2 p(x) \quad (2.5)$$

As  $\log_2 p(x)$  defines a random variable on  $\mathcal{X}$  (omitting the point of probability 0), the entropy of  $X$  is equivalently the expected value:

$$H(X) = E_p(-\log_2 p). \quad (2.6)$$

It is not hard to guess from (2.6) that the larger the entropy, the more uncertainty there is about the values of  $X$ . For example,  $X = \Omega = \{1, 2, \dots, N\}$  and  $P$  has uniform distribution on  $\Omega$  i.e.  $p(\omega) = \frac{1}{N} \quad \forall \omega \in \Omega$ , then any bijection  $X : \Omega \rightarrow \mathcal{X}$  satisfies  $H(X) = \log_2 N$ , since  $p_X(x) = \frac{1}{N} \quad \forall x \in \mathcal{X}$ . Using the method of Lagrange's multipliers, the min value of the function  $p = (p_1, p_2, \dots, p_N) \mapsto \sum_{\{p: p_j \neq 0\}} p_j \log_2 p_j$  subject to constraint  $\sum_j p_j = 1$  is achieved when  $p_j = \frac{1}{N} \quad \forall j$ . Hence, given  $\Omega, \mathcal{X}$  and  $p$ , the maximum value of entropy is achieved when all values in  $X$  are equally likely. This argument shows that for any probability space  $(\Omega, P)$ , and any random variable  $X$  with values in finite site  $\mathcal{X}$  consisting of  $N$  elements,

$$0 \leq H(X) \leq \log_2 N. \quad (2.7)$$

Here,  $\log_2 N$  is the number of digits needed to represent all integers between 0 and  $N$  in binary. If  $X$  is constant and  $p(x) \in \{0, 1\}$  i.e. the probability is either 0 or 1, then

$$\begin{aligned} H(X) &= -0 \times \log_2(0) - 1 \times \log_2(1) \\ &= \lim_{y \rightarrow 0^+} y \log_2(y) - 1 \cdot 0 \\ &= 0 \end{aligned} \tag{2.8}$$

In this case, we find that there is no uncertainty about possible values of  $X$ .

Entropy can also be defined in terms of a probability  $p$  on  $\mathbb{N}$ , the set of positive integers given by

$$H(p) = - \sum_{j \in \mathbb{N}: p(j) \neq 0} p(j) \log_2 p(j). \tag{2.9}$$

### 2.1.2 POISSON POINT PROCESS

Consider quasi-monochromatic laser light pulse with constant angular frequency  $\omega_0$  and phase  $\phi$

$$\begin{aligned} \tilde{E}(\mathbf{r}, t) &= E(\mathbf{r}, t) e^{(-j\omega_0 t + \phi)}, \quad t \in (0, T] \\ &= \psi(\mathbf{r}) s(t) e^{(-j\omega_0 t + \phi)}, \quad \mathbf{r} \equiv (x, y) \end{aligned} \tag{2.10}$$

where  $\psi(\mathbf{r})$  is spatial mode and  $s(t)$  is temporal mode of Electric field  $E(\mathbf{r}, t)$ , but it should be noted that spatial and temporal dependence may not be factorizable in general. Equation (2.10) reasonably approximates an ideal single-mode laser operating well above threshold. The intensity  $\mathcal{I}$  of the beam is proportional to the square of the amplitude. We also assume no intensity fluctuations and average photon flux to be constant in time. It is considered there must be statistical fluctuations in the stream of photons on a short time scale due to the discrete nature of photons.

Now, with the above assumptions, we show that the arrival of photons is a Poisson point process. Let  $N(t)$  be the number of arrivals of photons before time  $t$ . Let  $K$  is the random variable used to denote  $N(t)$ . We are interested in finding out  $p[K = k] = P_K[k]$  that is total number of arrivals  $k$  given  $k \in \mathbb{Z}$ . If events occur at a rate  $\lambda$  per second then in time  $t$ , it is  $\lambda t$ . Before we proceed, we should keep in mind two assumptions hold in this regard:

1. Outcome in each subinterval is a Bernoulli trial. It is because the probability of finding  $k$  photons is equivalent to finding one photon in  $k$  time segments and no photons in  $(n - k)$  time segments, in any possible order, where  $n$  is the number of trials.
2. Whether or not an event occurs in a subinterval is independent of the outcomes in other intervals. That is, these Bernoulli trials are independent.

Thus the counting process  $N(t)$  can be approximated by the binomial distribution that counts the number of successes in the  $n$  Bernoulli trials. Thus the expected number of event

occurrences in time interval  $[0, t]$  is given by  $np$ . Thus  $\lambda t = np$ . If there are  $n$  Bernoulli trials, then  $k$  successes i.e.  $k$  arrivals is given by

$$\begin{aligned}
 P(K = k) &= \binom{n}{k} p^k (1-p)^{n-k} \\
 P(K = k) &= \binom{n}{k} \left(\frac{\lambda t}{n}\right)^k \left(1 - \frac{\lambda t}{n}\right)^{n-k} \\
 &= \frac{n!}{(n-k)!k!} \frac{\lambda^k t^k}{n^k} \left(1 - \frac{\lambda t}{n}\right)^n \left(1 - \frac{\lambda t}{n}\right)^{-k} \\
 &= \frac{n!}{(n-k)!n^k} \frac{\lambda^k t^k}{k!} \left(1 - \frac{\lambda t}{n}\right)^n \left(1 - \frac{\lambda t}{n}\right)^{-k} \\
 &= \frac{n(n-1)\cdots(n-k+1)}{n^k} \frac{\lambda^k t^k}{k!} \left(1 - \frac{\lambda t}{n}\right)^n \left(1 - \frac{\lambda t}{n}\right)^{-k} \\
 &= \frac{n^k + (\text{Polynomial of order } k-1 \text{ or less})}{n^k} \frac{\lambda^k t^k}{k!} \left(1 - \frac{\lambda t}{n}\right)^n \left(1 - \frac{\lambda t}{n}\right)^{-k} \\
 &= \left(1 + \frac{(\text{Polynomial of order } k-1 \text{ or less})}{n^k}\right) \frac{\lambda^k t^k}{k!} \left(1 - \frac{\lambda t}{n}\right)^n \left(1 - \frac{\lambda t}{n}\right)^{-k}
 \end{aligned} \tag{2.11}$$

As  $n \rightarrow \infty$ ,

$$\begin{aligned}
 P(K = k) &= \lim_{n \rightarrow \infty} \left(1 + \frac{(\text{Polynomial of order } k-1 \text{ or less})}{n^k}\right) \frac{\lambda^k t^k}{k!} \left(1 - \frac{\lambda t}{n}\right)^n \left(1 - \frac{\lambda t}{n}\right)^{-k} \\
 &= 1 \cdot \frac{\lambda^k t^k}{k!} \lim_{n \rightarrow \infty} \left(1 - \frac{\lambda t}{n}\right)^n \lim_{n \rightarrow \infty} \left(1 - \frac{\lambda t}{n}\right)^{-k} \\
 & \text{(As } \lim_{n \rightarrow \infty} f(x)g(x) = \lim_{n \rightarrow \infty} f(x) \lim_{n \rightarrow \infty} g(x) \text{ )} \\
 &= \frac{(\lambda t)^k}{k!} e^{-\lambda t} \cdot 1 \\
 & \text{(As } \lim_{x \rightarrow \infty} \left(1 + \frac{a}{x}\right)^x = e^a \text{ )}
 \end{aligned} \tag{2.12}$$

If the mean number of arrivals from time  $t = 0$  to time  $t = T$  is  $N$  then,  $N = \lambda T$  substituting  $t = T$  for total time  $T$  and  $N = \lambda T$  in above equation, we have:

$$P(K = k) = \frac{N^k}{k!} e^{-N} = \frac{e^{-N} N^k}{k!} \tag{2.13}$$

Thus we see that photon arrivals follow Poisson point process. A Poisson point process satisfies following property:

- $N(0) = 0$
- $\exists \lambda > 0$  such that for any  $0 \leq t_1 \leq t_2$ ,  $\mathbb{E}[N(t_2) - N(t_1)] = \lambda(t_2 - t_1)$ .

## 2.2 BRA- AND KET-NOTATIONS

In quantum mechanics, Bra-ket notation is a standard notation for describing quantum states, composed of angle brackets and vertical bars. It is so-called because inner product of two states is calculated by *bra*, and *ket* as  $\langle \phi | \psi \rangle$  where  $\langle \phi |$  is bra and  $|\psi \rangle$  is ket. The expression  $\langle \phi | \psi \rangle$  is typically interpreted as the probability amplitude for the state  $\psi$  to collapse into the state  $\phi$ . To understand the significance of notation, let's consider a vector  $\mathbf{A} \in \mathbb{R}^3$ . The vector  $\mathbf{A}$  can be written using any set of basis vectors and corresponding coordinate system. Informally basis vectors are like "building blocks of a vector", they are added together to make a vector, and the coordinates are the number of basis vectors in each direction. An elaborate discussion about the basis vector can be found out in the textbook (Axler, 1997). Using the most common Cartesian basis, vector  $\mathbf{A}$  can be written as

$$\begin{aligned}
 \mathbf{A} &= A_x \mathbf{e}_x + A_y \mathbf{e}_y + A_z \mathbf{e}_z \\
 &= A_x \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + A_y \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + A_z \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \\
 &= \begin{bmatrix} A_x \\ A_y \\ A_z \end{bmatrix}
 \end{aligned} \tag{2.14}$$

where  $\mathbf{e}_x, \mathbf{e}_y, \mathbf{e}_z$  are the Cartesian basis vectors. Generalizing it to N-dimension, a vector  $\mathbf{A}$  can be written as

$$\mathbf{A} = \sum_{n=1}^N A_n \mathbf{e}_n = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_N \end{bmatrix} \tag{2.15}$$

Even more generally,  $\mathbf{A}$  can be a vector in a complex Hilbert space. Some Hilbert spaces, like  $\mathbb{C}^n$ , have finite dimensions, while others have infinite dimensions. In an infinite-dimensional space, the column-vector representation of  $\mathbf{A}$  would be a list of infinitely many complex numbers. In bra-ket notation, Equation (2.14) can be written as

$$|A\rangle = A_x |e_x\rangle + A_y |e_y\rangle + A_z |e_z\rangle = \begin{bmatrix} A_x \\ A_y \\ A_z \end{bmatrix} \quad (2.16)$$

Similarly, this can be extended to N-dimensional vectors.

**Inner products:** In bracket notation, inner products of  $\mathbf{A}$  and  $\mathbf{B}$  can be written as  $\langle A|B\rangle$

and  $\langle A|B\rangle = A_1^* B_1 + A_2^* B_2 + A_3^* B_3 + \dots = [A_1^* \ A_2^* \ A_3 \ \dots \ A_N^*] \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_N \end{bmatrix}$ . From this

notation, it is obvious that bra notation  $\langle A|$  denotes a row vector,  $|B\rangle$  denotes a column vector and bra next to ket denotes matrix multiplication.

**Outer product:** A convenient way to define linear operators on  $H$  is given by the outer product  $|\phi\rangle\langle\psi|$ .  $|\phi\rangle\langle\psi|$  denotes the rank-one operator that maps the ket  $|\rho\rangle$  to the ket  $|\phi\rangle\langle\psi|\rho\rangle$  where  $\langle\psi|\rho\rangle$  is scalar multiplying the vector  $|\phi\rangle$ . Further, conjugate transpose of bra is equal to ket and vice-versa, i.e.,  $\langle A|^\dagger = |A\rangle$ . In quantum mechanics, it is common practice to write down kets that have an infinite norm, i.e. non-normalizable wavefunctions. Examples include states whose wavefunctions are Dirac delta functions or infinite plane waves. These do not, technically, belong to the Hilbert space itself. However, the definition of "Hilbert space" can be broadened to accommodate these states (refer to the Gelfand–Naimark–Segal construction or rigged Hilbert spaces). The bra-ket notation continues to work analogously in this broader context. Banach spaces are a different generalization of Hilbert spaces. In a Banach space  $\mathcal{B}$ , the vectors may be notated by kets and the continuous linear functionals by bras. Over any vector space without topology, we may also notate the vectors by kets and the linear functionals by bras. In these more general contexts, the bracket does not have the meaning of an inner product, because the Riesz representation theorem does not apply (Goodrich, 1970).

### 2.2.1 USAGE OF BRAKET IN QUANTUM MECHANICS

Wave functions and other quantum states can be represented as vectors in a complex Hilbert space. In bra-ket notation, for example, an electron might be in the state  $|\psi\rangle$ . Quantum superpositions can be described as vector sums of the constituent states. An electron in the state  $|1\rangle + i|2\rangle$  is in a quantum superposition of  $|1\rangle$  and  $|2\rangle$ . The description of complete knowledge of a system is termed as pure state of the system. The pure state of a system is described by a column vector or  $|\psi\rangle$  in ket-notation.  $|\psi\rangle$  is a unit-norm column vector and  $\langle\psi|$  is its complex conjugate which is a unit-norm row vector. The unit-norm condition

is defined by  $\langle\psi|\psi\rangle = 1$ . For example, a qubit (two-level system) can be written as  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  where  $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$  and  $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$  are orthonormal basis. The unit-norm is given by  $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$ .

### 2.2.2 MEASUREMENTS IN QUANTUM SYSTEM

Measurements in Quantum mechanics mean applying some form of operation on qubits to get classical bits. This is pictorially represented in Figure 2.1

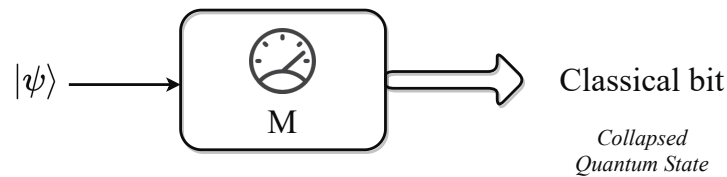


Figure 2.1: Measuring a Quantum bit

To understand the measurements in a quantum system, we need to look at two postulates:

- **Postulate 1:** If you have an isolated quantum system, there exists a complex vector-space with an inner-product attached to that system, called the state space.
- **Postulate 2:** Give a closed quantum system, the evolution of the system is governed by a unitary transformation

$$|\psi'\rangle = U|\psi\rangle$$

where  $U$  is a unitary matrix<sup>1</sup>. In general, for continuous system, the unitary transformation is given by Equation (2.30).

Hence, the description of measurement in terms of the measurement operators should be taken as a postulate of quantum mechanics. That is, it cannot be derived, but instead defines the mathematical structure of quantum mechanics.

### 2.2.3 PROJECTIVE MEASUREMENTS (VON NEUMANN MEASUREMENTS)

If we measure a quantum state along some orthonormal basis  $|0\rangle$  and  $|1\rangle$  as discussed in Section 2.2.1, then we can treat the measurement as ‘normal measurement’ or ‘regular measurement’. However, if we want to represent the quantum state along with some other basis, then we have to first project the quantum state onto the measurement basis vectors. The new measurement of the given quantum state is called projective measurement (also known as Von Neumann measurements) and the length of the projection on the basis vector gives

<sup>1</sup>Unitary matrix is a matrix whose product with its adjoint yields the identity matrix.



us the probability of collapsing to that basis vector. Formally, Von Neumann measurement on a state is described by a set of unit-norm orthonormal vectors

$$\{|w_k\rangle\}, \langle w_k|w_j\rangle = \delta_{kj} \quad (2.17)$$

In this case, if a state  $|\psi\rangle$  is measured, the k-th outcome appears with probability  $p_k = |\langle w_k|\psi\rangle|^2$ .

As an example, we will represent a qubit's state in different orthonormal bases. First, we define a  $45^\circ$  rotated basis

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \quad (2.18)$$

Then we express a state  $|\psi\rangle$  as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \gamma|+\rangle + \delta|-\rangle \quad (2.19)$$

1. Write down  $\gamma$  and  $\delta$  in terms  $\alpha$  and  $\beta$ .
2. What are the probabilities of measurement outcomes when measured in the  $\{0,1\}$  basis, and when measured in  $\{+, -\}$ .

Equation 2.18 can be broken down into two Equations as

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad (2.20)$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (2.21)$$

From Equations 2.20 and 2.21, we can get :

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \quad (2.22)$$

$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \quad (2.23)$$

Putting RHS of these Equations in 2.19,

$$\begin{aligned} \alpha \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) + \beta \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) &= \gamma|+\rangle + \delta|-\rangle \\ |+\rangle \left( \frac{\alpha}{\sqrt{2}} + \frac{\beta}{\sqrt{2}} \right) + |-\rangle \left( \frac{\alpha}{\sqrt{2}} - \frac{\beta}{\sqrt{2}} \right) &= \gamma|+\rangle + \delta|-\rangle \end{aligned} \quad (2.24)$$

Comparing both sides, we get

$$\begin{aligned}\gamma &= \left( \frac{\alpha}{\sqrt{2}} + \frac{\beta}{\sqrt{2}} \right) \\ \delta &= \left( \frac{\alpha}{\sqrt{2}} - \frac{\beta}{\sqrt{2}} \right)\end{aligned}\tag{2.25}$$

In  $\{0, 1\}$  basis:

$$p_0 = |\langle 0|\psi\rangle|^2 = |\langle 0|\alpha|0\rangle + \beta|1\rangle|^2 = |\alpha|^2\tag{2.26}$$

Similarly,

$$p_1 = |\langle 1|\psi\rangle|^2 = |\langle 1|\alpha|0\rangle + \beta|1\rangle|^2 = |\beta|^2\tag{2.27}$$

In  $\{+, -\}$  basis,

$$\begin{aligned}p_+ &= |\langle +|\psi\rangle|^2 = \left| \left\langle + \left| \left( \frac{\alpha}{\sqrt{2}} + \frac{\beta}{\sqrt{2}} \right) |+\rangle + \left( \frac{\alpha}{\sqrt{2}} - \frac{\beta}{\sqrt{2}} \right) |-\rangle \right\rangle \right|^2 \\ &= \left| \left( \frac{\alpha}{\sqrt{2}} + \frac{\beta}{\sqrt{2}} \right) \right|^2\end{aligned}\tag{2.28}$$

and,

$$\begin{aligned}p_- &= |\langle -|\psi\rangle|^2 = \left| \left\langle - \left| \left( \frac{\alpha}{\sqrt{2}} + \frac{\beta}{\sqrt{2}} \right) |+\rangle + \left( \frac{\alpha}{\sqrt{2}} - \frac{\beta}{\sqrt{2}} \right) |-\rangle \right\rangle \right|^2 \\ &= \left| \left( \frac{\alpha}{\sqrt{2}} - \frac{\beta}{\sqrt{2}} \right) \right|^2\end{aligned}\tag{2.29}$$

### 2.3 LASER PULSES AND DETECTION OF PHOTON

Although photons (in free space) have a definite energy, momentum relation, photons are not ‘objects’ in the sense of individual localizable classical particles. As a result, the classical theory fails to account for the detection of photons. However, using canonical quantization, based on Hamiltonian form, state vectors, and Schrödinger equations, we can “predict” states of photons. In this case, states of photons are described by (normalized) state vectors  $|\Psi\rangle$  which are elements of a Hilbert space  $\mathcal{H}$  with a scalar product

$$\langle \Psi_1 | \Psi_2 \rangle = \langle \Psi_2 | \Psi_1 \rangle^* .$$

A detail discussion on state vectors and their quantum mechanical aspects can be found in (Griffiths and Schroeter, 2018; Milonni and Eberly, 2010). Initially, the system is supposed to be in state  $|\Psi_0\rangle = |\Psi(t)\rangle$ , Then, sequence of state  $|\Psi(t)\rangle$  which the system runs through as a function of time is governed by Schrödinger equation

$$i\hbar \frac{\partial |\Psi(t)\rangle}{\partial t} = \hat{H} |\Psi(t)\rangle \quad (2.30)$$

where  $\hat{H}$  denotes Hamiltonian  $\equiv$  energy of the system. State vectors  $|\Psi\rangle$  describe pure states with zero entropy. The stationary states of a free harmonic oscillator  $|n\rangle$ ,  $n = 0, 1, \dots$  are eigenstates of the number operator  $\hat{N} = \hat{a}^\dagger \hat{a}$  where  $a$  represent the dynamical variables of the electromagnetic field (EMF). In addition, they are non-degenerate, orthogonal, and normalizable,  $\langle m|n\rangle = \delta_{m,n}$ . They define

$$\begin{aligned} \hat{a}^\dagger \hat{a} &= n |n\rangle \\ \hat{a} |n\rangle &= \sqrt{n} |n-1\rangle \\ \hat{a}^\dagger |n\rangle &= \sqrt{n+1} |n+1\rangle \end{aligned} \quad (2.31)$$

These operators are also called as *ladder operators*, because repeated operations on a particular energy eigenstate create the *ladder* of all other states, with  $\hat{a}^\dagger$  we climb up, whereas with  $\hat{a}$  we climb down the ladder.

### 2.3.1 STATE OF QUANTUM SYSTEM

The nature of the photon can be well understood using quantum mechanics. Although unintuitive, quantum mechanics describes concrete features of the world as we know it which has been proven repeatedly through experiments such as double-slit experiments, photoelectric effect, and black-body radiation. If we take a system as quantum, it is described by a complex function  $\Psi$  which varies with position and time.  $\Psi$  called as a wave function that does not depend on the momentum of the particle. The wave function encodes all the information about the system, although in a probabilistic sense.  $|\Psi(x, t)|^2 dx$  is the probability that a measurement of the position of the particle yields a result in the interval  $x \rightarrow x + dx$ . The total probability of finding the particle somewhere along the real axis must be unity and is given by

$$\|\Psi\|^2 = \int |\Psi(x, t)|^2 dx = 1 \quad (2.32)$$

A function such that its integral along the real axis is finite can be normalized by multiplying by an appropriate constant. Two wave functions that differ by an arbitrary factor  $c \in \mathbb{C}$  describes the same physical system.

## 2.4 COHERENT STATE (IDEAL SINGLE MODE LASER)

We are interested in a special state in which the fields vary sinusoidally in space and time with time-independent uncertainties in quadrature amplitude with  $\Delta X_1 = \Delta X_2 = \frac{1}{2}$  and  $\Delta X_1 \Delta X_2 = \frac{1}{4}$ . These states are called as Gaussian ground state wavefunctions. In number states, these states are given by

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad \alpha = x_c + ip_c$$

$x_c$  corresponds to classical position operator,  $p_c$  corresponds to classic momentum operator. (2.33)

$|\alpha\rangle$  are called coherent states.  $|\alpha\rangle$  states have number of interesting properties such as

- $|\alpha\rangle$  is an eigenstate of the destructor operator

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle$$

where  $a$  is a non-hermitian operator and  $\alpha = |\alpha|e^{i\phi} \in \mathbb{C}$  is a complex number and corresponds to the complex wave amplitude in classical optics. Thus coherent states are wave-like states of the electromagnetic oscillator.

- $\alpha$ -states can be generated by unitary displacement operator  $\hat{D}$ :

$$\begin{aligned} |\alpha\rangle &= \hat{D}(\alpha) |0\rangle \\ \hat{D}(\alpha) &= e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{-\alpha\hat{a}} \\ \hat{D}^\dagger \hat{a} \hat{D} &= \hat{a} + \alpha \end{aligned} \quad (2.34)$$

- Time independence is obtained by replacing  $\alpha$  by  $\alpha(t)$ :

$$|\alpha, t\rangle = e^{i\phi(t)} |\alpha(t)\rangle$$

For a free oscillator,  $\alpha(t) = \alpha e^{-i\omega t}$ .

- Although the  $\alpha$ -eigenvalues form a continuous spectrum, the  $|\alpha\rangle$  states are normalized but they are not orthogonal. Moreover, the set  $|\alpha\rangle$  states is complete and forms a convenient basis for an *almost classical description* of laser physics.

Expectation values, uncertainties of the electric field and photon number and probability to measure  $n$  photons(omitting the polarization index) are

$$\begin{aligned} \tilde{E}(\mathbf{r}, t) &= \langle \alpha(t) | \hat{E}(t) | \alpha(t) \rangle \\ &= -2E_0 |\alpha| \sin(\mathbf{k}\mathbf{r} - \omega_k t + \phi) \end{aligned} \quad (2.35)$$

$$(\Delta \tilde{E})^2 = E_0^2 \quad (2.36)$$

$$\begin{aligned}\langle \hat{N} \rangle &= |\alpha|^2 = N \\ &= (\Delta \hat{N})^2\end{aligned}\tag{2.37}$$

$$p_k = |\langle k|\alpha \rangle|^2 = e^{-N} \frac{N^k}{k!}\tag{2.38}$$

Also,  $\alpha = |\alpha|e^{j\phi}$  and  $N = |\alpha|^2 \Rightarrow |\alpha| = \sqrt{N}$ . Hence,

$$\alpha = \sqrt{N}e^{j\phi}\tag{2.39}$$

where  $N$  is the mean photon number, also given by

$$\begin{aligned}N &= \int_0^T \int_{\mathcal{A}} |\tilde{E}(\mathbf{r}, t)|^2 d\mathbf{r} dt \\ &= \int_0^T \int_{\mathcal{A}} |E(\mathbf{r}, t)|^2 d\mathbf{r} dt \quad (\text{Using (2.10)})\end{aligned}\tag{2.40}$$

where  $\mathcal{A}$  is aperture area. It should be noted that no detector can accurately measure the field  $E(\mathbf{r}, t)$ . Here the relative amount of fluctuation in the electric field decreases with increasing amplitudes. In above equations,  $p_k$  denotes a Poisson distribution with mean photon number  $N = |\alpha|^2$  and uncertainty  $(\Delta k)^2 = N$ . Thus in a coherent state, photon behaves like they were uncorrelated classical objects. In contrast to naive expectations, the photons in a single-mode laser and well above threshold arrive randomly; in practice, they don't ride on electric field maxima.

#### 2.4.1 IDEAL PHOTON DETECTION OF SQUARE PULSE

Consider an optical square pulse<sup>2</sup> as shown in Figure 2.2.  $s(t)$  is the temporal shape of the pulse with the unit of  $\sqrt{\text{photon/s}}$ . Actually,  $s(t)$  is the amplitude of the electric field of the pulse. Square of the magnitude of  $s(t)$  gives square of electric field. Integrating the square of the magnitude of the pulse  $s(t)$  over the pulse duration gives mean number of the photon:



**Figure 2.2:** A Square Pulse

$$s(t) = \begin{cases} E, & t \in [0, T] \\ 0, & \text{otherwise} \end{cases}\tag{2.41}$$

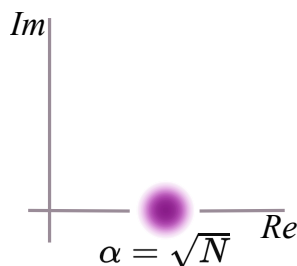
<sup>2</sup>In reality there is no such thing as square pulse due to ripple effect and many other factors.

$$\lambda(t) = |s(t)|^2 = \lambda = E^2, \quad t \in [0, T] \quad (2.42)$$

$$N = \int_0^T \lambda(t) dt = \lambda T = E^2 T \quad (2.43)$$

Here, photon square pulse simply generates a Poisson point process where the arrival of the photons are associated with clicks (shown with a red cross sign in Figure 2.2), i.e. these are the timestamps when (an ideal) detector says ‘I saw a photon’. These arrival timestamps come at the rate of  $\lambda = E^2$ .

We are going to define one more thing in the following paragraph:  $\alpha$ , coherent state, already seen in Equation (2.39). We can think of  $\alpha$  as associated with the pulse once we define the shape of the pulse. In this case, only the complex number  $\alpha$  is needed to describe the state of the pulse. In this case,  $\alpha = \sqrt{N}$  (Figure 2.3). It will be more clear in the later discussion.



**Figure 2.3:** Mean photon number

In above discussion, we didn’t include carrier phase. Along with the shape or envelope of the optical pulse, there will always be an oscillating phase. Frequency of the oscillating phase is the center frequency of the optical pulse. After including oscillating phase, we can write the pulse equation as:

$$s(t) = \begin{cases} Ee^{j\phi}, & t \in [0, T] \\ 0, & \text{otherwise} \end{cases} \quad (2.44)$$

If we want to denote the same pulse with oscillating phase, we include an additional term  $e^{j\phi}$  as shown in Figure 2.4. It should be noted that the oscillatory part doesn’t affect the detection statistics about the pulse. But if we want to describe the state of the pulse before detection, we need  $\alpha$  and  $\phi$ . In general  $s(t)$  doesn’t have to be constant but can vary with time over the same pulse duration  $T$ . In this case the, rate of arrival of the PPP will be a function of time, i.e if the square pulse is  $s(t)e^{-j\omega_0 t + \phi}$  then detector will produce clicks at a rate of  $\lambda(t) = |s(t)|^2$ . Mean photon number simply will be  $N = \int_0^T \lambda(t) dt$ .

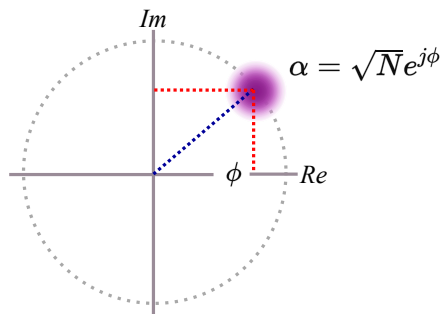


Figure 2.4: Mean photon number with oscillating phase

## 2.5 DISCRIMINATION OF STATES

We consider an ensemble of quantum systems with each systems on one of the  $N$  possible states given by their density operators  $\rho_1, \rho_2, \dots, \rho_N$  each with prior probabilities  $p_1, p_2, \dots, p_N$  such that  $\sum_{k=0}^N p_k = 1$ . Even though an observer performing the state discrimination might have full knowledge of ensemble, he doesn't know which one of those  $N$  states he has. To determine the state, the observer is required to make a measurement. State discrimination is required by the observer to estimate one of the  $N$  states observers may have.

One common strategy for state discrimination is through minimum error probability. Helstrom (Helstrom, 1969) outlined an optimal measurement strategy for an ensemble of two quantum states. The optimum measurement strategy is called the Helstrom measurement and the minimum error is referred to as the Helstrom bound. If we consider a POVM  $\Pi_k$  corresponding to state  $\rho_k$ , then as per the postulates of quantum mechanics, the probability of guessing  $\rho_k$  is  $\text{tr}\{\rho \Pi_k\}$ , if the actual state is  $\rho$ . The guess work is correct when  $\rho = \rho_k$ . In such case, the probability of correct classification is

$$P_c = \sum_{k=1}^N p_j \text{tr}\{\rho_k \Pi_k\} \quad (2.45)$$

and the error probability is given by

$$P_e = 1 - P_c \quad (2.46)$$

We minimize  $P_e$  over all possible set of  $\Pi_k$  in order to minimize the error. In some cases, it is not possible to find optimal measurements. In such cases, we have another scheme called square-root measurement (Eldar and Forney, 2001; Hausladen and Wootters, 1994). For a given set of  $N$  states, we can write the following POVM elements of square-root measurement:

$$\Pi_k = p_k \rho_i^{-1/2} \rho^{-1/2} \quad \forall i \in [1, N] \quad (2.47)$$

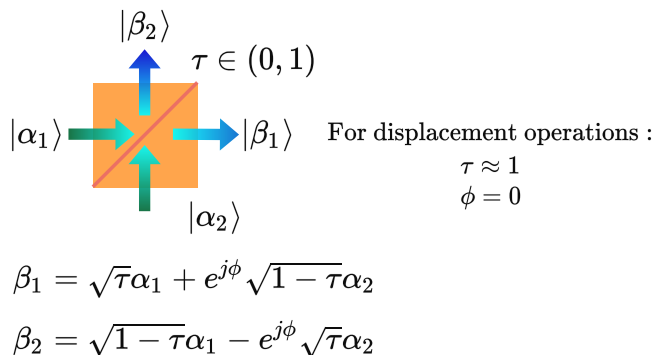
where  $\rho = \sum_{k=1}^N p_k \rho_k$ . The POVM elements of Equation (2.47) satisfies the properties of positivity and completeness. For most cases, minimum error probability measurement turns to be square-root measurement.

State discrimination plays a crucial role in quantum error correction. Further, the state discrimination of quantum states is at the center of quantum computation and communication. The strategy of state discrimination depends on the given task in quantum information science. As an example, using state discrimination methods, we can demonstrate that quantum mechanics doesn't allow discrimination between two non-orthogonal states  $|\psi_0\rangle$  and  $|\psi_1\rangle$ . The non-discrimination of non-orthogonal states makes quantum key distribution possible (Djordjevic, 2019c).

## 2.6 BEAMSPLITTER AND MIXING OPERATION

Classically, a 50-50 beamsplitter divides the intensity of an incoming light beam into two. However, quantum-mechanically, it won't split each photon into two, but rather it transmits or reflect each photon with 50% probability. A beamsplitter combines and splits two input coherent states  $|\alpha_1\rangle$  and  $|\alpha_2\rangle$ . A beamsplitter is represented by Unitary operator  $U(\theta, \phi)$  with transmittivity  $\tau = \cos^2 \theta$  and phase  $\phi$  such that input output relationship can be written as

$$\begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} = U \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix}, \quad U = \begin{bmatrix} \cos \theta & e^{j\phi} \sin \theta \\ \sin \theta & -e^{j\phi} \cos \theta \end{bmatrix} \quad (2.48)$$



**Figure 2.5:** A schematic diagram showing a beamsplitter's operation as a displacement operator. A beamsplitter acts as a displacement operator when a laser beam of a coherent state amplitude  $\alpha_1$  is mixed with a strong local oscillator of amplitude  $\alpha_2$ .

The displacement operator  $D(\beta)$  shifts the amplitude of the coherent state as  $D(\beta)|\gamma\rangle = |\gamma + \beta\rangle$ . The displacement operator is realized by a beamsplitter of transmittivity  $\tau \approx 1$  and



a strong local oscillator of amplitude  $\frac{\beta}{\sqrt{1-\tau}}$  (Takeoka and Sasaki, 2008). We can describe a beamsplitter as a displacement operator as follows. Using trigonometric identities, assume

$$\begin{aligned}\tau &= \cos^2 \theta \\ \Rightarrow \sin \theta &= \pm\sqrt{1-\tau} \text{ and } \cos \theta = \pm\sqrt{\tau}\end{aligned}\tag{2.49}$$

Taking only + sign without the loss of generality (negative sign just flips states on constellation diagram across y-axis) and putting in Equation (2.48), we obtain:

$$\begin{aligned}\begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} &= \begin{bmatrix} \sqrt{\tau} & e^{j\phi}\sqrt{1-\tau} \\ \sqrt{1-\tau} & -e^{j\phi}\sqrt{\tau} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} \\ \Rightarrow \beta_1 &= \sqrt{\tau}\alpha_1 + e^{j\phi}\sqrt{1-\tau}\alpha_2 \\ \text{and, } \beta_2 &= \sqrt{1-\tau}\alpha_1 - e^{j\phi}\sqrt{\tau}\alpha_2\end{aligned}\tag{2.50}$$

To perform the displacement operation using a beamsplitter, we set  $\phi = 0$  and use a beamsplitter with transmittivity  $\tau$  close to 1 (but not exactly one, and in practice transmittivity can never be unity). One arm of the beamsplitter is fed with desired laser beam with coherent state amplitude of  $\alpha_1 = \gamma$  while another arm is given a strong local oscillator of amplitude  $\alpha_2 = \frac{\beta}{\sqrt{1-\tau}}$ . Essentially with this design, we only need laser beam of the coherent state amplitude  $\gamma$  as an input. Putting the input values in Equation (2.50), we obtain:

$$\begin{aligned}\beta_1 &= \gamma + \sqrt{1-\tau} \cdot \frac{\beta}{\sqrt{1-\tau}} = \gamma + \beta \\ \beta_2 &= \gamma\sqrt{1-\tau} - \frac{\beta}{\sqrt{1-\tau}}\end{aligned}\tag{2.51}$$

with an approximation of  $\sqrt{\tau} \approx 1$ . The displacement operation ignores the second output from the beamsplitter. A schematic representation of beamsplitter acting as a displacement operator is shown in Figure 2.5. We denote the overall displacement procedure as an operator  $D(\beta)$  where  $\beta$  is the displacement produced on a laser beam's coherent state amplitude after passing through the beamsplitter.

In addition to displacement operation, the beamsplitter can be used to generate entangled state using two-mode mixing and two-mode squeezing that we discuss in Section 2.8.

## 2.7 SQUEEZED-STATES

A quantum system consisting of  $M$  bosonic modes can be described by quadrature operators  $\{I_m, Q_m\}_{m=1}^M$ . They can be written in vector form as  $\hat{\mathbf{x}} = [I_1 Q_1, \dots, I_M Q_M]^T$ . These quadrature operators satisfy the commutation relation  $[\hat{x}_m, \hat{x}_n] = 2j\Omega_{mn}$  where  $\Omega_{mn}$  is

mth-row, nth-column element of  $2M \times 2M$  matrix

$$\Omega = \begin{bmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{bmatrix}, \quad \omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad (2.52)$$

which is called symplectic form. For the quadrature operator, the first moment of  $\hat{x}$  represents the displacement which is given by

$$\bar{x} = \langle \hat{x} \rangle = \text{tr}\{\hat{x}\rho\} \quad (2.53)$$

The elements of covariance matrix  $\Sigma$  is given by

$$\sigma_{mn} = \frac{1}{2} \left( \langle \hat{x}_m, \hat{x}_n \rangle + \langle \hat{x}_n, \hat{x}_m \rangle \right) - \langle \hat{x}_m \rangle \langle \hat{x}_n \rangle \quad (2.54)$$

where  $\langle \cdot, \cdot \rangle$  is the anticommutator. The diagonal elements of covariance matrix are variances of the quadratures given by

$$V(\hat{x}_i) = \langle (\hat{x}_i)^2 \rangle - \langle \hat{x}_i \rangle^2. \quad (2.55)$$

The first moment i.e. mean and variance are enough to completely characterize the density operator  $\rho$ , i.e.  $\rho \equiv \rho(\bar{x}, V)$ . Thus, they represent the Gaussian states.

A *squeezed state* is a Gaussian state which has unequal fluctuations in quadratures:  $V(I) = e^{2r}$  and  $V(Q) = e^{-2r}$  where  $r$  is squeezing amplitude. In such case, we can define a more general version of coherent state as squeezed-displaced state given by

$$|z, \alpha\rangle = D(\alpha)S(z)|0\rangle, \quad S(z) = e^{\frac{1}{2}(za^\dagger 2 - z^* a^2)} \quad (2.56)$$

where  $S(z)$  is the squeezing operator,  $z = re^{j\theta}$  is the squeezing factor with  $r$  being squeezing amplitude and  $\theta$  being squeezing phase. In practice  $r$  is real and thus squeezing operator simplifies to  $S(z) = \exp\{z(a^\dagger 2 - a^2)/2\}$ .

When we set  $r = 0$ , squeezed state is effectively a coherent state. Squeezed states lead to following notations:

1.  $|z, \alpha\rangle$ : squeezed-displaced state
2.  $|0, \alpha\rangle = |\alpha\rangle$ : coherent state
3.  $|z, 0\rangle$ : squeezed vacuum state

Squeezed states live in an infinite-dimensional Hilbert state. Squeezed-displaced states are specified by Fock expansion.

The Equation (2.56) leads to following eigenvalue problem, derivation of which is provided in (Djordjevic, 2022):

$$(a \cosh(r) - a^\dagger e^{j\theta} \sinh(r)) \left| re^{j\theta}, \alpha \right\rangle = (\alpha \cosh(r) - \alpha^* e^{j\theta} \sinh(r)) \left| re^{j\theta}, \alpha \right\rangle \quad (2.57)$$

If we want to represent squeezed-displaced states in terms of Fock state, we may have following expansion:

$$|z, \alpha\rangle = \sum_n C_n |n\rangle \quad (2.58)$$

Equation (2.58) must satisfy Equation (2.57). We can make a guess of the form of  $C_n$  as

$$C_n = K \left( \frac{1}{2} e^{j\theta} \tanh(z) \right)^{n/2} h_n(x), \quad x \in \mathbb{C} \quad (2.59)$$

where  $K$  is the normalization constant and  $h_n$  is the recursive function. We can find  $C_n$  by equating coefficients of  $n$ th terms which gives the recursive function  $h_n$  as

$$h_n(x) = \frac{2x}{\sqrt{n}} h_{n-1}(x) + 2\sqrt{\frac{n-1}{n}} h_{n-2}(x) \quad (2.60)$$

$$h_0(x) = \frac{C_0}{K} \quad (2.61)$$

$$h_1(x) = 2x h_0(x) \quad (2.62)$$

Coefficient  $C_0$  can be obtained by solving  $C_0 = \langle 0|z, \alpha\rangle = \langle 0|D(\alpha)S(z)|0\rangle$  which gives  $C_0$  as

$$C_0 = (\cosh(r))^{-1/2} \exp\left\{-\frac{1}{2}|\alpha|^2 + \frac{1}{2}\alpha^* e^{j\theta} \tanh(r)\right\} \quad (2.63)$$

We choose  $h_0(x) = 1$  by setting  $K = C_0$ . Thus the Fock state expansion of squeezed-displaced state is

$$|z, \alpha\rangle = (\cosh(r))^{-1/2} \exp\left\{-\frac{1}{2}|\alpha|^2 + \frac{1}{2}\alpha^* e^{j\theta} \tanh(r)\right\} \sum_{n=0}^{\infty} \left(\frac{1}{2} e^{j\theta} \tanh(r)\right)^{n/2} h_n\left(\frac{\beta}{\sqrt{e^{j\theta} \sinh(2r)}}\right) |n\rangle \quad (2.64)$$

where  $\beta = \alpha \cosh(r) - \alpha^* e^{j\theta} \sinh(r)$ .

## 2.8 ENTANGLED STATE

When two photons arrive at a beamsplitter at exactly the same time, with frequency and polarization close enough so that they emerge from the beamsplitter with their origins impossible to know, we get entangled photons. An entangled two-mode Gaussian state can be prepared by passing two single-mode squeezed vacuum states with each of them squeezed along axes orthogonal to each other into the two input ports of a 50-50 beamsplitter.

Loosely speaking, entanglement is a type of correlation, called as Einstein-Podolsky-Rosen (EPR) correlation that is specific to quantum mechanics. An entanglement state is defined to be one whose quantum state cannot be factored as product states of its local constituents. In other words, they are individual particles but inseparable as a whole. As an example, given two basis vectors  $\{|0\rangle_A, |1\rangle_A\}$  in Hilbert space  $\mathcal{H}_A$  and  $\{|0\rangle_B, |1\rangle_B\}$  in Hilbert space  $\mathcal{H}_B$ , then the following is an entangled state:

$$\frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \quad (2.65)$$

If a composite system is in the state (2.65), it is impossible to attribute either system A or B a definite pure state. Even if the von Neumann entropy of the whole state is zero, the entropy of the subsystem is greater than zero. In this sense, we can say that the systems are entangled.

Quantum teleportation is at the heart of entanglement. Quantum teleportation tells that once we determine the value or a state of one part of the entangled state, the state of other part will automatically be known using some mathematical operation. If two photons come into contact with one another, they become entangled. Later, if one photon is measured by linear polarizer to have, say, a vertical polarization, then the other photon's state collapses to horizontal polarization. One important entity in teleportation is entangled qubit. The measurement of the joint states of multiple qubits performed in the basis of four maximally entangled states, known as Bell states or EPR states are

$$\begin{aligned} |\Phi_A\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) \\ |\Phi_B\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \\ |\Phi_C\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \\ |\Phi_D\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \end{aligned} \quad (2.66)$$

In quantum teleportation scheme, a qubit can be transmitted from one place to another by using classical communication, given that Alice and Bob have previously received each one half of two-qubit entangled state. For an example, if Alice has a qubit 1 in the state  $|q\rangle_1 = a|0\rangle_1 + b|1\rangle_1$  with  $a$  and  $b$  unknown amplitude such that  $|a|^2 + |b|^2 = 1$ . Further, if Alice has qubit 2 entangled to Bob's qubit 3 being in one of the EPR states, refer to as  $|\Phi\rangle_{23}$ . In this example, the goal of teleportation would be to transmit the state of qubit 1 possessed by Alice to bob. The initial state  $|q\rangle_1 |\Phi\rangle_{23}$  can be rewritten in Bell's basis as

$$\begin{aligned} &\frac{1}{2} \left[ |\Phi_A\rangle_{12} (a|0\rangle_3 + b|1\rangle_3) + |\Phi_B\rangle_{12} (a|0\rangle_3 - b|1\rangle_3) \right. \\ &\quad \left. - |\Phi_C\rangle_{12} (a|1\rangle_3 + b|0\rangle_3) + |\Phi_D\rangle_{12} (a|1\rangle_3 - b|0\rangle_3) \right] \end{aligned} \quad (2.67)$$

Here, we omit the global phase term  $e^{j\pi} = -1$ . Alice can measure the joint state of qubits 1 and 2 on Bell's basis and obtain one of the four results 00, 01, 10, 11 in the classical sense. Irrespective of what states qubits are in, Alice's measure will give a uniformly distributed random two classical bits. If the measured qubits 1 and 2 are found to be in  $|\Phi_A\rangle_{12}$ , then Alice's output is 00 and thus Bob's output would be  $|p\rangle_3 = a|0\rangle_3 + b|1\rangle_3$ , which is the initial state of Alice's  $|q\rangle_1$ , without a need to apply for any additional transformation. If qubits 1 and 2 are found to be in  $|\Phi_B\rangle$ , then Alice's output is 01 and Bob's state would be  $|p\rangle_3 = a|0\rangle_3 - b|1\rangle_3$  which indeed differs from  $|q\rangle_1$ . But if we apply a phase flip operation, realized by Pauli operator  $U_B$ , Bob gets the state as  $a|0\rangle_3 - b|1\rangle_3$  which is same as  $|q\rangle_1$ . For the case of C and D, Bob needs to apply a bit flip and (a bit flip + phase flip) respectively. Hence, for successful teleportation, Alice and Bob must have some pre-shared information.

## 2.9 SPONTANEOUS PARAMETRIC DOWNCONVERSION

Spontaneous parametric downconversion (SPDC) is a process of generating entangled photons where a nonlinear crystal is used to split a photon into a pair of photons such that the state of one photon is complementary to the state of another photon. Two photons generated in the process of SPDC are called signal-idler pairs for historical reasons. SPDC process uses a nonlinear optical phenomenon where the response of a medium to an applied optical field is mediated by the electric polarization of the medium. If we consider a polarization

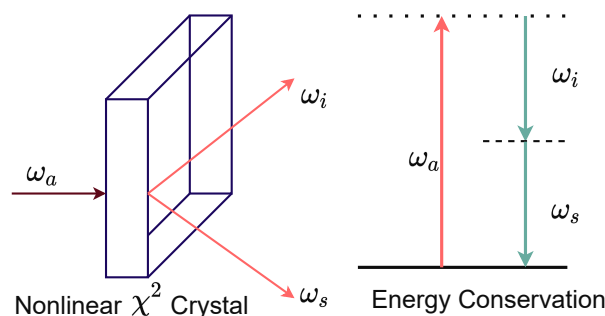
$$\mathcal{P}(t) = \epsilon_0 \left[ \chi^{(1)} \mathcal{E}(t) + \chi^{(2)} \mathcal{E}^2(t) + \dots \right] \quad (2.68)$$

where  $\mathcal{P}$  is polarization,  $\mathcal{E}$  is the electric field, and  $\chi^{(n)}$  is nonlinear susceptibility of order  $n$ . The electric field is usually composed of one or more frequencies (Lopez-Mago, 2012; Christ et al., 2013). For simplicity, we can assume that the electric field consists of two frequencies  $\omega_1$  and  $\omega_2$  such that  $\mathcal{E}(t) = \mathcal{E}_1 e^{-j\omega_1 t} + \mathcal{E}_2 e^{-j\omega_2 t} + c.c.$ . In our formulation, *c.c.* stands for complex conjugate of the previous terms. Using second order susceptibility from Equation (2.68), we can write an expression of nonlinear polarization as

$$\begin{aligned} \mathcal{P}_2(t) = \epsilon_0 \chi^{(2)} & \left[ \mathcal{E}_1^2 e^{-2j\omega_1 t} + \mathcal{E}_2^2 e^{-2j\omega_2 t} + 2E_1 E_2 e^{-j(\omega_1 + \omega_2)t} \right. \\ & \left. + 2E_1 E_2^* e^{-j(\omega_1 - \omega_2)t} + c.c. \right] + 2\epsilon_0 \chi^{(2)} \left[ |E_1|^2 + |E_2|^2 \right] \end{aligned} \quad (2.69)$$

The first term of Equation (2.69) generates two EM fields at frequencies  $2\omega_1$  and  $2\omega_2$ , the third and fourth term generates waves at frequencies called sum-frequency generation (SFG) and difference frequency generation (DFG). For generating entanglement, we leverage DFG. Using an optical parametric amplifier (OPA), a laser with frequency  $\omega_a$  is used to pump a nonlinear crystal, and at the same time, a small EM wave with a frequency  $\omega_s$  is introduced

into the medium, given  $\omega_s \ll \omega_a$ . Using DFG,  $\omega_i = \omega_a - \omega_s$  is generated, which is called as idler. Idler stimulates the generation of fields with frequency  $\omega_s = \omega_a - \omega_i$ . The  $\omega_s$  is a signal wave that repeats the process. The generation of idler reinforces the generation of the signal and vice-versa. This process of generation of signal/idler pair is called stimulated emission. It is also possible to create signal/idler pair using spontaneous emission. In spontaneous emission, it is not possible to distinguish between idler and signal. When a nonlinear crystal with second-order susceptibility is pumped by a laser, then there is a small probability of order of  $10^{-12}$  that the pump photon splits into signal/idler pair. The process of spontaneous emission is shown in Figure 2.6. The interaction Hamiltonian with signal-idler pair can be



**Figure 2.6:** Spontaneous Parametric Down-Conversion: A pump with frequency  $\omega_a$  is passed through nonlinear crystal that converts photons into signal-idler pair conserving energy and momentum.

written as

$$\hat{H} = j\hbar[c_1\hat{a}_{s\alpha}\hat{a}_{i\gamma} + c_s\hat{a}_{s\beta}\hat{a}_{i\delta}] + H.C. \quad (2.70)$$

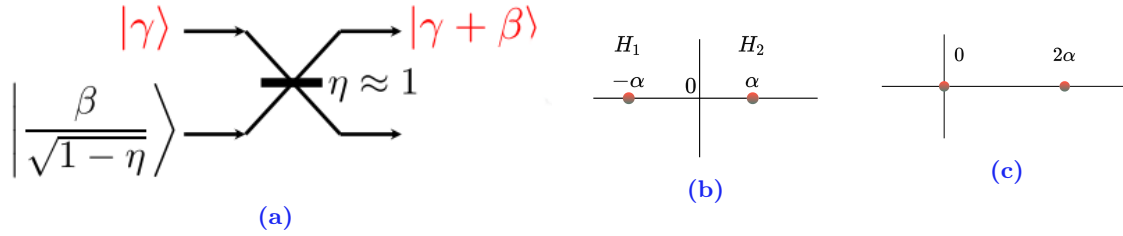
where  $H.C.$  are Hermitian conjugate terms.  $\hat{a}_s$  and  $\hat{a}_i$  are annihilation operators for signal and idler.  $c_1$  and  $c_2$  are constants related to the second order susceptibility. Consider pump as a classical field, the quantum state evolves as  $|\psi(t)\rangle = |\psi(0)\rangle e^{-j\hat{H}t/\hbar}$ . If we expand the quantum state and take initial state as vacuum, our state approximates to

$$|\psi\rangle \approx \eta_1 |\alpha\rangle |\gamma\rangle + \eta_2 |\beta\rangle |\delta\rangle. \quad (2.71)$$

The Equation (2.71) suggests that with probability  $\eta_1$ , one photon is in mode  $\alpha$  and other is in mode  $\gamma$  while with probability  $\eta_2$ , one photon is in mode  $\beta$  while other is in mode  $\delta$ .

## 2.10 A REVIEW OF EXISTING RECEIVER DESIGNS EMPLOYING COHERENT STATES

Photodetectors in combination with laser beams have made possible the optical communication system. The initial optical communication system mimicked radio-frequency techniques

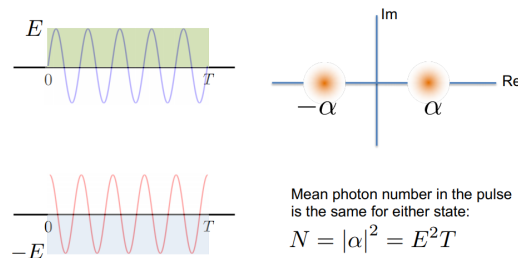


**Figure 2.7:** **Left:** A simple circuitry to perform displacement using beamsplitter. **Middle:** One-off pulse with  $|\alpha\rangle$  and  $|0\rangle$ . **Right:** Displaced coherent states.

and used incoherent and homodyne detection. However, for applications such as deep space communication, the use of quantum detection gives an advantage since the received field is weak where classical detection is not optimum. A standard communication model consists of a transmitter, a physical channel, and a receiver. As the topic of the thesis is optimal receiver design, in the next few paragraphs, we review some popular existing receiver design techniques that employ coherent states.

### 2.10.1 KENNEDY’S RECEIVER

Kennedy receiver (Kennedy, 1973) has the ability to distinguish between binary coherent states. We can use the Kennedy receiver to distinguish Binary Phase Shift Keying (BPSK) encoded states. Binary Phase Shift Keying (BPSK) is a two-phase modulation scheme, where the 0s and 1s in a binary message are represented by two different phase states in the carrier signal. For example, consider a square pulse with oscillating phase  $Ee^{j\phi}$  with  $\phi = \{0, \pi\}$  as shown in Figure 2.8. In order to discriminate BPSK using Kennedy receiver,



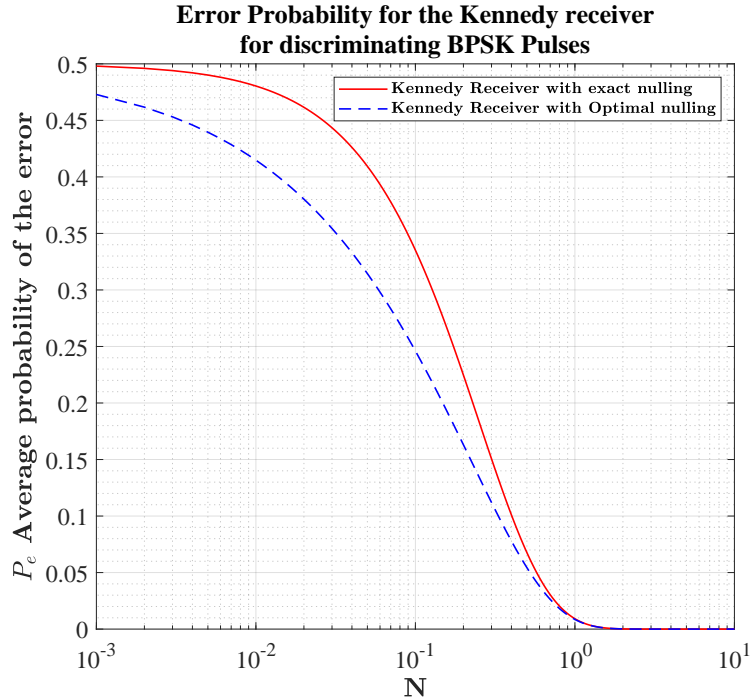
**Figure 2.8:** Binary Phase Shift Keying.

we require perfect amplitude phase reference in theory. One way to discriminate BPSK pulses is to apply exact displacement using a beamsplitter which translates  $\{ |-\alpha\rangle, |\alpha\rangle \}$  to  $\{ |0\rangle, |2\alpha\rangle \}$ . These displaced states will be allowed to go on detector. Assume that we count  $k$  clicks. We define following rules for hypotheses  $H_1$  i.e. we have off pulse and  $H_2$  that is we have on pulse, then:

$$\begin{cases} \text{IF } k = 0, & H_1 \text{ IS TRUE, I.E. OFF PULSE} \\ \text{IF } k > 0, & H_2 \text{ IS TRUE, I.E. ON PULSE} \end{cases} \quad (2.72)$$

In the above condition, we can easily calculate the error probability. For that, let's assume both BPSK symbols are equally likely. When  $\alpha$  pulse is given, then  $2\alpha$  goes to the detector. In this case, probability of choosing  $-\alpha$  pulse, given an  $\alpha$  pulse is equivalent of  $P(k = 0)$  in the Poisson distribution, i.e.,  $e^{-|2\alpha|^2}$ . When  $-\alpha$  (or 0 after displacement) goes to the detector, the probability of declaring an  $\alpha$  pulse is  $1 - e^{-|0|^2} = 0$ . Since  $|\alpha|^2 = N$ , the mean photon number is  $|2\alpha|^2$  or  $4N$ . Thus, error probability for discriminating BPSK pulses is

$$\begin{aligned} P(\text{error}) &= P(H_1)P(H_2|H_1) + P(H_2)P(H_1|H_2) \\ &= P(\text{on})P(\text{off}|\text{on}) + P(\text{off})P(\text{on}|\text{off}) \\ &= \frac{1}{2} \cdot e^{-4N} + \frac{1}{2} \cdot 0 = \frac{1}{2}e^{-4N} \end{aligned} \quad (2.73)$$



**Figure 2.9:** Error probability,  $P_e$  of state discrimination for the Kennedy receiver with BPSK.

Later, in (Takeoka and Sasaki, 2008), it was shown that an additional displacement of  $\beta$  can be made to further minimize the error probability of state discrimination. In such scheme,



the displacement  $\beta$  is chosen optimal depending the mean photon  $N$ . In such case the error probability is given by

$$P_e = \frac{1}{2}e^{-(2\alpha+\beta)^2} + \frac{1}{2}(1 - e^{-\beta^2}) \quad (2.74)$$

which can be minimized over  $\beta$  by solving the optimization problem  $\frac{dP_e}{d\beta} = 0$ . Error probability plot of Kennedy receiver with exact nulling and optimal nulling is given in in Figure 2.9.

### 2.10.2 UNAMBIGUOUS STATE DISCRIMINATION RECEIVER (USD)

In USD receiver, with probability  $e^{-N}$ , it produces an erasure (i.e., I don't know) outcome but with probability  $1 - e^{-N}$  probability, it guesses the hypothesis correctly. Whenever the receiver does make a guess (i.e. when one of the pulse slots generates a click), it knows – without any ambiguity – which was the received state. If forced to make a decision, i.e. by mapping the erasure to one possible input, the receiver makes mistake. The concept of USD receiver is shown in Figure 2.10.

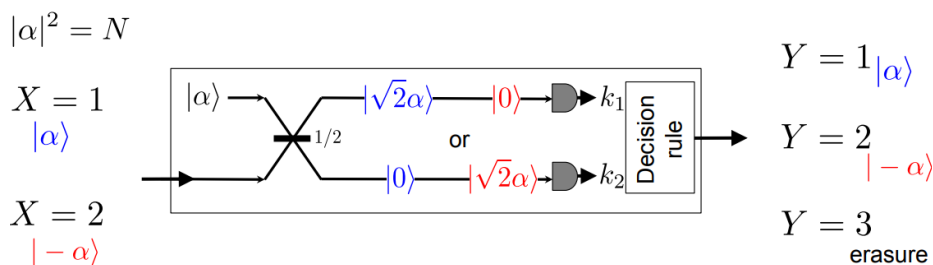


Figure 2.10: BPSK USD receiver design.

Thus probability of error in such case can be calculate as follows. Probability of  $Y = 1$ , if  $X = 1$  was sent is anything other than zero click. Hence,  $p_{1|1}(1|1) = 1 - e^{-2N}$ . Probability of  $Y = 2$ , if  $X = 2$  was sent is anything other than zero click. Hence,  $p_{2|2}(2|2) = 1 - e^{-2N}$ . As per USD design, we if  $X = 1$  is sent , detector will never say that  $|- \alpha\rangle$  was detected. Thus, Probability of  $Y = 1$ , if  $X = 2$  was sent is zero click. Hence,  $p_{2|1}(2|1) = 0$ . Similarly, Probability of  $Y = 2$ , if  $X = 1$  was sent is zero click. Hence,  $p_{1|2}(1|2) = 0$ . Thus the transition probability matrix ( $(2 \times 3)$  form) is:

$$TPM_{3 \times 2} = \begin{bmatrix} 1 - e^{-2N} & 0 & e^{-2N} \\ 0 & 1 - e^{-2N} & e^{-2N} \end{bmatrix} \quad (2.75)$$

However, USD also says with probability  $e^{-2N}$  for each input that it does not know. Now if we force the receiver to make a random guess with equal priori it will say with 0.5 probability

that  $|\alpha\rangle$  was transmitted. Let  $H_i$  is hypothesis that  $Y = i$  was outcome, where  $i = [1, 3]$ . Then

$$\begin{aligned} P(X = 1|H_1) &= 1 \\ P(X = 2|H_1) &= 0 \\ P(X = 1|H_2) &= 0 \\ P(X = 2|H_2) &= 1 \\ P(X = 1|H_3) &= \frac{1}{2} \\ P(X = 2|H_3) &= \frac{1}{2} \end{aligned} \tag{2.76}$$

Then we can write  $2 \times 2$  transition probability matrix as:

$$TPM_{2 \times 2} = \begin{bmatrix} (1 - e^{-N}) + \frac{e^{-2N}}{2} & \frac{e^{-2N}}{2} \\ \frac{e^{-2N}}{2} & 1 - e^{-2N} + \frac{e^{-2N}}{2} \end{bmatrix} \tag{2.77}$$

Thus error probability in this case is:

$$P_e = \frac{1}{2} \left( \frac{e^{-2N}}{2} \right) + \frac{1}{2} \left( \frac{e^{-2N}}{2} \right) = \frac{e^{-2N}}{2} \tag{2.78}$$

### 2.10.3 DOLINAR RECEIVER

Sam Dolinar in 1973 (Dolinar, 1973b) proposed an adaptive receiver based on a combination of photon-counting and feedback mechanisms. The Dolinar's receiver theoretically achieves Helstrom bound. However, Dolinar receiver is difficult to implement in practice.

Dolinar receiver uses multi-copy of a coherent state  $|\alpha\rangle$  such that we have

$$|\psi\rangle = |\alpha\rangle \otimes |\alpha\rangle \otimes |\alpha\rangle \cdots |\alpha\rangle \tag{2.79}$$

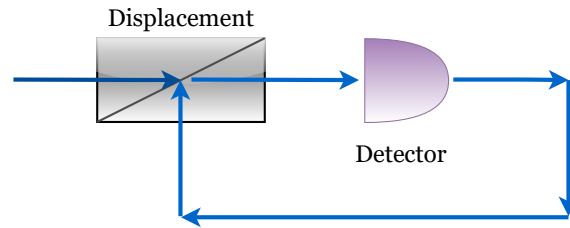
as a tensor product in Hilbert space  $\mathcal{H}^{\otimes n}$ . If we consider BPSK symbol with multi-copies as

$$\begin{aligned} |\psi_1\rangle &= |\alpha\rangle \otimes |\alpha\rangle \otimes |\alpha\rangle \cdots |\alpha\rangle \\ |\psi_2\rangle &= |-\alpha\rangle \otimes |-\alpha\rangle \otimes |-\alpha\rangle \cdots |-\alpha\rangle \end{aligned} \tag{2.80}$$

then the inner product is  $\langle \alpha | -\alpha \rangle = \chi$  and  $\langle \psi_1 | \psi_2 \rangle = \chi^2 = \sigma$ . With adaptive measurement strategy, the global optimal error probability is given by

$$P_{e,d} = \frac{1}{2} \left[ 1 - \sqrt{1 - 4p(1-p)\sigma^2} \right] \tag{2.81}$$

where  $p$  is prior probability of one of the BPSK symbols. The idea behind Dolinar receiver is illustrated in Figure 2.11.



**Figure 2.11:** A schematic of Dolinar's Receiver

Although Dolinar's receiver promises to achieve Helstrom Bound, delay due to introduction by the optical-electrical feedback control may greatly affect the efficiency of Dolinar's receiver and in practice, Helstrom Bound may not be achievable.

In the next few chapters, we discuss optimal receiver design for realizable receivers where information can be encoded using a number of quantum states in addition to coherent states such as squeezed displaced states and entangled states.



---

## RECEIVER DESIGN FOR PHASE-SHIFT KEYING COHERENT STATES

---

“ An important problem in quantum information theory is finding the best possible capacity of the optical communication channel employing suitable codewords, receiver design, and constellation optimization techniques. In this chapter, we derive an alternative channel capacity,  $C_G$ , of phase-shift keying coherent state with a realizable displacement receiver by maximizing mutual information over symbol priors and pre-detection displacement. We find that  $C_G$  is higher than the capacity achieved by maximizing mutual information over symbol prior but with zero displacement. The overall scheme demonstrates designing an improved, yet easy-to-implement receiver for better communication performance by tuning it at different photon number regime. Further, we present a comparative analysis of  $C_G$  with existing receiver designs. We extend our study to account for detector imperfections. ”

### 3.1 INTRODUCTION

One of the prime goals in Quantum Information Theory (QIT) is to innovate novel code-words, receiver design, and constellations to transmit information over a communication channel in the best possible way with a given set of resources. In the lieu of recent development in QIT, there are two types of communications possible: (i) transmitting a quantum state and expecting the receiver to detect the quantum state, and (ii) use quantum states to transmit classical information (in terms of 0s and 1s) (Hausladen et al., 1996). We call the latter semi-classical optical communication. If quantum states are orthogonal, then in theory we can distinguish quantum states with 100% certainty, and the amount of information transmitted will be maximum. However, in practice communication systems experiences detector imperfections, thermal noise, and turbulent channels, as a result of which orthogonality of states is compromised. Coherent states are non-orthogonal states that are known to possess loss-tolerant property. When transmitting through lossy bosonic channel merely suffer decay in amplitude but preserving coherence (Giovannetti et al., 2004). Of all challenges, we focus mainly on the design of the quantum receiver to maximize the amount of information transmitted. The metric of the information transmitted, called the mutual information was given by Shannon (Shannon, 1948). However, unlike classical communication,

the notion of maximizing mutual information to obtain Channel Capacity varies in the case of a quantum channel. In an early work (Shor, 2003), Peter W. Shor noted that depending upon the protocol, channel usages, detection algorithm, etc, capacity can be defined in several manners. Of all the definitions, the Holevo limit, denoted by  $C_\infty$  is when the receiver does the joint measurement over long codeword blocks. For symbol-by-symbol measurement with post-processing, the maximum attainable capacity was given by Sam Dolinar (Dolinar, 1976). Due to the complexity in designing a receiver to attain the maximum attainable capacity, several sub-optimal, but practical receivers were proposed for distinguishing coherent states (Kennedy, 1973; Vilmotter and Rodemich, 1984; Bondurant, 1993; Takeoka and Sasaki, 2008; Nair et al., 2014; Izumi et al., 2012; Yuan et al., 2020). The class of receivers based on displacement technique using beamsplitters and on-off photodetectors are much simpler to understand, simpler in design, and are of low-cost.

## CONTRIBUTION

In this chapter, we focus on designing a displacement receiver to design an optimum symbol constellation to maximize the mutual information. The past development so far doesn't deal with optimization problems concerning displacement and symbol priors simultaneously. Our optimization procedure demonstrates that the capacity, denoted by  $C_G$ , obtained from simultaneous optimization procedure over displacement and prior probabilities achieved is higher than one achieved with zero displacement. The overall scheme of designing a receiver by optimizing displacement prior to detection at on-off photodetector demonstrates that the receiver must be tuned differently at different photon number regimes to achieve the best performance. Previous work (Kennedy, 1973; Vilmotter and Rodemich, 1984; Bondurant, 1993; Takeoka and Sasaki, 2008; Nair et al., 2014; Izumi et al., 2012; Yuan et al., 2020) in this regard doesn't aim at tuning the receiver based on the photon-number regime under which the system operates. We demonstrate, by numerical simulation, that by tuning the receiver's parameters to optimize the objective function, the receiver performance comes out superior to the state-of-the-art method. The potential of such design is immense, specifically in deep-space communication that requires extreme optimization of resources.

The rest of the chapter is organized as follows: we first provide some fundamentals of a quantum channel for Free-Space Optical (FSO) communication as self-sufficiency for the readers in Section 3.2. Next, we discuss our methods of calculating capacity  $C_G$  concerning displacement and symbol prior in the absence and presence of thermal noise and detector imperfection. In the subsequent section, we present the result and provide a comparison concerning existing ways of calculating capacity. We end our discussion with some future goals.

### 3.2 PHASE-SHIFT KEYED COHERENT STATES, NOISE MODELS, AND DETECTOR IMPERFECTIONS

After the discovery of laser, in 1963, R.J. Glauber proposed the theory of optical coherence (Glauber, 1963b) which further lead to development of QIT by Helstrom (Helstrom et al., 1970), Dolinar (Dolinar, 1973b, 1982, 1976, 1973a), Kennedy (Yuen et al., 1975; Helstrom and Kennedy, 1974) and various other researchers. The initial objective of QIT was to provide a mathematical theory of *information* and develop methods to represent information in an efficient way for transmission and storage. Theories were also developed to preserve information in presence of noise and defects. After Voyager 2 (Smith et al., 1989), Jet Propulsion Laboratory (JPL) at NASA took immense interest in QIT and its application for deep-space communication using the free-space optical channel. In last few decades, a number of treatise have been written and theories have been developed for applications such as deep-space communication, (Vilnrotter and Lau, 2001) channel coding and data compression, (Liu et al., 2019a; Ninacs et al., 2019; Liu et al., 2019b) cryptography and encryption, (Alsina and Razavi, 2019; Djordjevic, 2019b,a; Qu and Djordjevic, 2018) and quantum internet (Sadeghi-Zadeh et al., 2019; Das et al., 2019; Loncar and Raymer, 2019; Asif, 2020; Pant et al., 2019) - all of them employing FSO communication channel.

In the case of semi-classical communication, the transmitted symbols are encoded by a series of quantum states  $\{|\alpha_i\rangle\}$ ,  $i \in [1, M]$  where we send pure quantum states through the FSO communication channel. At the end of the channel, a receiver performs detection by the means of hypothesis testing. FSO quantum communication offers reliable means to transmit both classical and quantum information. Laser lightwaves consisting of coherent states are the most convenient way of communication in FSO. A standard coherent state (henceforth called coherent state), denoted by ket notation  $|\alpha\rangle$  is written as

$$|\alpha\rangle = \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} e^{-\frac{|\alpha|^2}{2}} |n\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (3.1)$$

where  $|n\rangle$  is a number state or a Fock state. Fock states form an orthonormal basis for measurement that can be used in spectral decomposition. See (Gazeau, 2009), Section 2.3.1, and 2.4 for more details.

In M-ary phase-shift keyed coherent state communication, every state out of M states for the signaling interval  $[0, T]$  is denoted by  $|\psi_i\rangle = |\alpha e^{j2\pi(i-1)/M}\rangle$ ,  $i \in [1, M]$ . All coherent states  $|\alpha\rangle$ ,  $\alpha \in \mathbb{C}$  form an overcomplete basis in the Hilbert space. In QIT, the existence of a probability distribution on the states accessible to a system is defined by a statistical operator called the *density matrix*:

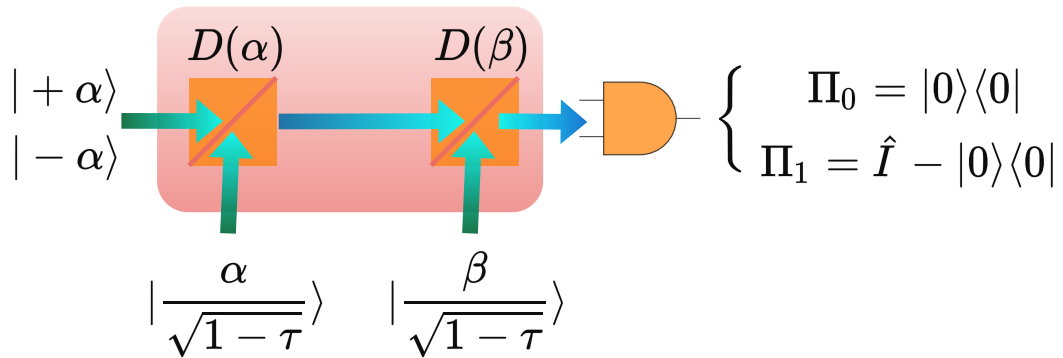
$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| = \sum_i p_i \rho_i \quad (3.2)$$

where  $\rho_i$  is the outer product,  $p_i$  is the probability for the system to be in state  $|\psi_i\rangle$  when  $|\psi\rangle$  is represented using orthonormal basis with  $\sum p_i = 1$ .

When using the quantum state as an information carrier, the communication is done using an ensemble of quantum states with alphabet  $\mathcal{A} = \{\rho_1, \rho_2, \dots, \rho_M\}$  through a sequence of quantum operations representing the channel. Optical coherent states are not orthogonal - one can attempt to minimize the overlap  $\langle\alpha|\beta\rangle$  between two coherent states  $|\alpha\rangle$  and  $|\beta\rangle$ . Several receivers have been proposed in an attempt to minimize the error probability of distinguishing quantum states or maximize the mutual information being transmitted over the channel. In the next section, we discuss the design of displacement receivers based on photon counting and an on-off photodetector.

### 3.3 DISPLACEMENT RECEIVERS WITH PHOTON-COUNTING AND ON-OFF PHOTODETECTOR FOR BPSK

In semi-classical quantum communication, BPSK is represented by a pair of coherent states differ only in phase by  $\pi$  radian, i.e.,  $\{|\alpha\rangle, |-\alpha\rangle\}$ . Detecting coherent states in such case using photon-counting and on-off detector requires some form of optical operation as with direct detection phase information can not be detected by an on-off detector. One such operation is amplitude displacement. A displacement operation is performed using optical circuit so as to shift the amplitude of a coherent state. A beamsplitter is used to perform displacement operation as described in Section 2.6. For a displacement receiver to act on BPSK, we first null out one of the two coherent state to a vacuum state followed by another displacement operation such that  $\{|-\alpha\rangle, |\alpha\rangle\} \rightarrow \{|0\rangle, |2\alpha\rangle\} \rightarrow \{|\beta\rangle, |2\alpha + \beta\rangle\}$ . The overall operation of a displacement receiver with BPSK is shown in Figure 3.1.



**Figure 3.1:** A schematic diagram of the displacement receiver with BPSK symbols. An optimized displacement receiver uses a two-step displacement operation where one of the two coherent states of BPSK is nulled out to a vacuum state and then displaced by  $\beta$  amount.

The operation of the displacement receiver is most straightforward with the BPSK symbols.



Let  $X$  represent the input coherent state (one of two possible)  $\{|-\alpha\rangle, |\alpha\rangle\}$  to the channel. When the input to the channel is binary,  $X$  can be used to represent the transmission of the pulse with either phase of 0 degrees or 180 degrees by using the corresponding coherent state. During each symbol epoch when  $X$  is transmitted, an integer number of photons is detected by the photodetector. Detection of photons results in real-valued output denoted by  $Y$  at the detector that can be passed to a decoder or a simple threshold to identify the transmitted symbol  $X$ . Recall that the statistics of photon arrival is given by the Poisson point process:

$$P(K = k) = \frac{N^k}{k!} e^{-N} \quad k = 0, 1, 2, \dots \quad (3.3)$$

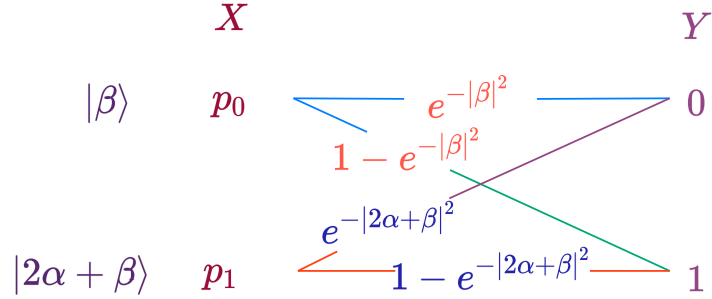
i.e. the probability of detecting  $k$  photon over a given time interval is given by Equation (3.3) when we know the mean photon number is  $N$ . The detector will see clicks when the transmitter transmits the pulse following the Poisson point process. If we have a pulse with a mean photon number  $N$ , then the probability of not getting any clicks as per the Poisson point process is given by

$$P(\text{no clicks}) = e^{-N} \quad (3.4)$$

In case of displacement receivers, a beamsplitter and a local oscillator is used to shift BPSK symbols to  $\{|\beta\rangle, |\beta + 2\alpha\rangle\}$  via two step process as shown in Figure 3.1, where  $\beta$  is the displacement amount. The receiver tries to assess which symbol or state was transmitted by performing quantum measurement,  $\Pi$  on the channel (see Section 4.3.2 of (Gazeau, 2009) for further reading). The operator  $\Pi$  is described by an appropriate Positive-Operator Valued Measurement (POVM) represented by a complete (here countable) set of positive operators resolving the identity  $\sum_i \Pi_i = \hat{I}$ ,  $\Pi_i \geq 0$  with  $i$  representing index of possible measurement or hypothesis. For BPSK, POVM resolution unity corresponds to  $\Pi_0 + \Pi_1 = \hat{I}$ . If hypothesis  $H_0$  is true, i.e  $\rho_0$  corresponding to  $|-\alpha\rangle$ , the measurement outcome corresponds to  $\Pi_0$ , otherwise  $\Pi_1$ . For displacement receiver with on-off detector, the receiver decides in the favor of  $H_0$  when number of click on detector is 0, otherwise  $H_1$ . In practice, this operation is equivalent to measurement operation given by  $\Pi_0$  and  $\Pi_1$ . In order to write mutual information, we first need to write probability distribution of the output  $Y$ . We can use Bayes' rule to write the probability distribution of  $Y$  as follows:

$$p_Y(y) = p_0 p_{Y|X}(y|x=0) + p_1 p_{Y|X}(y|x=1) \quad (3.5)$$

where  $p_0, p_1$  are the probabilities of BPSK symbols.  $p_{Y|X}(y=0|x=0)$  is the probability of no clicks when  $|\beta\rangle$  after displacement was sent. Since the photon counting follows Poisson distribution, probability of generating no clicks, when  $|\beta\rangle$  was transmitted, is equal to  $e^{-|\beta|^2}$  (we simply put  $N = |\beta|^2$  in Equation (3.4)). Similarly,  $p_{Y|X}(y=0|x=1)$  is the probability of no clicks when  $|\alpha\rangle$ , or  $|2\alpha + \beta\rangle$  after the displacement, was transmitted, which is equal to  $e^{-|2\alpha + \beta|^2}$ . Similarly,  $p_{Y|X}(y=1|x=0)$  is the conditional probability of non-zero click, i.e., detection  $|\alpha\rangle$  when  $|-\alpha\rangle$  was transmitted which is  $1 - e^{-|\beta|^2}$ .  $p_{Y|X}(y=1|x=1)$  is



**Figure 3.2:** Transition probability matrix for BPSK. Transition probability matrix is used to describe a channel visually where a connection between each possible input and output is connected and annotated by the transition probability, mapping a particular input to an output. For example, probability of receiving output  $Y = 0$  when  $X = 0$  was transmitted is given by  $e^{-|\beta|^2}$ .

the probability of non-zero clicks that detecting  $|\alpha\rangle$  when  $|\alpha\rangle$  was transmitted which is  $1 - e^{-|2\alpha+\beta|^2}$ . This idea is illustrated in Figure 3.2. Hence, we can write probability of outcome  $Y$  as follows:

$$p_Y(0) = p_0 e^{-|\beta|^2} + p_1 e^{-|2\alpha+\beta|^2} \quad (3.6)$$

$$p_Y(1) = p_0(1 - e^{-|\beta|^2}) + p_1(1 - e^{-|2\alpha+\beta|^2}) \quad (3.7)$$

Based on Equations (3.6) and (3.7), conditional entropy can be written as

$$\begin{aligned} H(Y|X=0) &= -p_{Y|X}(Y=0|X=0) \log_2 p_{Y|X}(Y=0|X=0) \\ &\quad - p_{Y|X}(Y=1|X=0) \log_2 p_{Y|X}(Y=1|X=0) \\ &= -e^{-\beta^2} \log_2 e^{-\beta^2} - (1 - e^{-\beta^2}) \log_2(1 - e^{-\beta^2}) \end{aligned} \quad (3.8)$$

$$\begin{aligned} H(Y|X=1) &= -p_{Y|X}(Y=0|X=1) \log_2 p_{Y|X}(Y=0|X=1) \\ &\quad - p_{Y|X}(Y=1|X=1) \log_2 p_{Y|X}(Y=1|X=1) \\ &= -e^{-(2\alpha+\beta)^2} \log_2(e^{-(2\alpha+\beta)^2}) - (1 - e^{-(2\alpha+\beta)^2}) \log_2(1 - e^{-(2\alpha+\beta)^2}) \end{aligned} \quad (3.9)$$

Then conditional entropy can be used to write the mutual information  $I_{\text{BPSK}}(X; Y)$ .

$$\begin{aligned}
I_{\text{BPSK}}(X; Y) &= H(Y) - H(Y|X) \\
&= H(Y) - \sum_i p(X = i) H(Y|X = i) \\
&= \left[ -p_Y(0) \log_2(p_Y(0)) - p_Y(1) \log_2(p_Y(1)) \right] - \\
&\quad \left[ p \cdot H(Y|X = 0) + (1 - p) \cdot H(Y|X = 1) \right] \\
&= \left( \frac{\ln(1 - e^{-(2\alpha+\beta)^2}) (e^{-(2\alpha+\beta)^2} - 1)}{\ln(2)} - \frac{\ln(e^{-(2\alpha+\beta)^2}) e^{-(2\alpha+\beta)^2}}{\ln(2)} \right) (p - 1) \\
&\quad + p \left( \frac{e^{-\beta^2} \ln(e^{-\beta^2})}{\ln(2)} - \frac{\ln(1 - e^{-\beta^2}) (e^{-\beta^2} - 1)}{\ln(2)} \right) \\
&\quad - \frac{\ln\left(\left(e^{-(2\alpha+\beta)^2} - 1\right) (p - 1) - p \left(e^{-\beta^2} - 1\right)\right) \left(\left(e^{-(2\alpha+\beta)^2} - 1\right) (p - 1) - p \left(e^{-\beta^2} - 1\right)\right)}{\ln(2)} \\
&\quad - \frac{\ln\left(p e^{-\beta^2} - e^{-(2\alpha+\beta)^2} (p - 1)\right) \left(p e^{-\beta^2} - e^{-(2\alpha+\beta)^2} (p - 1)\right)}{\ln(2)}
\end{aligned} \tag{3.10}$$

In our generalized displacement receiver design, we aim to derive generalized capacity  $C_G$  by maximizing mutual information over symbol prior as well as displacement amount  $\beta$ . Hence, our new problem statement becomes simultaneous maximization of mutual information over the displacement vector and prior probabilities which we denote by  $C_G$ :

$$C_G = \max_{p_X(x), \beta} I_{\text{BPSK}}(X; Y) \tag{3.11}$$

To solve the Equation (3.11) using (3.10), we take partial derivative of (3.10) with respect to  $p$  and  $\beta$  and use newton's method to numerically find the optimum solution. We calculate the Hessian matrix to validate the maximizer.

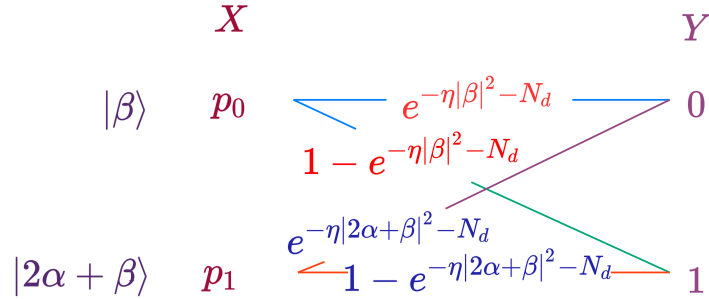
### 3.3.1 DETECTOR IMPERFECTIONS

Our previous discussion has ignored the situation of imperfect detection. We now discuss some detector imperfections and how they are modeled. For coherent states, subunity ( $< 1$ ) **detection efficiency** translates to an ideal detector masked by a beamsplitter with transmission efficiency  $\eta < 1$  (Gazeau, 2009). It can be shown that detection efficiency can be incorporated into coherent state notation by replacing  $\alpha$  by  $\sqrt{\eta}\alpha$ . Another notable imperfections is **dead time**. In an avalanche photodiode, a detection phenomenon must be followed

by a quenching process to settle down electron avalanche before any further detection can be done. The time during which quenching happens is called as dead time (Müller and Marquardt, 2015). During the dead-time detector is blind to the incoming photon. However, for a Kennedy-like receiver that makes a decision based on first photon detection, dead-time is irrelevant. Another notable imperfection is **dark count** (or dark click). The dark count rate is the average rate of counts registered without any incident photon. The dark count statistics are Poissonian in nature, assuming dark count rate to be  $N_d$  that adds to a photon count rate of the displaced signal, overall mean photon number becomes  $N_T = N + N_d$ . The effect of the dark count is similar to having a random displacement of the quantum state. Dark count leads to the deformation of the signal constellation on the circle and leads to increased mutual overlap of the signal. To determine the probability of correct detection, it should be noted that when we include the process of the dark count, then we are dealing with two independent Poisson processes. The resulting mean of a Poisson process consisting of two independent Poisson process is the sum of the individual means. In such a case, the on-off detector is described by the measurement operator (Izumi et al., 2012)

$$\begin{aligned}\hat{\Pi}_{\text{off}} &= e^{-N_d} \sum_{n=0}^{\infty} (1-\eta)^n |n\rangle \langle n| \\ \hat{\Pi}_{\text{on}} &= \hat{I} - \hat{\Pi}_{\text{off}}\end{aligned}\tag{3.12}$$

The transition probability matrix with dark count and detection efficiency included is depicted in Figure 3.3. Accordingly, we can modify Equations (3.6) and (3.7) to include the

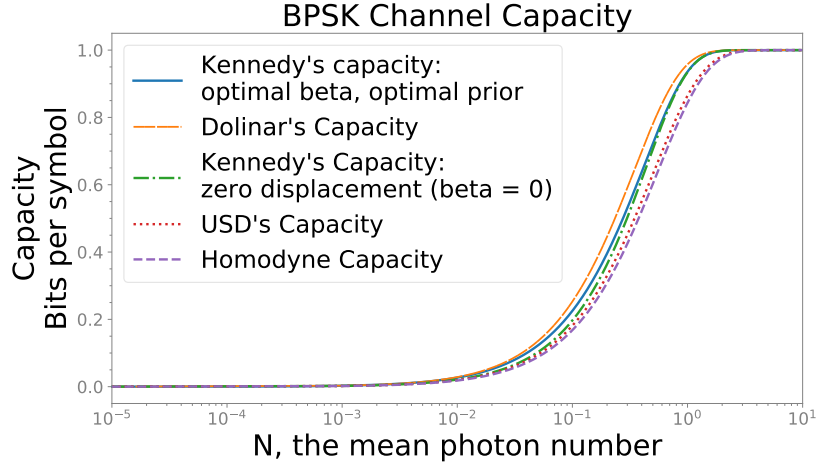


**Figure 3.3:** Transition probability matrix for BPSK with sub-efficient detector and notable dark count. Transition probability connecting possible inputs and outputs are updated to include detected efficiency and dark count.

two parameters:  $\eta$  and  $N_d$ .

Figure 3.4 shows the channel capacity for BPSK in the units of bits transmitted per symbol for the ideal case and its comparison with a few known receiver design techniques. Orange curve is for capacity in bits transmitted per symbol for Dolinar receiver which is given by

$$C_d = 1 + p \log_2(p) + (1 - p) \log_2(1 - p)\tag{3.13}$$



**Figure 3.4:** BPSK channel capacity for the ideal case. We present a comparison of prior-maximized-displacement maximized mutual information with Capacity from other receiver design in units of bits transmitted per BPSK symbol (bits per mode).

where  $p = \frac{1}{2} \left( 1 - \sqrt{1 - e^{-4N}} \right)$  is the prior error probability for the case of Dolinar receiver that maximizes the mutual information with  $N$  being the mean photon number (Carriolaro, 2015). Theoretically, Dolinar receiver is the best performing receiver known to the date. However, its practical realization is difficult and also requires multiple copies of quantum states. Green dotted-dashed curve represents capacity in bits per symbol for classical Kennedy receiver where no attempt is made to optimize the displacement while maximizing the mutual information. Capacity for classical Kennedy receiver with no optimum displacement is given by

$$C_k = \log_2 \left( 1 + (1 - p)p^{p/(1-p)} \right) \quad (3.14)$$

where  $p = e^{-4N}$  is the prior probability for the case of classical Kennedy receiver. Dotted red curve in Figure 3.4 is capacity for Unambiguous state discrimination (USD) receiver for BPSK. Capacity for USD receiver is given by

$$C_u = 1 - e^{-2N} \quad (3.15)$$

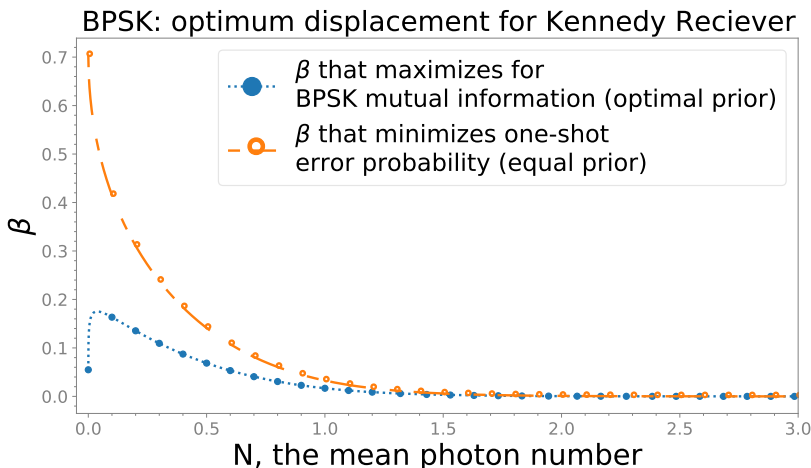
Purple dashed curve in Figure 3.4 represents capacity in bits per symbol for Homodyne receiver. The capacity for Homodyne receiver is given by

$$C_h = 1 + p \log_2(p) + (1 - p) \log_2(1 - p) \quad (3.16)$$

with  $p = \frac{1}{2} \text{erfc}(\sqrt{2N})$ , erfc is the Gauss error function. Finally, the blue solid line curve is the capacity obtained using prior-maximized-displacement-maximized mutual information

that is the focus of our work. Interested readers may refer to Chapter 9 of (Cariolaro, 2015), (Chefles and Barnett, 1998; Shor, 2003; Takeoka and Guha, 2014) for a detailed discussion on derivation of capacities for Dolinar receiver, Kennedy receiver, USD receiver, and Homodyne receiver we discussed. We note that the prior maximized-displacement maximized mutual information performs only subpar to the Dolinar receiver but beats other receiver designs and does not require multiple copies of the quantum state to be transmitted.

From Figure 3.5, we see the optimum displacement is quite different in two cases where (i) we minimize one-shot error probability, (ii) we maximize mutual information. Based on this theoretical result, we emphasize that the receiver design is influenced by the information-processing task at hand. Optimizing a receiver to minimize symbol error probability may not result in a capacity-maximizing setting for that same receiver and vice-versa.



**Figure 3.5:** This graph compares the  $\beta$ , optimum displacement for the Kennedy receiver, for (a) optimizing capacity (blue dotted), and (b) minimizing error probability assuming equal priors (orange dashed)

### 3.4 DISPLACEMENT RECIVER DESIGN FOR QPSK

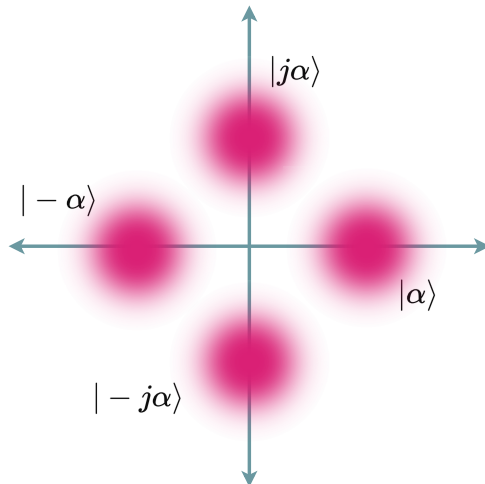
The quadriphase-shift keying (QPSK) is composed of four coherent states with states defined by

$$|\alpha_k\rangle = \left| \alpha e^{2\pi jk/4} \right\rangle \quad k \in [0, 3] \quad (3.17)$$

with *a priori*  $\{p_0, p_1, p_2, p_3\}$ . Unlike previous works, we do not assume equal probability. There are several receiver designs for QPSK that have been proposed in the literature, how-

ever, there is not enough discussion available on capacity or mutual information calculation. In the next few paragraphs, we reproduce one of those designs - proposed by Izumi and Sasaki (Izumi et al., 2012) and extend the existing work to obtain optimized capacity.

### 3.4.1 IZUMI-SASAKI DESIGN WITHOUT FEEDFORWARD



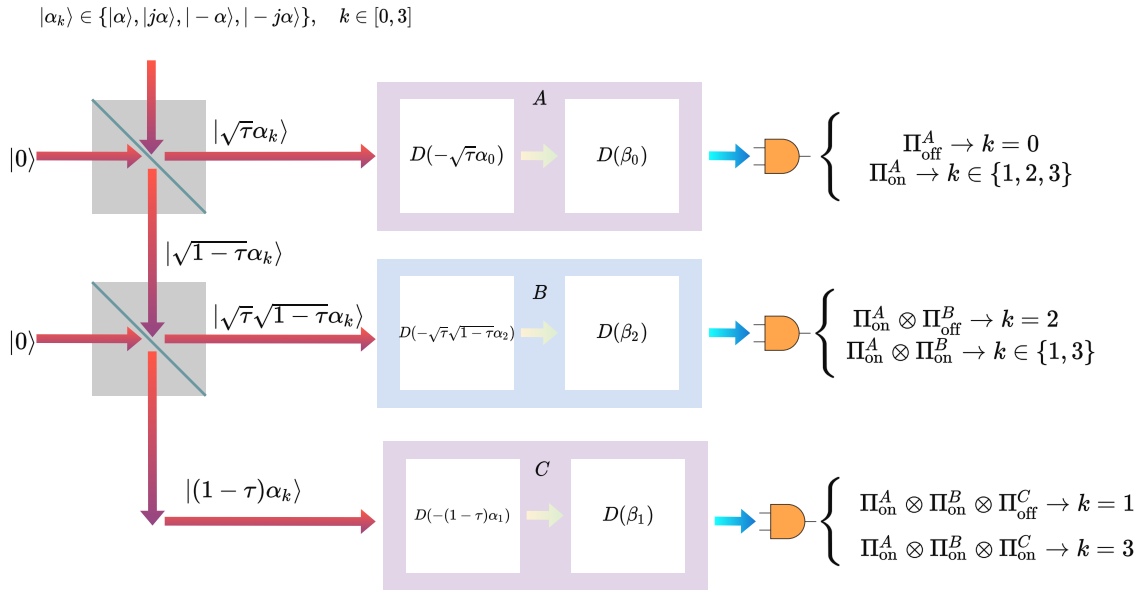
**Figure 3.6:** QPSK signal constellation at the input. In phase-shift keying (PSK), the constellation points are positioned with equal angular spacing around a circle. QPSK, a PSK with four points, is denoted by four points on a circle, equispaced. Each point differs from its preceding point by a phase of  $\pi/4$ .

In this section, we start with initial design of QPSK constellation proposed by Izumi-Sasaki (Izumi et al., 2012). Based on coherent state considered in Equation (3.17), the quantum states without displacement or any transformation are  $\{|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle\} \equiv \{|\alpha\rangle, |j\alpha\rangle, |-\alpha\rangle, |-j\alpha\rangle\}$  (see Figure 3.6).

A sequential operation of a three-port scheme is achieved by using two beamsplitters with transmittivities  $\tau_1$  and  $\tau_2$  that create three additional branches at which displacement operation  $D(\beta_i)$ ,  $i \in [1, 3]$  is applied where  $\beta_i$  are optimized displacement value. The original Izumi-Sasaki design uses exact nulling, however, we employ optimized displacement operation and assume that the transmittivity of all beamsplitter employed in the circuitry is  $\tau = \tau_1 = \tau_2$ . The overall design is shown in Figure 3.7.

After branching from the first beamsplitter, a nulling displacing of  $-\sqrt{\tau}\alpha_0$  follows an optimized displacement  $\beta_0$ . An on-off photodetector performs detection and if it doesn't register a click, it means the symbol  $\alpha_0 = \alpha$  was transmitted. At this point, the probability of correct classification is

$$p_{Y|X}(y = 0|x = 0) = e^{-\eta|\beta_0|^2 - N_d} \quad (3.18)$$



**Figure 3.7:** QPSK semi-classical demodulator. In this type of receiver design, two beamsplitters are employed where decisions are made sequentially. The first output of the first beamsplitter is displaced twice and photo-detection is performed. If the decision is ambiguous, then observation is moved to the other stages. At the second stage, the second output of the first beamsplitter is fed through the first input port of the second beamsplitter, mixed with a vacuum state. The first output of the second beamsplitter is displaced twice before performing binary decision using a photodetector. The procedure is repeated at the third stage if the decision remains ambiguous. The second output of the second beamsplitter is displaced twice and finally, the photodetector provides an unambiguous decision.



If the detector registers a non-zero click, then we look at part B of the circuit. If the second detector doesn't register a click, then the probability of detecting  $\alpha_2 = -\alpha$  is

$$p_{Y|X}(y = 2|x = 2) = \left(1 - e^{-N_d - \eta| -2\sqrt{\tau}\alpha + \beta_0|^2}\right) e^{-\eta|\beta_2|^2 - N_d} \quad (3.19)$$

If the second detector registers a non-zero click, then we move to branch C. In branch C, if the third detector doesn't register a click then the probability of detecting  $j\alpha$ , when it was actually sent, is

$$\begin{aligned} p_{Y|X}(y = 1|x = 1) &= \left(1 - e^{-N_d - \eta|j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2}\right) \\ &\times \left(1 - e^{-N_d - \eta|j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2}\right) \times e^{-\eta|\beta_1|^2 - N_d} \end{aligned} \quad (3.20)$$

and finally if detector 3 registers a click, then we declare that the state  $\alpha_3$  was transmitted such that

$$\begin{aligned} p_{Y|X}(y = 3|x = 3) &= \left(1 - e^{-N_d - \eta| -j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2}\right) \\ &\times \left(1 - e^{-N_d - \eta| -j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2}\right) \times \left(1 - e^{-N_d - \eta| -2j(1-\tau)\alpha + \beta_1|^2}\right) \end{aligned} \quad (3.21)$$

Similar to the Section 3.3, we can use Bayes' rule to write the probability distribution of  $Y$  for the QPSK receiver as follows:

$$\begin{aligned} p_Y(y) &= p_0 p_{Y|X}(y|x = 0) + p_1 p_{Y|X}(y|x = 1) \\ &+ p_2 p_{Y|X}(y|x = 2) + p_3 p_{Y|X}(y|x = 3) \end{aligned} \quad (3.22)$$

with  $\sum_0^3 p_i = 1$ . The expression for conditional entropies and mutual information is similar to ones in Equations (3.8), (3.9), and (3.10). The generalized capacity  $C_G$  is obtained by solving the optimization problem:

$$C_G = \max_{p_X(x), \beta_0, \beta_1, \beta_2} I_{\text{QPSK}}(X; Y) \quad (3.23)$$

with  $p_X(x)$  the prior probabilities for random variable  $X$ , i.e.  $\{p_0, p_1, p_2, p_3\}$  subject to  $\sum_0^3 p_i = 1$ . In the design of QPSK receiver, we consider  $N_d$ ,  $\eta$ , and  $\tau$  to be design parameters and hence, constant. In this case,  $I_{\text{QPSK}}$  is function of  $\alpha$  with optimization parameters  $p_0, p_1, p_2, p_3, \beta_0, \beta_1$ , and  $\beta_2$ . Hence the optimization problem looks like as follows:

$$C_G = \max_{p_0, p_1, p_2, p_3, \beta_0, \beta_1, \beta_2} f(\alpha, N_d, \eta, \tau; p_0, p_1, p_2, p_3, \beta_0, \beta_1, \beta_2) \quad (3.24)$$

subject to constraint  $\sum_0^3 p_i = 1$ , and  $0 \leq p_i \leq 1$ .

The conditional probabilities are used to construct transition probability matrix (also known as channel matrix in some literature) and can be used for calculating entropy and conditional

entropy by using Equations similar to one presented in Equations (3.8), (3.9), and (3.10). We omit the exact expression of entropies for the case of QPSK but they can be calculated as we calculated for BPSK. We will be able to calculate them using definitions of entropy and conditional probability expressions presented below. In the following expressions,  $X$  denotes a random variable corresponding to an input state and  $Y$  denotes a random variable corresponding to the detected state.

$$p_{Y|X}(y = 0|x = 0) = e^{-\eta|\beta_0|^2 - N_d} \quad (3.25)$$

$$p_{Y|X}(y = 1|x = 0) = \left(1 - e^{-N_d - \eta|\beta_0|^2}\right) \times \left(1 - e^{-N_d - \eta|2\sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2}\right) \times e^{-N_d - \eta|(1-\tau)\alpha - j(1-\tau)\alpha + \beta_1|^2} \quad (3.26)$$

$$p_{Y|X}(y = 2|x = 0) = \left(1 - e^{-N_d - \eta|\beta_0|^2}\right) e^{-N_d - \eta|2\sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2} \quad (3.27)$$

$$p_{Y|X}(y = 3|x = 0) = \left(1 - e^{-N_d - \eta|\beta_0|^2}\right) \times \left(1 - e^{-N_d - \eta|2\sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2}\right) \left(1 - e^{-N_d - \eta|(1-\tau)\alpha - j(1-\tau)\alpha + \beta_1|^2}\right) \quad (3.28)$$

$$p_{Y|X}(y = 0|x = 1) = e^{-N_d - \eta|j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2} \quad (3.29)$$

$$p_{Y|X}(y = 1|x = 1) = \left(1 - e^{-N_d - \eta|j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2}\right) \times \left(1 - e^{-N_d - \eta|j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2}\right) e^{-\eta|\beta_1|^2 - N_d} \quad (3.30)$$

$$p_{Y|X}(y = 2|x = 1) = \left(1 - e^{-N_d - \eta|j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2}\right) e^{-N_d - \eta|j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2} \quad (3.31)$$

$$p_{Y|X}(y = 3|x = 1) = \left(1 - e^{-N_d - \eta|j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2}\right) \times \left(1 - e^{-N_d - \eta|j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2}\right) \times \left(1 - e^{-\eta|\beta_1|^2 - N_d}\right) \quad (3.32)$$

$$p_{Y|X}(y = 0|x = 2) = e^{-N_d - \eta|-2\sqrt{\tau}\alpha + \beta_0|^2} \quad (3.33)$$

$$p_{Y|X}(y = 1|x = 2) = \left(1 - e^{-N_d - \eta| -2\sqrt{\tau}\alpha + \beta_0|^2}\right) \times \left(1 - e^{-\eta|\beta_2|^2 - N_d}\right) e^{-N_d - \eta| -(1-\tau)\alpha - j(1-\tau)\alpha + \beta_1|^2} \quad (3.34)$$

$$p_{Y|X}(y = 2|x = 2) = \left(1 - e^{-N_d - \eta| -2\sqrt{\tau}\alpha + \beta_0|^2}\right) e^{-\eta|\beta_2|^2 - N_d} \quad (3.35)$$

$$p_{Y|X}(y = 3|x = 2) = \left(1 - e^{-N_d - \eta| -2\sqrt{\tau}\alpha + \beta_0|^2}\right) \times \left(1 - e^{-\eta|\beta_2|^2 - N_d}\right) \left(1 - e^{-N_d - \eta| -(1-\tau)\alpha - j(1-\tau)\alpha + \beta_1|^2}\right) \quad (3.36)$$

$$p_{Y|X}(y = 0|x = 3) = e^{-N_d - \eta| -j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2} \quad (3.37)$$

$$p_{Y|X}(y = 1|x = 3) = \left(1 - e^{-N_d - \eta| -j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2}\right) \times \left(1 - e^{-N_d - \eta| -j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2}\right) \times e^{-N_d - \eta| -2j(1-\tau)\alpha + \beta_1|^2} \quad (3.38)$$

$$p_{Y|X}(y = 2|x = 3) = \left(1 - e^{-N_d - \eta| -j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2}\right) e^{-N_d - \eta| -j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2} \quad (3.39)$$

$$p_{Y|X}(y = 3|x = 3) = \left(1 - e^{-N_d - \eta| -j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0|^2}\right) \times \left(1 - e^{-N_d - \eta| -j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2|^2}\right) \left(1 - e^{-N_d - \eta| -2j(1-\tau)\alpha + \beta_1|^2}\right) \quad (3.40)$$

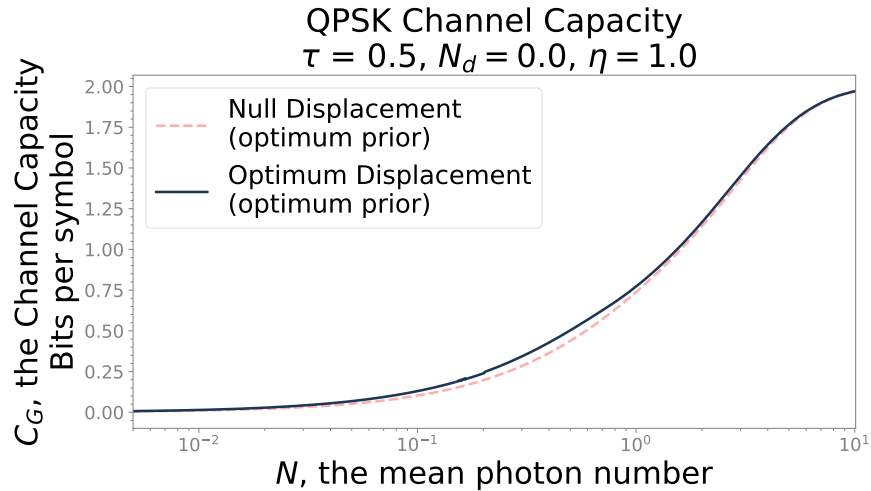
Figure 3.8 shows the channel capacity for QPSK using Izumi Sasaki design in the units of bits transmitted per symbol for zero displacements (i.e. when we maximize mutual information only over prior and set displacement  $\beta_i$  to zero) and its comparison with optimum displacement using optimization method.

To solve the optimization problem (3.24), we use MATLAB's `fmincon` function. `fmincon`, however, aims to minimize a function, hence in our case, we minimize  $-I_{\text{QPSK}}$  subject constraint mentioned in Section 3.4.1. In vector form we can write optimization parameter  $\mathbf{x} \equiv (p_0, p_1, p_2, p_3, \beta_0, \beta_1, \beta_2)$ . Equality constraint for this optimization problem is

$$\begin{aligned}
& A_{\text{eq}} \mathbf{x} = b \\
\Rightarrow & \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \\ \beta_0 \\ \beta_1 \\ \beta_2 \end{bmatrix} = 1
\end{aligned} \tag{3.41}$$

and the lower bound constraint is  $lb = [0 \ 0 \ 0 \ 0 \ -\text{Inf} \ -\text{Inf}]$ . The upper bound constraint is  $ub = [1 \ 1 \ 1 \ 1 \ \text{Inf} \ \text{Inf}]$ .

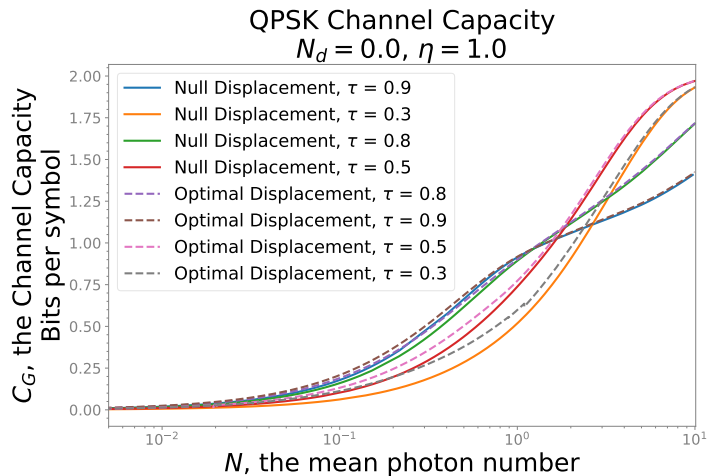
We start with initial condition  $\mathbf{x}_0 = [0.25, 0.25, 0.25, 0.25, 0, 0, 0]$ . In addition to that, we also execute few simulation with random initial points and we find out that  $C_G$ , the capacity comes out to be same with varying optimal values of priors and displacements (there may be multiple local minima). We choose  $\tau = 0.5$ ,  $N_d = 0.0$  and  $\eta = 1.0$  for the purpose of optimization.



**Figure 3.8:** QPSK channel capacity using Izumi-Sasaki design. We present a comparison for a case when displacement is zero and when displacement is optimum that maximizes the mutual information. We observe that the receiver achieves higher capacity for low photon numbers regime but converges for 1 to 10 photons regime.

We further performed some simulation studies on the impact of varying transmittivity  $\tau$  on the channel capacity. See Figure 3.9. For all the values of the transmittivity  $\tau$ , optimal displacement provides higher capacity. In the low photon regime, capacity is higher as the

transmittivity is increased but at the higher photon regime, it seems  $\tau = 0.5$  provides the best channel capacity.

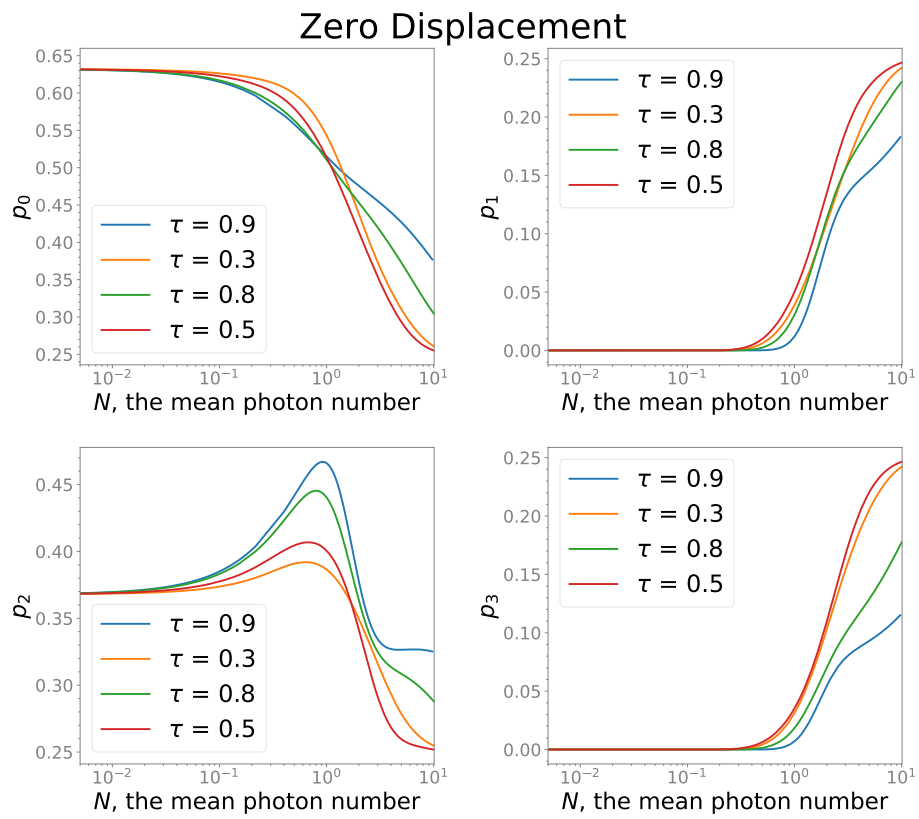


**Figure 3.9:** QPSK channel capacity using Izumi-Sasaki design. A comparison of the channel capacity with varying transmittivity for null and optimal displacement. For a particular  $\tau$ , optimal displacement provides higher channel capacity. Further, in low photon numbers regime, increasing  $\tau$  increases the channel capacity, but that cannot be said in the higher photon number regime, when we should use different parameters.

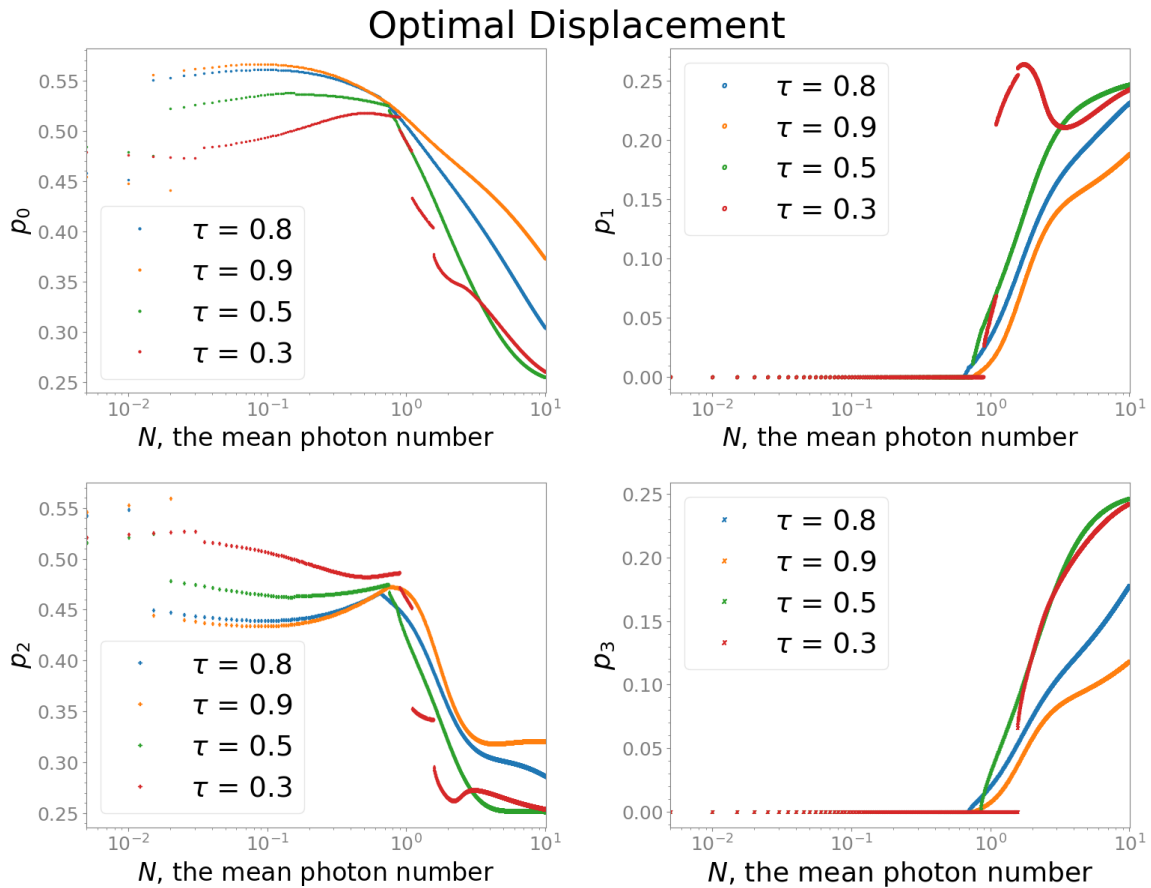
The optimal priors for maximizing mutual information in case of both, zero displacement and optimum displacement are provided in Figure 3.10 and Figure 3.11. From Figure 3.11, it is evident that priors we found with our optimization method may be local optima and not the global one. In fact, `fmincon` function doesn't promise to provide global optima. This is one reason behind discontinuity in the curves presented in Figure 3.11 since `fmincon` merely focuses on optimization and doesn't care about Lipschitz continuity (Hager, 1979). Finding global optima for a non-convex function is NP-hard, but we only strive to demonstrate that the receiver design is influenced by the objective and there is still room for improvement by making optimal choices such as transmittivity of beamsplitters, displacement amount and taking into account imperfections in optical elements.

Finally, we study the impact of dark current on the channel capacity. From our study, we observe that the higher the dark current, the lower the capacity gets. However, for optimal displacement-optimal prior, capacity remains higher than one with zero displacement even in the presence of the dark current. We provide a comparative illustration of capacity with a dark current of 0.2, 0.4, 0.6, and 0.8. The relevant graph is shown in Figure 3.12.

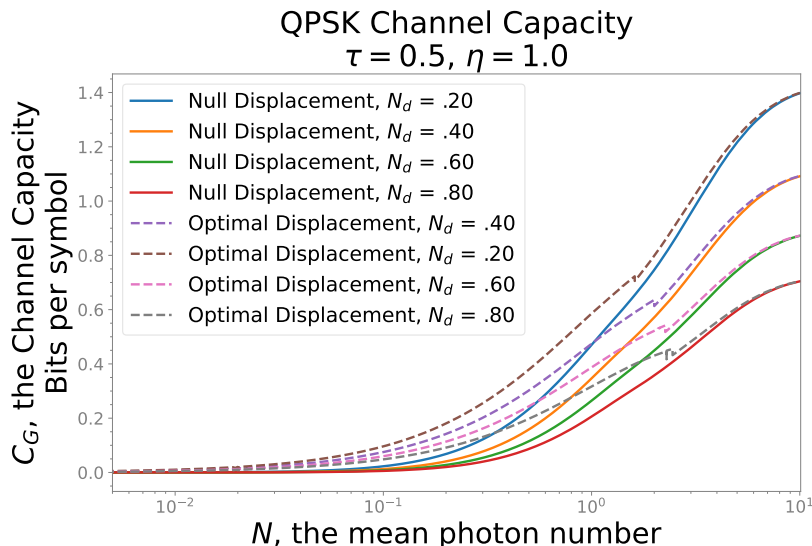
From the analysis presented in figures 3.8-3.12, it is evident that no single choice of design parameters for a displacement receiver can work optimally in every condition. The receiver needs to be tuned depending on the photon number regime at which the commu-



**Figure 3.10:** The optimal priors that maximizes mutual information for QPSK (keeping displacement null).



**Figure 3.11:** The optimal priors that maximizes mutual information for QPSK (simultaneously maximizing the displacement). We only show one in every 50 data points for clean visualization. Discontinuities are observed in probability values as a function of the mean photon number since the optimization routine only finds local minima. As the objective function is not convex, we do not expect to get global optima.



**Figure 3.12:** The impact of dark current on the capacity of QPSK and optimality study. Higher the dark current, the lower the capacity we get. However, at the higher photon regime, the effect of dark current is negligible.

nication system needs to operate, and properties of optical elements such as beamsplitter's transmittivity, and dark count statistics of the photodetector.

### 3.5 CONCLUSION

In this work, we proposed an optimized receiver design based on an earlier design for BPSK and QPSK modulation formats. We compared two different strategies, one with zero displacement and one with the optimal displacement that maximizes the mutual information. Our work also demonstrated the impact of optical elements' imperfections on the capacity of the receiver for QPSK. Further, we conclude that the receiver needs to be tuned based on the photon number regime, and properties of optical elements used in the optical communication system. We believe that optimization methods like the one proposed here may translate to the transmission of higher data rates over a dynamic optical link that is available for a short period. This may lead to improved communication performance over the FSO communication channel, especially for deep-space communication. In upcoming work, we strive to perform similar analysis beyond semi-classical quantum communication and apply optimization methods on quantum channels. Besides, some other practical considerations such as atmospheric turbulence, thermal noise, etc. remain that we may consider in a derivative work.



---

## OPTIMAL SQUEEZING OPERATION FOR DISPLACEMENT RECEIVER

---

“ Many receiver designs have been studied in the past to discriminate Phase-Shift Keying (PSK) quantum states that are used to encode information before transmitting over the communication channel. Among many types of quantum states, there has been significant work on the use of coherent states for encoding information. Previous work has sought to improve the communication performance in terms of various metrics such as error probability of state discrimination and capacities by employing more complex quantum states such as squeezed-displaced states. In this chapter, we use a squeezing operation with a displacement receiver for state discrimination. Our calculation demonstrates that we see no performance improvement in terms of probability of error of state discrimination as well as mutual information using displacement receivers when optimal squeezing parameters are used with squeezing operation on the transmitter side for BPSK and QPSK. In addition, we also study the receiver design scheme for QPSK modulation where squeezing is employed at the receiver side. We find that using squeezing operation on the receiver side provides an advantage in terms of increased mutual information for the low-photon regime compared to when no squeezing is used. ”

### 4.1 INTRODUCTION

Light is considered to be in a squeezed state if its electromagnetic field strength  $\mathcal{E}$  for some phases  $\Theta$  has quantum uncertainty smaller than that of a coherent state. Squeezing is nothing but reduced uncertainty in either in-phase or quadrature components. Quantum uncertainty can be quantified by performing a large number of identical measurements on identical quantum objects such as modes of light. Historically, the squeezed state was developed as the two-photon coherent state which is different from Glauber's coherent state (Glauber, 1963a). In the 1960s, Glauber wrote a series of treatises on quantum-mechanical properties of optical fields, especially focusing on coherence and correlation. He noted that photon statistics at a few photon-level lie outside the domain of classical physics. Later on, Horace P. Yuen presented the theory of two-photon coherent states (Yuen, 1976) which led to the formal development of squeezed states.

For state discrimination, a number of practical receiver designs have been proposed such as Kennedy receiver (Kennedy, 1973), and optimal Kennedy receiver (Izumi et al., 2012) that uses the coherent state to encode information using Binary Phase-Shift Keying (BPSK) modulation. Later on, the work was extended to near-optimal receiver design using Quadrature Phase Shift Keying (QPSK) in (Müller and Marquardt, 2015; Izumi et al., 2012) where no attempts were made to optimize receiver design parameters. In Chapter 3, we presented an optimal receiver design concept for BPSK and QPSK using a coherent state where we optimized the receiver design parameters for superior performance in terms of mutual information.

### CONTRIBUTION

Attempts have been made to use squeezing operation for quantum state discrimination such as one presented in (Izumi et al., 2013). However, in (Izumi et al., 2013), the squeezing was applied on the receiver side and required three separate squeezing operations. Further, the study was limited to error probability calculation. In this article, we study the impact of squeezing operation in quantum state discrimination for classical communication when squeezing is applied on the transmitter side. Our numerical study shows that on contrary to popular belief, squeezing offers no advantage in terms of state discrimination for optimal displacement receivers when squeezing is performed on the transmitter side. We present our receiver design for the case of BPSK and QPSK. We also extend (Izumi et al., 2013) to calculate the optimal mutual information when squeezing is applied on the receiver side. We find out that when squeezing is used on the receiver side, increased mutual information is achieved as compared to when purely coherent states are used.

## 4.2 SQUEEZING OPERATION

Squeezed light is a form of non-classical light in which states cannot be described by a mixture of coherent states. Squeezed states are characterized by measuring canonical continuous-variable phase-space observables. The squeezing effect can be observed continuously, independent of the time when the measurement is performed. The squeezing effect is also independent of the measurement integration time. Such properties of squeezed light can be used to enhance the sensitivity of laser interferometer or the performance of image beyond the shot noise (Vahlbruch et al., 2005; Goda et al., 2008). Squeezed light is generally obtained from laser radiation through parametric amplifiers.

We know that a coherent state  $|\alpha\rangle$  is completely described by a complex number  $\alpha$  but for a squeezed-displaced state (more commonly called squeezed state), the state is described by two complex parameters, the displacement  $\alpha$  and squeezing parameter  $z = re^{j\theta}$ . A brief description on the Fock-state expansion of squeezed-displaced states is provided in Section 2.7. Next, we discuss photon statistics for squeezed-displaced states.

### 4.2.1 PHOTON STATISTICS FOR SQUEEZED-DISPLACED STATES

The probability distribution of the number of photons in a squeezed state is obtained by squaring the coefficients in Equation (2.64). The probability of detecting  $k$  photons is given by

$$\bar{p}_n(\alpha, n = k) = \frac{p_n(\alpha, n = k)}{\sum_{k=0}^{k=n} |p_n(\alpha, n = k)|^2} \quad (4.1)$$

where  $p_n(\alpha, n = k) = \left| |re^{i\theta}, \alpha\rangle_k \right|^2$ . However, numerically, the accuracy of probability calculation is limited to how many terms we use in the Fock state expansion. The higher the number of Fock states, the better the accuracy. In this chapter, we use  $n = 30$ , beyond which no significant improvement is made in terms of probability calculation. The probability distribution of photon number in squeezed displaced state as per Equation (2.64) is given in Figure 4.1 which is inherently sub-Poissonian.

## 4.3 RECEIVER DESIGN WITH SQUEEZING OPERATION

In this section, we describe displacement receiver design for state discrimination when information is encoded using a squeezed-displaced state at the transmitter side. We also consider an alternative receiver design for QPSK modulation where squeezing is performed on the receiver side. We assess the performance of the receiver in terms of the probability of error of state discrimination and mutual information.

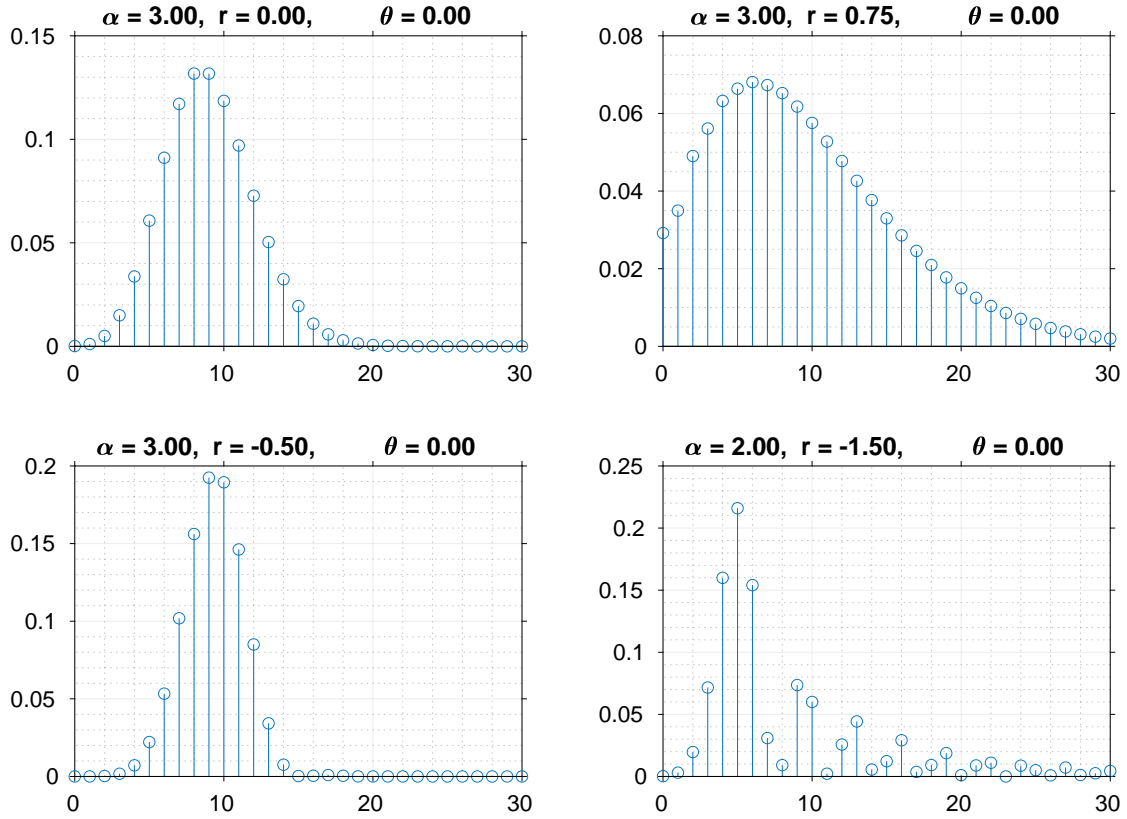
### 4.3.1 RECEIVER DESIGN FOR BPSK STATE DISCRIMINATION

Extending our work from Chapter 3, we apply squeezing operation to the reference coherent state at the transmitter side before applying displacement operation. Consider BPSK constellation representing  $\{-\alpha, \alpha\}$ , on which a Gaussian unitary operation consisting of phase-shift, displacement, and squeezing is applied and then detection of the state is performed using an on-off photodetector. The transition probability matrix for such receiver design is given in Figure 4.2. A schematic of the receiver design is provided in Figure 4.3.

### 4.3.2 RECEIVER DESIGN FOR QPSK STATE DISCRIMINATION

We apply squeezing at the transmitted side of the displacement receiver we discussed in Chapter 3. The signals to be discriminated are QPSK coherent states defined as

$$|\alpha_k\rangle = \left| \alpha e^{2\pi jk/4} \right\rangle \quad k \in \{0, 1, 2, 3\} \quad (4.2)$$



**Figure 4.1:** The probability distribution of photon number in squeezed-displaced states from Equation (2.64).

A schematic diagram of the proposed receiver is shown in Figure 4.4. We also study an alternative receiver design concept where squeezing is performed on the receiver side. In such an alternative scheme, we require three separate squeezing operations. Figure 4.5 illustrates the concept of such receiver design. The QPSK signal after squeezing is split into three branches via two beamsplitters with transmittivity  $\tau_1 = \tau_2 = \tau$ . A sequential operation of a three-port scheme is achieved by using two beamsplitters with transmittivities  $\tau_1$  and  $\tau_2$  that create three additional branches at which displacement operation  $D(\beta_i)$ ,  $i \in [1, 3]$  is applied where  $\beta_i$  are optimized displacement value. After displacement, the signal is detected by an on-off detector which decides if the signal is present or not.

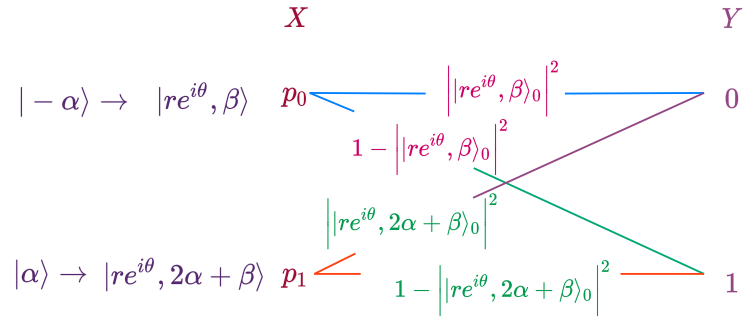


Figure 4.2: BPSK symbols and their displaced symbols.

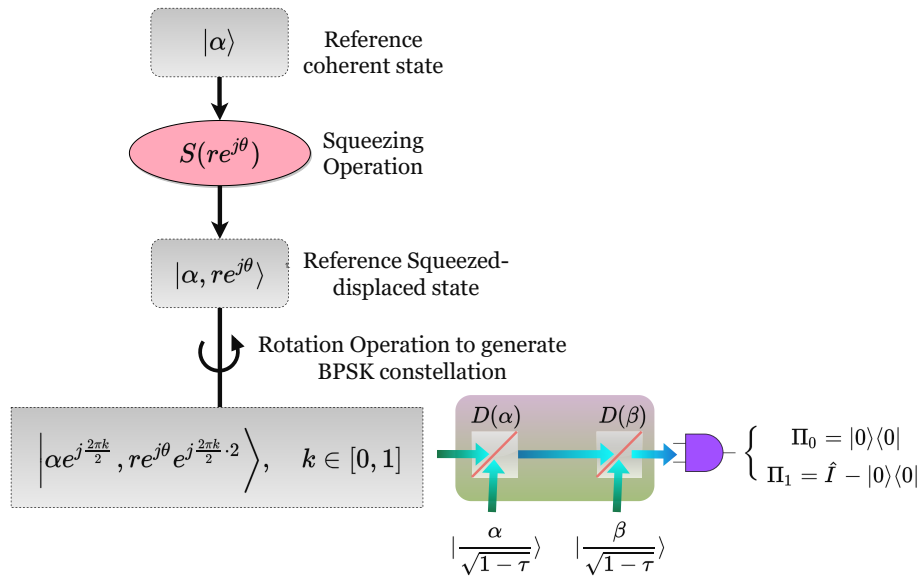


Figure 4.3: A schematic diagram of the displacement receiver with BPSK symbols. Squeezed-displaced states are used to encode information using BPSK modulation.

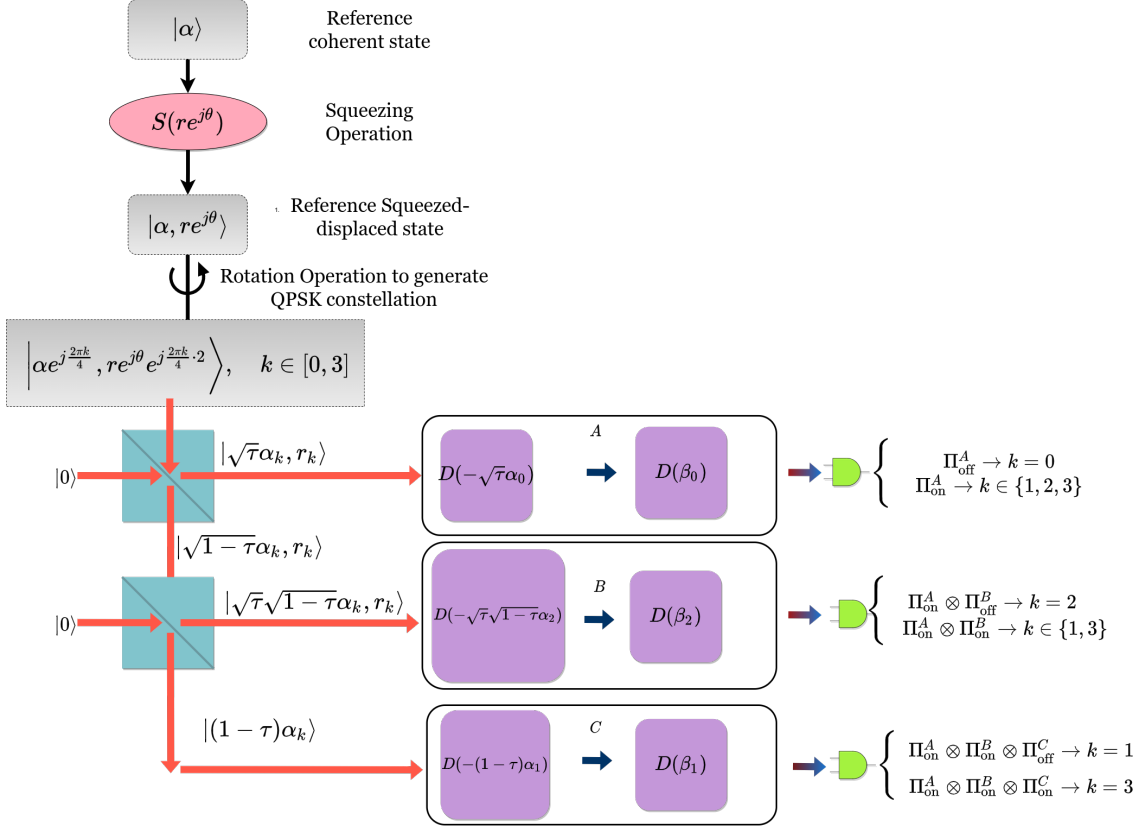


Figure 4.4: QPSK semi-classical demodulator with squeezing on transmitter side.

## 4.4 PERFORMANCE ASSESSMENT OF PROPOSED RECEIVER DESIGN

### 4.4.1 ERROR PROBABILITY CALCULATION FOR BPSK

The error probability for BPSK can be written as

$$\begin{aligned}
 P_e &= p_0 P(\text{off}|\text{on}) + p_1 P(\text{on}|\text{off}) \\
 &= p_0 P(\text{off}|\text{on}) + (1 - p_0) P(\text{on}|\text{off}) \\
 &= p_0 \bar{p}_n(2\alpha + \beta, n = 0) \\
 &\quad + (1 - p_0)(1 - \bar{p}_n(\beta, n = 0)) \equiv f(p_0, r, \theta, \beta; \alpha)
 \end{aligned} \tag{4.3}$$

where  $P(\text{off}|\text{on})$  is the probability of detecting 0 photons when in fact non-zero photon state is transmitted. We consider the case of equal prior, i.e.  $p_0 = 0.5$ . Since Equation (4.3) is monotonic in  $p_0$ , there is no such optimized  $p_0$  that minimizes Equation (4.3). However, we can perform a multivariable objective approach to minimize error probability with respect

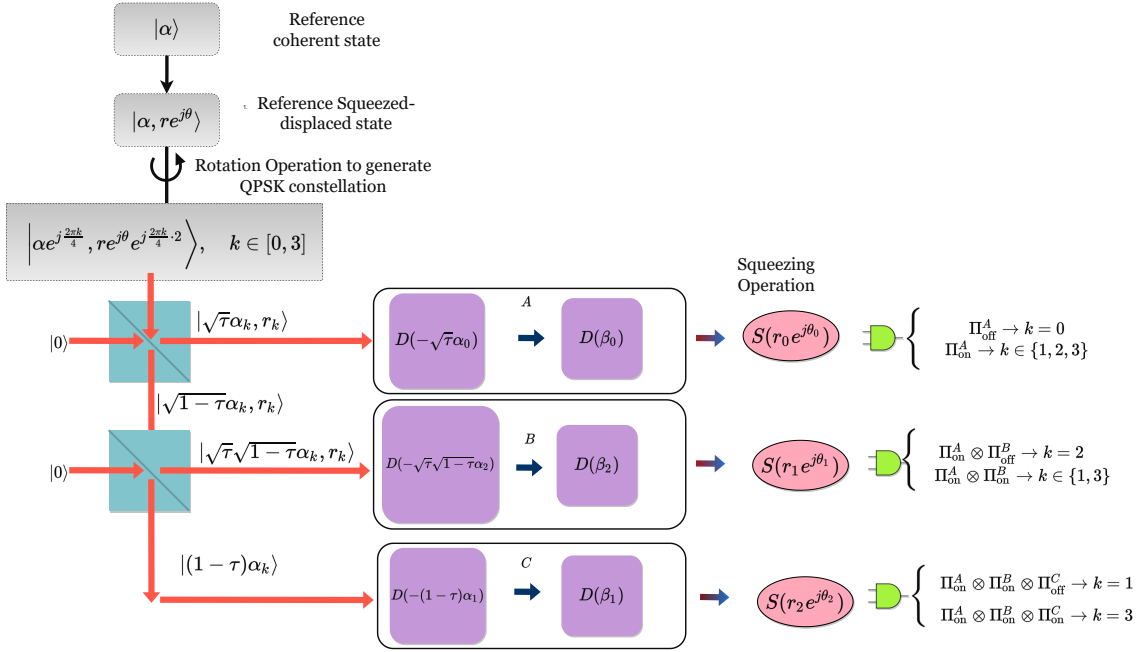


Figure 4.5: QPSK semi-classical demodulator with squeezing on receiver side.

to  $r$ ,  $\theta$ , and  $\beta$ . Our objective function in this case is

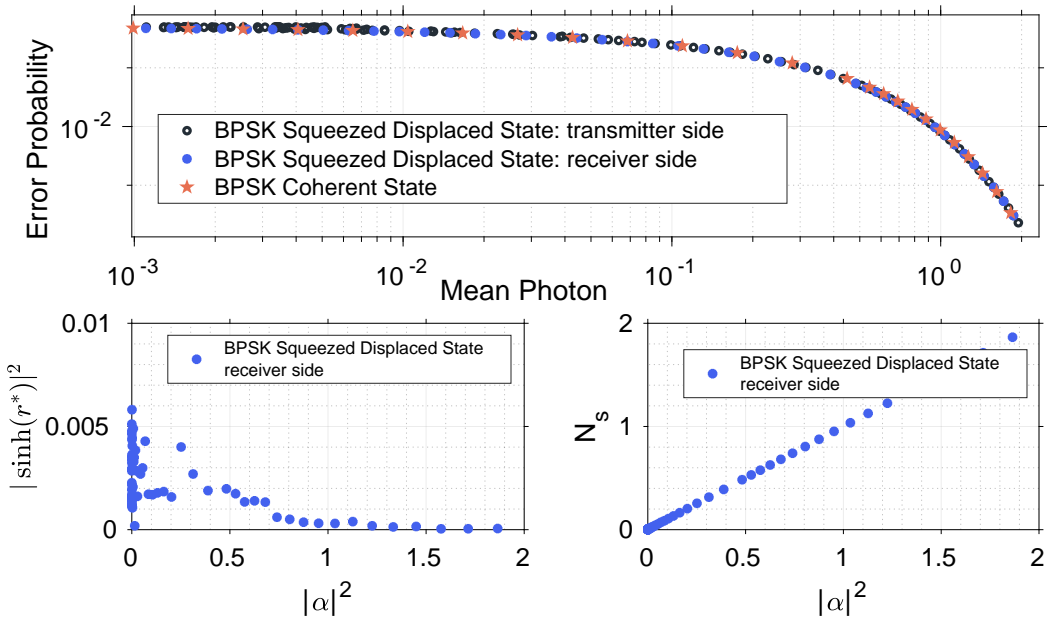
$$\min_{r, \theta, \beta} f(r, \theta, \beta; \alpha) \equiv P_e \quad (4.4)$$

subject to

$$\begin{aligned} \infty > r &\geq 0.0 \\ \pi &\geq \theta \geq -\pi \\ \beta &\in [-\infty, \infty] \end{aligned} \quad (4.5)$$

We compare the result of minimization to the case of a coherent state when no squeezing is used. Note that after applying squeezing operation, the mean photon number doesn't stay as  $N = |\alpha|^2$  for the coherent state  $|\alpha\rangle$  but rather is given by  $N_s = |\alpha|^2 + \sinh^2(r^*)$  since squeezing on the transmitted side effectively increase the mean photon.  $r^*$  is the optimized squeezing amplitude. Our results show that squeezing offers no advantage in terms of error probability when error probability is plotted against mean photon number  $N$  for the case of coherent state and  $N_s$  for the case of the squeezed displaced state, when the comparison is performed against then optimized coherent state case for Kennedy receiver with optimal nulling. The corresponding plot is shown in Figure 4.6.

We also analyzed the case of the squeezing operation on the receiver side for BPSK. In such a case, the mean photon number is  $|\alpha|^2$  but the functional form of Equation (4.3) doesn't change since displacement operation is additive. We find out that, the result is the same as for the case of transmission side squeezing, i.e. no improvement in optimal error probability due to squeezing. This is primarily due to the fact the optimized squeezing amplitude doesn't contribute significantly to the mean photon number  $N_s$  as shown in lower subplots of Figure 4.6.



**Figure 4.6:** Optimal error probability for BPSK. We compare optimal error probability when BPSK is encoded using coherent states vs when it is encoded using squeezed-displaced state. We find that squeezing offers no obvious advantage. However, squeezing operation requires additional optical elements which may complicate or introduce additional errors due to imperfect implementation.

4.4.2 MAXIMIZING MUTUAL INFORMATION FOR BPSK

In order to calculate mutual information for BPSK, we calculate posterior  $p_Y(0)$  and  $p_Y(1)$ . The posterior probability for  $Y$  is given as

$$\begin{aligned}
 p_Y(0) &= p_0 \bar{p}_n(\beta, n = 0) + p_1 \bar{p}_n(2\alpha + \beta, n = 0) \\
 p_Y(1) &= p_0 \left( 1 - \bar{p}_n(\beta, n = 0) \right) + p_1 \left( 1 - \bar{p}_n(2\alpha + \beta, n = 0) \right)
 \end{aligned}
 \tag{4.6}$$



Next, we write condition entropy as:

$$\begin{aligned}
 H(Y|X=0) &= -p_{Y|X}(Y=0|X=0) \log_2 p_{Y|X}(Y=0|X=0) \\
 &\quad - p_{Y|X}(Y=1|X=0) \log_2 p_{Y|X}(Y=1|X=0) \\
 H(Y|X=1) &= -p_{Y|X}(Y=0|X=1) \log_2 p_{Y|X}(Y=0|X=1) \\
 &\quad - p_{Y|X}(Y=1|X=1) \log_2 p_{Y|X}(Y=1|X=1)
 \end{aligned} \tag{4.7}$$

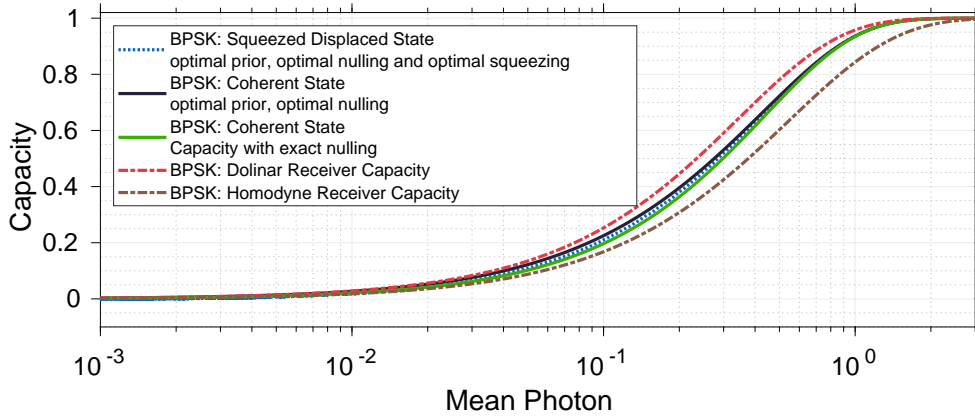
Entropy for the posterior is given by

$$H(Y) = -p_Y(0) \log_2(p_Y(0)) - p_Y(1) \log_2(p_Y(1)) \tag{4.8}$$

Finally, we can calculate mutual information as

$$I_{\text{BPSK}} = H(Y) - \sum_{i=0}^1 p(X=i) H(Y|X=i) \tag{4.9}$$

$I_{\text{BPSK}}$  is a function of priors  $p_0, p_1$ , squeezing amplitude  $r$ , squeezing phase  $\theta$ , and displacement  $\beta_0$ . We perform multivariate optimization (4.9) over priors, squeezing parameters, and displacement parameters to calculate optimal mutual information. Our results indicate that squeezing offers no advantage compared to the case when squeezing is not used. The result is summarized in Figure 4.7. In such a case using merely coherent states are sufficient.



**Figure 4.7:** A comparison of optimal mutual information (capacity) for various receiver design schemes. We find that capacity is lower for the case when squeezing is used compared to the case when squeezing is not used.

#### 4.4.3 ERROR PROBABILITY CALCULATION FOR QPSK STATE DISCRIMINATION

We are interested in optimizing the parameters of displacement operation, and squeezing operation to minimize  $P_e$ . We first consider the case when squeezing is applied on the

transmitter side. The on-off detection process is described by the measurement operator  $\Pi_i$  and the correct detection of the probability is given by

$$P_{Y|X}(Y = i|X = i) = \langle \Psi_i | \Pi_i | \Psi_i \rangle \quad (4.10)$$

From Equation (4.10), we can write average error probability as

$$P_e = 1 - \sum_{i=0}^3 p_i \cdot P_{Y|X}(Y = i|X = i) \quad (4.11)$$

We can represent Equation (4.10) as a function  $q$  of  $\alpha$ ,  $r$ , and  $\theta$ , i.e.  $q(\alpha, r, \theta)$  represents the probability of having an \*off\* outcome or detecting no photons for squeezed-displaced coherent state for quantum state  $|\alpha, re^{j\theta}\rangle$ . Based on the receiver design from Figure 4.4, our **input** QPSK constellation is as follows:

$$\begin{aligned} |\Psi_k\rangle &\equiv \left| \alpha e^{j\frac{2\pi k}{4}}, re^{j\theta} e^{j\frac{2\pi k}{4} \cdot 2} \right\rangle \equiv \left| \alpha e^{j\frac{2\pi k}{4}}, re^{j(\theta + \frac{2\pi k}{4} \cdot 2)} \right\rangle, \\ k &\in \{0, 1, 2, 3\} \end{aligned} \quad (4.12)$$

In our scheme, we generate QPSK constellation from reference squeezed-displaced coherent state  $|\alpha, re^{j\theta}\rangle$  where rotation operation  $R(\frac{2\pi k}{4})$ ,  $k \in \{0, 1, 2, 3\}$  is applied to the reference state to generate the whole constellation. The rotation operator  $R(\theta)$  introduces phases  $\theta$  to the reference squeezed-displaced state. The effect of the application of the rotation operator on the reference state is provided in (Cariolaro, 2015), Sections 7.14.5 and 11.20.

Now, we are ready to write down the probability of the current classification.  $\Pi_k$  is the correct classification of QPSK states given by Equation (4.12).  $\Pi_0$  is given by  $\langle \Omega_0 | \Pi_{\text{off}}^A | \Omega_0 \rangle$  where  $\Omega_0$  represents quantum state after optimal displacement and  $\Pi_{\text{off}}^A$  denotes measurement operator for photodetector A in Figure 4.4 when photodetector detects no photon. After splitting from the first beamsplitter, a nulling displacement  $-\tau\alpha_0$  is applied then an optimized displacement operation  $\beta_0$  is performed. An on-off photodetector performs detection and if no clicks are registered, then the first state was transmitted. Similarly, if  $\alpha_2$  is sent, the first detector won't register a click and control will go to the second arm. If  $\alpha_1$  is sent, then control will go to the second term and if the third detector doesn't register a click then  $X = 1$  was transmitted. Finally, when all of the detectors register click one by one then the fourth state was transmitted, and we decide that  $X = 3$  was transmitted. The conditional probability of correct decision is given in Equations (4.13)-(4.16).

$$P_{Y|X}(y = 0|x = 0) = \langle \Omega_0 | \Pi_{\text{off}}^A | \Omega_0 \rangle = q(\beta_0, r, \theta) \quad (4.13)$$

$$\begin{aligned} P_{Y|X}(y = 2|x = 2) &= \left( 1 - \langle \Omega_2 | \Pi_{\text{off}}^A | \Omega_2 \rangle \right) \times \langle \Omega_2 | \Pi_{\text{off}}^B | \Omega_2 \rangle \\ &= \left( 1 - q(-2\sqrt{\tau}\alpha + \beta_0, r, \theta + 2\pi) \right) \\ &\quad \times q(\beta_2, r, \theta + 2\pi) \end{aligned} \quad (4.14)$$

$$\begin{aligned}
P_{Y|X}(y = 1|x = 1) &= \left(1 - \langle \Omega_1 | \Pi_{\text{off}}^A | \Omega_1 \rangle\right) \\
&\quad \times \left(1 - \langle \Omega_1 | \Pi_{\text{off}}^B | \Omega_1 \rangle\right) \\
&\quad \times \langle \Omega_1 | \Pi_{\text{off}}^C | \Omega_1 \rangle \\
&= \left(1 - q(j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0, r, \theta + \pi)\right) \\
&\quad \times \left(1 - q(j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2, r, \theta + \pi)\right) \\
&\quad \times q(\beta_1, r, \theta + \pi)
\end{aligned} \tag{4.15}$$

$$\begin{aligned}
P_{Y|X}(y = 3|x = 3) &= \left(1 - \langle \Omega_1 | \Pi_{\text{off}}^A | \Omega_1 \rangle\right) \\
&\quad \times \left(1 - \langle \Omega_1 | \Pi_{\text{off}}^B | \Omega_1 \rangle\right) \\
&\quad \times \left(1 - \langle \Omega_1 | \Pi_{\text{off}}^C | \Omega_1 \rangle\right) \\
&= \left(1 - q(-j\sqrt{\tau}\alpha - \sqrt{\tau}\alpha + \beta_0, r, \theta + 3\pi)\right) \\
&\quad \times \left(1 - q(-j\sqrt{\tau}\sqrt{1-\tau}\alpha + \sqrt{\tau}\sqrt{1-\tau}\alpha + \beta_2, r, \theta + 3\pi)\right) \\
&\quad \times \left(1 - q(-2j(1-\tau)\alpha + \beta_1, r, \theta + 3\pi)\right)
\end{aligned} \tag{4.16}$$

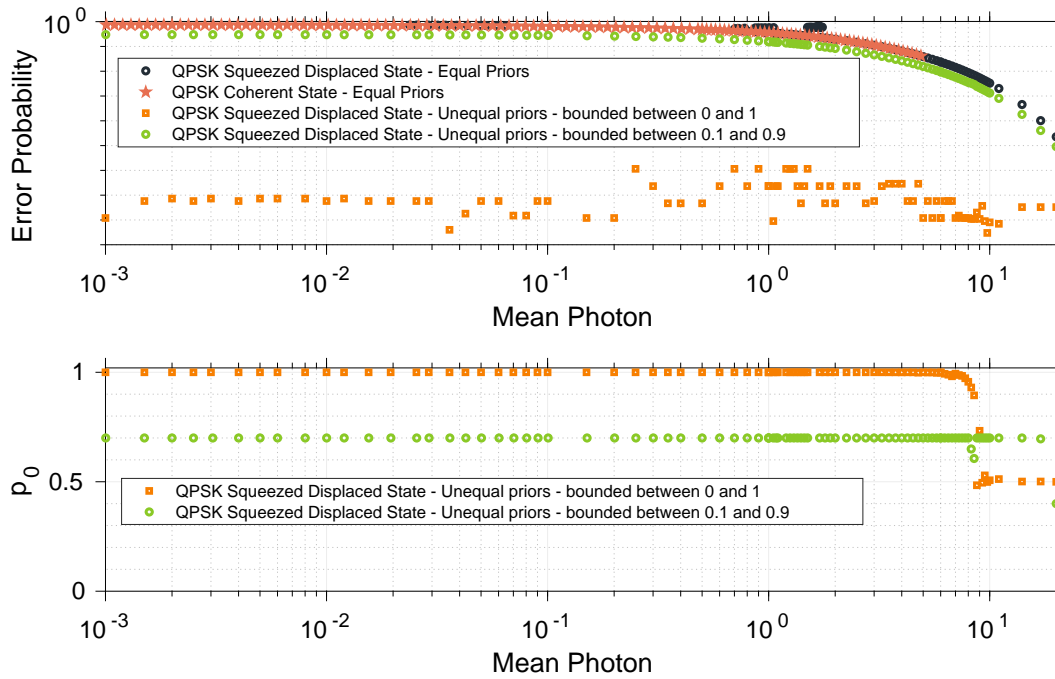
Using Equations (4.13), (4.15), and (4.14), (4.16), we can write the expression for average error probability by substituting them into Equation (4.11).

We assume two cases of optimization: equal priors and unequal priors. In the first case, optimization problem is to minimize error probability  $P_e$  over  $r$ ,  $\theta$ ,  $\beta_0$ ,  $\beta_1$ , and  $\beta_2$ . Thus, we can write  $P_e \equiv f(r, \theta, \beta_0, \beta_1, \beta_2; \alpha, \tau)$ . Thus

$$\begin{aligned}
&\min_{r, \theta, \beta_0, \beta_1, \beta_2; \alpha, \tau} f(r, \theta, \beta_0, \beta_1, \beta_2; \alpha, \tau) \\
&\quad \text{such that} \\
&\quad r \in [0, \infty) \\
&\quad \theta \in [-\pi, \pi] \\
&\quad \beta_i \in [-\infty, \infty]
\end{aligned} \tag{4.17}$$

We choose  $\tau = 0.5$ , assume the presence of no dark current and detector efficiency to be 1 for simplicity. Further, we limit the value of  $r$  within  $[0, 6]$  since it is prohibitively expensive to achieve squeezing with amplitude greater than 6. We compare the optimal error probability obtained from the optimization problem (4.17) to the error probability obtained by setting

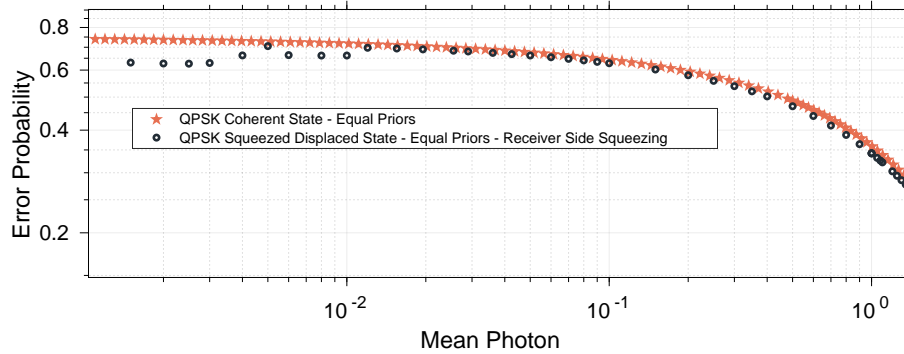
$r \approx 0$ , i.e. no squeezing. Similar to the error probability for BPSK state discrimination, squeezing in the case of QPSK state discrimination doesn't offer any advantage as shown in Figure 4.8. Further, we perform optimization for the case of unequal priors. Note that Equation (4.11) is monotonic in priors, hence we would not have any true optimized prior  $p_0$  that minimizes the error probability. However, we do demonstrate that non-uniform signaling provides a lower probability than a uniform signal. The summary of the analysis is given in Figure 4.8.



**Figure 4.8:** Optimal error probability for QPSK. We compare optimal error probability when QPSK is encoded using coherent states vs when it is encoded using squeezed-displaced state. From our results, we find that squeezing offers no obvious advantage. However, squeezing operation requires additional optical elements which may complicate or introduce additional errors during implementation. In addition, we also consider non-uniform signaling when priors are not equal. In such a case, no true optimal prior is available. However, non-uniform signaling does provide a lower error probability of state discrimination. We consider two cases while minimizing error probability: (i) when priors are bounded between 0 and 1, (ii) when priors are bounded between 0.1 and 0.9. We find that for the latter case,  $p_0$  converges to 0.7 while  $p_1$ ,  $p_2$ , and  $p_3$  attain the value of 0.1.

We also analyzed the case of using squeezing on the receiver side for which we had three separated squeezing operations as demonstrated in Figure 4.5. In such a case, we find out that, squeezing operation on the receiver side does lead to a slight improvement in error

probability as depicted in Figure 4.9.



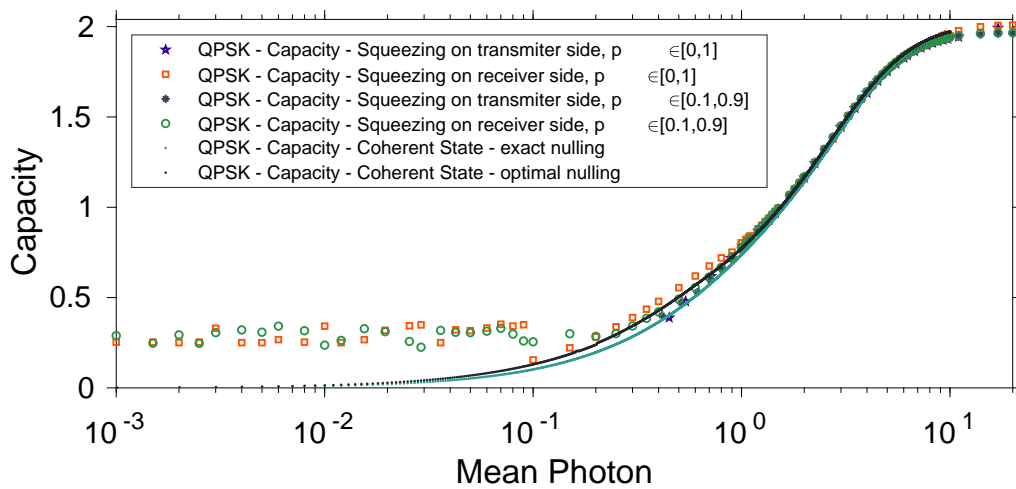
**Figure 4.9:** Optimal error probability for QPSK with squeezing operation on the receiver side. We find out that squeezing operation on receiver side improves error probability slightly as compared to one with purely coherent states.

#### 4.4.4 MAXIMIZING MUTUAL INFORMATION FOR QPSK

Similar to BPSK, we calculate the mutual information for QPSK where optimization is performed over priors, squeezing parameters, and displacement amplitudes. For squeezing on transmitter side, we consider two cases: (i) priors are constrained within  $[0,1]$ , (ii) priors are constrained within  $[0.1, 0.9]$ . Further, we put constrained on squeezing amplitude  $r$  to be within  $[0.0, 6]$  for the practical reason mentioned earlier in the chapter. Similarly, we analyze receiver design for optimal mutual information when squeezing is performed on the receiver side. We compare the maximal mutual information achieved with the case of a purely coherent state. We find out the when squeezing is performed on the receiver side, optimal mutual information is higher as compared to when no squeezing is performed at all. The result is summarized in Figure 4.10.

## 4.5 DISCUSSION AND CONCLUSION

While single-mode squeezing offers an advantage in certain cases, for example, reduced error probability for QPSK state discrimination when squeezing is performed on the receiver side, the performance is minuscule which comes at the cost of more complex circuitry. The theoretical advantage demonstrated in such a case may be lost by imperfections in the optical component used for squeezing. Based on our study, we conclude that using squeezing offers no additional advantage for a displacement-style receiver. When squeezing is applied at the transmitter side, the squeezing operation effectively increases the mean photon number. In such respect, merely using a coherent state is sufficient to achieve optimal performance



**Figure 4.10:** Optimal mutual information for QPSK with squeezing operation on the transmitter side vs on the receiver side. We find out that squeezing operation on the receiver side improves mutual information slightly as compared to when squeezing is performing on the transmitter side. Further, we find out that as compared to the purely coherent state, mutual information is greater increased when squeezing is performed on the receiver side. We observe sub-optimal solutions for certain mean photon values which may be attributed to the optimization routine being stuck on local minimal and failing to achieve global minima. Regardless, we demonstrate that it is possible to create a receiver configuration for QPSK modulation that provides increased mutual information when squeezing is used on the receiver side.

as long as long receiver design parameters are optimized. However, it is possible to use some alternative receiver design where a squeezing operation might provide a substantial advantage. We leave the exploration of such receiver design for future work.

Studies have shown that on the contrary to single-mode squeezing, two-mode squeezing provides a substantial advantage in terms of lower error probability and higher mutual information ([Hao et al., 2021](#); [Djordjevic, June 2021, Article ID: 7500114](#); [Shi et al., 2020](#)). Two-mode squeezing is used to facilitate entanglement-assisted communication which can surpass ultimate classical capacity. We describe receiver design for entanglement-assisted communication in the next chapter.





---

## OPTIMIZED RECEIVER DESIGN FOR ENTANGLEMENT-ASSISTED COMMUNICATION USING BPSK

---

“ The use of pre-shared entanglement in entanglement-assisted communication provides a superior alternative to classical communication specifically in the photon-starved regime and highly noisy environment. In this chapter, we analyze the performance of a few low-complexity receivers that employ optical parametric amplifiers. In the simulation, we demonstrate that receiver designs with an entanglement-assisted scheme using phase-shift-keying modulation can outperform classical capacities. We describe a newly proposed 2x2 optical hybrid receiver for entanglement-assisted communication whose performance is roughly 10% better in terms of error probability as compared to previously proposed optical parametric amplifier-based receivers. Further, we find that using unequal priors for BPSK provides approximately three times the advantage over equal priors in terms of information rate. ”

### 5.1 INTRODUCTION

Quantum Information Processing (QIP) has seen dramatic progress in recent decades with multiple research directions towards quantum sensing, covert communication, quantum cryptography, and so on. A quantum channel can be considered as transferring quantum information from one party (commonly referred to as Alice) to another party (commonly referred to as Bob). In the case of a perfect channel, the transfer of the quantum information remains intact while if the channel is noisy, some changes occur to the quantum information being transmitted. Quantum channels can also be used to carry classical information. Further, if the channel is noisy within a certain limitation, the quantum channel can be used to share entanglement between Alice and Bob. A pre-shared entanglement can be used to improve classical capacity and evade an adversary, commonly known as Eve (Holevo and Werner, 2001; Holevo, 2002; Bennett et al., 2002; Shi et al., 2020; Zhuang, 2021). Recent experiments have demonstrated that even in the case of entanglement breaking scenario, the rate of entanglement assisted (EA) communication can be much larger than the communication without entanglement (Zhang et al., 2015; Hao et al., 2021). For the Holevo Schumacher-Westmoreland (HSW) capacity  $C$  in the classical regime, and the entanglement-assisted

Capacity  $C_{\text{EA}}$ , the ratio  $\frac{C_{\text{EA}}}{C}$  diverge logarithmically with the inverse of the signal power over a lossy and noisy Bosonic channel (Holevo, 2002).

Some recent efforts have been developed to propose receiver design for EA communication where authors have used Gaussian approximation for determining bit error rate (BER) (Guha, 2009; Shi et al., 2020; Zhuang, 2021; Djordjevic, June 2021, Article ID: 7500114). The previously proposed design of the receiver is limited to a demonstration using BPSK with repetition coding over more than  $10^6$  bosonic modes that occupy the whole C-band and a portion of the L-band.

In this work, we analyze the receiver design for EA communication using Optical Parametric Amplifier (OPA) and show that EA communication doesn't need to occupy the whole C-band. Additionally, we analyze a 2x2 optical hybrid-based receiver for EA communication which is suitable for implementation in integrated optics and quantum nanophotonics. We further propose an optimized hypothesis testing scheme and numerically demonstrate that optimized receiver design provides superior communication capacity as compared to capacity obtained without entanglement assistance. When employing the BPSK modulation format to represent the digital information, we find that non-equal priors perform at least three times superior in terms of information rate when compared to an equal prior encoding scheme.

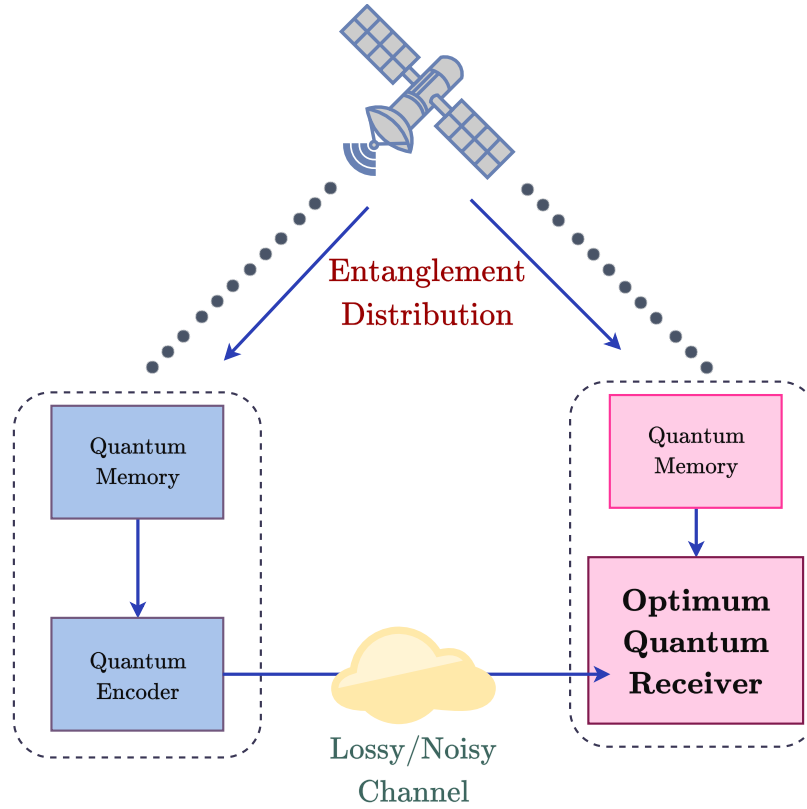
The rest of the chapter is organized as follows. In Section 5.2, we provide a brief review of entanglement-assistance with mathematical formalism required for the rest of the chapter. In Section 5.3, we discuss receiver design scheme followed by their evaluation in Section 5.4.

## 5.2 ENTANGLEMENT ASSISTED CLASSICAL COMMUNICATION CONCEPT

An entanglement state is defined to be one whose quantum state cannot be factored as product states of its local constituents. In other words, they are individual particles but inseparable as a whole. As an example, given two basis vectors  $\{|0\rangle_A, |1\rangle_A\}$  in Hilbert space  $\mathcal{H}_A$  and  $\{|0\rangle_B, |1\rangle_B\}$  in Hilbert space  $\mathcal{H}_B$ , then  $\frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$  is in an entangled state. If a composite system is in an entangled state, it is impossible to attribute either system A or B a definite pure state. Even if the von Neumann entropy of the whole state is zero, the entropy of the subsystem is greater than zero. In this sense, we can say that the systems are entangled.

In Entanglement-assisted classical communication, either optic fiber or satellites can be used to distribute the entangled states which are stored in quantum memories. On the transmitter side, Alice transmits classical data using signal photon of entangled pair, marred by noisy and lossy quantum channel. Bob, on the receiver side, employs idler photon of entangled pair to make a decision about what was transmitted using an optimum quantum receiver.

The overall design is shown in Figure 5.1. We can assume that some error correction is applied to quantum states to restore information transmitted and to alleviate the effect of decoherence.



**Figure 5.1:** An illustration showing the concept of EA communication.

### 5.3 RECEIVER DESIGN FOR EA COMMUNICATION

Entanglement-assisted communication requires two-mode Gaussian states that are generated by spontaneous parametric down-converted entangled-photon pairs. The SPDC source is a broadband source with modes  $M = T_m W$  independently and identically distributed source-idler pair where  $W$  is phase-matching bandwidth and  $T_m$  is the measurement interval. An SPDC process generates  $M$  independent pairs of signal-idler photons in space and time denoted by their annihilation operation  $\{\hat{a}_s^{(m)}, \hat{a}_i^{(m)}\}$ ,  $m \in [1, M]$ , prepared in identical entangled two-mode squeezed vacuum (TMSV) state. They can be represented in Fock

state basis as

$$|\psi\rangle_{si} = \sum_0^{\infty} \sqrt{\frac{N_s^n}{(N_s + 1)^{n+1}}} |n\rangle_s |n\rangle_i \quad (5.1)$$

where  $N_s$  is the mean photon number in each of signal and idler (Mauerer et al., 2009; Guha, 2009). TMSV belongs to a class of Gaussian states where  $M$ -modes Gaussian state  $\hat{\rho}$  comprising of  $\{\hat{a}^{(m)}, m \in [1, M]\}$  modes is characterized by mean and variance of their respective quadrature field operators such that  $\hat{a}^{(m)} = \hat{p}^{(m)} + j\hat{q}^{(m)}$ . Covariance matrix for a TMSV state is given by Equation (5.2) where  $\mathbf{I}$  and  $\mathbf{Z}$  are  $2 \times 2$  Pauli matrices. If we consider

$$\Lambda_{\text{TMSV}} = \begin{bmatrix} 2N_s + 1 & 0 & 2\sqrt{N_s(N_s + 1)} & 0 \\ 0 & 2N_s + 1 & 0 & 2\sqrt{N_s(N_s + 1)} \\ 2\sqrt{N_s(N_s + 1)} & 0 & 2N_s + 1 & 0 \\ 0 & -2\sqrt{N_s(N_s + 1)} & 0 & 2N_s + 1 \end{bmatrix} \quad (5.2)$$

$$= \begin{bmatrix} (2N_s + 1)\mathbf{I} & 2\sqrt{N_s(N_s + 1)}\mathbf{Z} \\ 2\sqrt{N_s(N_s + 1)}\mathbf{Z} & (2N_s + 1)\mathbf{I} \end{bmatrix}$$

the Phase-shift keying (PSK) modulation scheme for communication, then mathematically, we can use the unitary operator  $\hat{U}_\theta = e^{j\hat{a}^\dagger \hat{a}}$  to denote rotation of base annihilation operator  $\hat{a}$ . For transmitting information using entangled photons generated from SPDC, a signal photon of signal-idler pair is used while idler is pre-shared before transmission happens. The received photon mode (after passing through the communication channel) at Bob's end is denoted by  $\hat{a}_R = \hat{a}_{R'} e^{j\theta}$ . Note that from here onwards, we drop the mode notation from the annihilation operator for simplicity. Under the phase-encoding scheme, the covariance matrix of the return-idler pair  $\{\hat{a}_R, \hat{a}_I\}$  is given by Equation (5.3) where  $N_R = \eta N_s + N_B$ ,

$$\begin{bmatrix} (2(N_s + \eta N_B) + 1)\mathbf{I} & 2\sqrt{\eta N_s(N_s + 1)}\mathbf{Z} R e^{[e^{j\theta}(Z - jX)]} \\ 2\sqrt{\eta N_s(N_s + 1)} R e^{[e^{j\theta}(Z - jX)]}\mathbf{Z} & (2N_R + 1)\mathbf{I} \end{bmatrix} \quad (5.3)$$

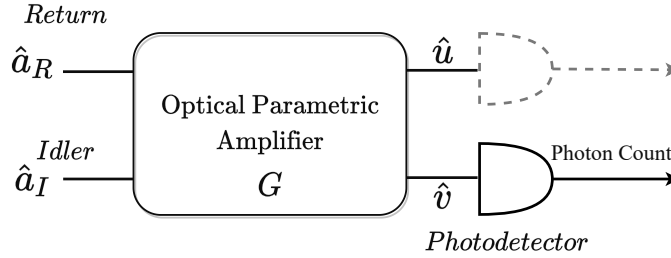
$\eta$  being the transmittivity of Bosonic channel, and  $N_B$  the mean photon number of thermal mode. In order to transmit the information, Alice modulates the signal  $\hat{a}_{s'}$  with the help of a phase modulator to apply rotation  $\theta$  to modulate the signal photon. The signal passes through lossy thermal Bosonic quantum channel and is received by Bob as  $\hat{a}_R = \hat{a}_{R'} e^{j\theta}$  where  $\hat{a}_{R'}$  is the base photon mode at the receiving end. Bob uses the idler part of the pre-shared entanglement photon pair and an optimum quantum detector to make hypothesis testing to decide which symbol was transmitted.

### 5.3.1 OPA BASED RECEIVER WITH THRESHOLD DETECTION

A joint detection receiver for state discrimination of EA communication consists of an optical parametric amplifier (OPA). At the receiver side, an Optical Parametric Amplifier (OPA) is used to combine return-idler pair as shown in Figure 5.2. The return and idler modes are evolved as given by Heisenberg's picture as

$$\begin{aligned}\hat{u} &= \sqrt{G}\hat{a}_R + \sqrt{G-1}\hat{a}_I^\dagger \\ \hat{v} &= \sqrt{G}\hat{a}_I + \sqrt{G-1}\hat{a}_R^\dagger\end{aligned}\quad (5.4)$$

where  $G$  is gain of OPA such that  $G = 1 + \epsilon, \epsilon \ll 1$ . OPA receiver can be used to



**Figure 5.2:** Operating Principle of Optical Parametric Amplifier (OPA): At the receiver end, parametric amplification is applied to return-idler pair with gain  $G$ . Error probability of discrimination is higher at  $\hat{u}$ , hence the photon detection is made  $\hat{v}$ .

combine and amplify return-idler pair using a strong local pump that gives rise to a pair of Equations given by (5.4). At output ports, a photodetector is used to do photon counting and a threshold detection rule is applied to make state discrimination. Let us assume photodetector output operator as  $\hat{u}$  and  $\hat{v}$  at two output ports which can be commonly called as return and idler output port respectively. For each output, the mean photon number is given by expectation  $\langle \hat{u}^\dagger \hat{u} \rangle$  or  $\langle \hat{v}^\dagger \hat{v} \rangle$  depending on whether threshold detection is made at signal output port or idler output port.

The photocurrent operator and its expectation is given by Equations (5.5) and (5.6). Assuming M-ary PSK modulation is imposed by the phase modulator, the return mode at return port is given by  $\hat{a}_R = \hat{a}_R e^{i\theta}$  where  $\theta$  is the phase shift introduced by the phase modulator. Further, we assume mean photon number  $N_i = N_s$  for TMSV states where  $N_i$  is the mean photon number for idler mode and  $N_s$  is the mean photon number for signal mode. In the case of a pre-shared entangled state, the idler is assumed to be undisturbed, hence at the receiver side, the idler mean photon number  $N_I = N_i = N_s$ . However, signal mode passes through a thermal lossy bosonic channel, hence signal mode is altered and called return mode on the receiver side with mean photon number  $N_R = \eta N_s + N_B$ .

For practical communication, consider that information is encoded using repetition code-words that employ Binary Phase-Shift Keying (BPSK) modulation with phases  $\theta \in \{0, \pi\}$ .

$$\begin{aligned}
\hat{u}^\dagger \hat{u} &= (\sqrt{G}\hat{a}_R^\dagger + \sqrt{G-1}\hat{a}_I)(\sqrt{G}\hat{a}_R + \sqrt{G-1}\hat{a}_I^\dagger) \\
&= G\hat{a}_R^\dagger \hat{a}_R + \sqrt{G(G-1)}\hat{a}_R^\dagger \hat{a}_I^\dagger + \sqrt{G(G-1)}\hat{a}_I \hat{a}_R + (G-1)\hat{a}_I \hat{a}_I^\dagger \\
&= G\hat{a}_R^\dagger \hat{a}_R + (\sqrt{G(G-1)})(\hat{a}_R^\dagger \hat{a}_I^\dagger + \hat{a}_I \hat{a}_R) + (G-1)\hat{a}_I \hat{a}_I^\dagger \\
\langle \hat{u}^\dagger \hat{u} \rangle &= G \langle \hat{a}_R^\dagger \hat{a}_R \rangle + (\sqrt{G(G-1)})(\langle \hat{a}_R^\dagger \hat{a}_I^\dagger \rangle + \langle \hat{a}_I \hat{a}_R \rangle) + (G-1) \langle \hat{a}_I \hat{a}_I^\dagger \rangle \\
&= GN_R + \sqrt{G(G-1)}(e^{j\theta} + e^{-j\theta})\sqrt{\eta N_s(N_s+1)} + (G-1)(1+N_I) \\
\text{As, } \hat{a}_R &= \hat{a}_{R'} e^{j\theta}, \quad \langle \hat{a}_{R'} \hat{a}_I \rangle = \sqrt{\eta N_s(N_s+1)}, \quad \hat{a}_I \hat{a}_I^\dagger = \hat{a}_I^\dagger \hat{a}_I + I \\
\text{Further, } N_R &= \eta N_s + N_B \text{ after passing through a channel} \\
&\text{with mean thermal photon number } N_B \\
N_I &= N_s, \text{ As, idler is per-shared}
\end{aligned}$$

$$\bar{N}_1(\theta) = \langle \hat{u}^\dagger \hat{u} \rangle = G(\eta N_s + N_B) + (G-1)(1+N_s) + 2 \cos \theta \sqrt{G(G-1)} \sqrt{\eta N_s(N_s+1)} \quad (5.5)$$

$$\begin{aligned}
\hat{v}^\dagger \hat{v} &= (\sqrt{G}\hat{a}_I^\dagger + \sqrt{G-1}\hat{a}_R)(\sqrt{G}\hat{a}_I + \sqrt{G-1}\hat{a}_R^\dagger) \\
\langle \hat{v}^\dagger \hat{v} \rangle &= GN_I + 2 \cos \theta \sqrt{G(G-1)} \sqrt{\eta N_s(N_s+1)} + (G-1)(1+N_R) \\
\bar{N}_2(\theta) = \langle \hat{v}^\dagger \hat{v} \rangle &= GN_s + (G-1)(1+\eta N_s + N_B) + 2 \cos \theta \sqrt{G(G-1)} \sqrt{\eta N_s(N_s+1)} \quad (5.6)
\end{aligned}$$

---

Decoding BPSK can be modeled as hypothesis testing such that detecting if  $H_0$  is true, then BPSK symbol with  $\theta = 0$  was transmitted, and if the hypothesis  $H_1$  is true, then the symbol with  $\theta = \pi$  was transmitted.

To allow for efficient error correction, repeated PSK codewords consisting of  $M$  signal-idler pairs are used in EA communication (Shi et al., 2020). In a joint-detection scheme, the receiver mixes all  $M$  received modes and counts the total number of photons at output ports. Under the hypothesis testing, if a total number of photons detected is  $N < N_{\text{th}}$ , then  $H_0$  is true, otherwise,  $H_1$  is true. Joint detection state, in this case, becomes  $M$ -fold tensor product  $\rho^{\otimes M}$  with identical zero-mean thermal states and per mode mean photon is given by  $\bar{N}_1(\theta)$  or  $\bar{N}_2(\theta)$ , depending on which output port of OPA we decide to use. Optimum joint measurement for state discrimination requires photon counting at an output port and decide between two hypotheses using total photon  $N$  over  $M$  modes. Under such scenario,

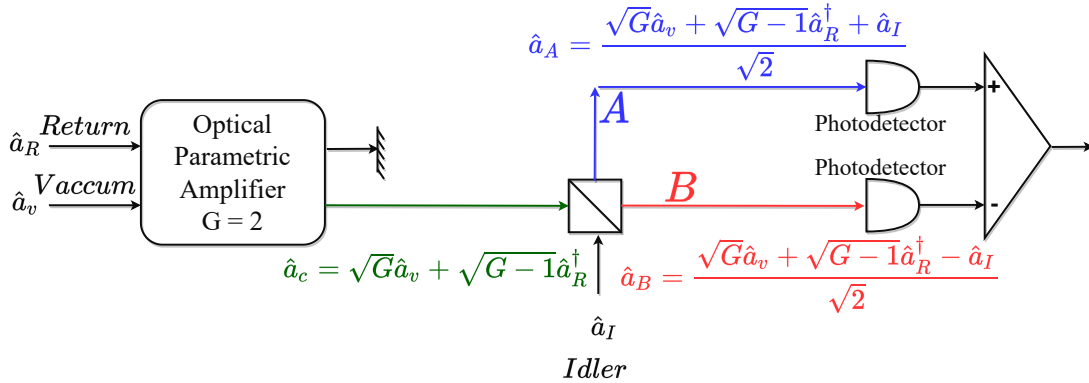
the probability mass function (pmf) is negative binomial with mean  $M\bar{N}(\theta)$ , and standard deviation  $\sigma(\theta) = \sqrt{M\bar{N}(\theta)(\bar{N}(\theta) + 1)}$  given by

$$P_{\text{OPA}}(n|\theta; M) = {}^{n+M-1}C_n \left( \frac{\bar{N}(\theta)}{1+\bar{N}(\theta)} \right)^n \left( \frac{1}{1+\bar{N}(\theta)} \right)^M \quad (5.7)$$

where  $\bar{N}$  is generalized representation for  $\bar{N}_1$  and  $\bar{N}_2$ . Equation (5.7) can be approximated as Gaussian distribution with mean  $M\bar{N}(\theta)$ , and standard deviation  $\sigma(\theta) = \sqrt{M\bar{N}(\theta)(\bar{N}(\theta) + 1)}$ , for sufficiently large  $M$ . At the detector end, we use threshold detection, and decide in the favor of  $H_0$  if the total number of photons detected is  $N < N_{\text{th}}(\theta)$  otherwise  $H_1$  for  $N \geq N_{\text{th}}(\theta)$  where  $N_{\text{th}}(\theta)$  is the threshold number of photons which is a function of phase  $\theta$ .

### 5.3.2 OPTICAL PHASE CONJUGATION RECEIVER

OPA can also be used in a different fashion where return  $\hat{a}_R$  mode can interact with vacuum mode  $\hat{a}_v$  to produce  $\sqrt{G}\hat{a}_v + \sqrt{G-1}\hat{a}_R^\dagger$  which becomes  $\hat{a}_c = \sqrt{2}\hat{a}_v + \hat{a}_R^\dagger$  for  $G = 2$ . By mixing idler with  $\hat{a}_c$  using a 50-50 beamsplitter, we get two modes  $\frac{1}{\sqrt{2}}(\hat{a}_c \pm \hat{a}_I)$ . Output from two arms are fed to a balanced detector and difference of the detector is measured as photocurrent. We call this Optical Phase Conjugate receiver or OPC receiver. Consider the schematic of OPC receiver given in Figure 5.3. For the case of BPSK, the mean photon



**Figure 5.3:** Operating Principle of Optical Phase Conjugate (OPC) receiver: signal interacts with vacuum followed by mixing with idler using 50-50 beamsplitter and a balanced detection is applied using photodetectors.

operators of two output arms of beamsplitters are given by Equation (5.8).

$$\hat{a}_{A/B}^\dagger \hat{a}_{A/B} = \frac{1}{2} \left[ (G-1) \hat{a}_R \hat{a}_R^\dagger \pm \sqrt{G-1} \hat{a}_R \hat{a}_I \pm \sqrt{G-1} \hat{a}_I^\dagger \hat{a}_R^\dagger + \hat{a}_I^\dagger \hat{a}_I \right] \quad (5.8)$$

with + sign for arm A and – sign for arm B.

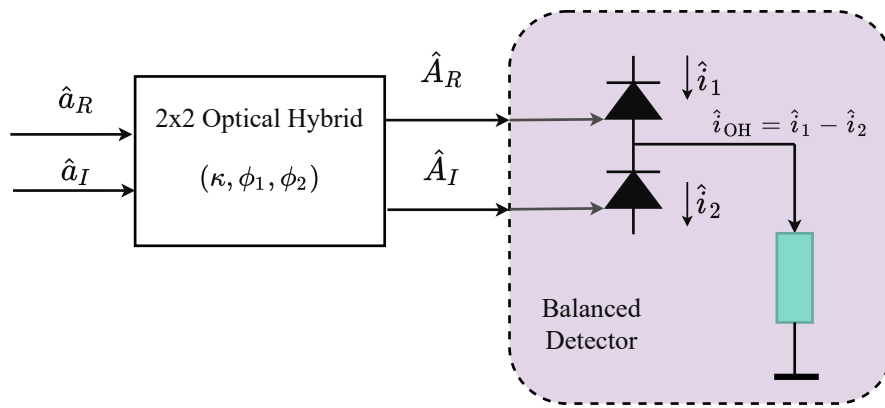
We adopt a joint-detection scheme similar to one adopted for the OPA receiver discussed in Section 5.3.1 containing  $M$  modes for error correction. The difference of mean photon number detected at two photodetectors of OPC is converted to photocurrent with photocurrent operator  $\hat{b}$  given by

$$\begin{aligned} \hat{b} &= \hat{a}_A^\dagger \hat{a}_A - \hat{a}_B^\dagger \hat{a}_B = \sqrt{G-1} \hat{a}_R \hat{a}_I + \sqrt{G-1} \hat{a}_I^\dagger \hat{a}_R^\dagger \\ N_{\text{OPC}}(\theta) &= \langle \hat{b} \rangle = 2 \cos \theta \sqrt{\eta N_s (N_s + 1)}, \\ \text{as, } \hat{a}_R &= \hat{a}_{R'} e^{j\theta}, \\ \langle \hat{a}_{R'} \hat{a}_I \rangle &= \sqrt{\eta N_s (N_s + 1)}, \quad \hat{a}_R \hat{a}_R^\dagger = \hat{a}_R^\dagger \hat{a}_R + I \end{aligned} \quad (5.9)$$

Variance  $\sigma_{\text{OPC}}^2$  is given by

$$\begin{aligned} \sigma_{\text{OPC}}^2(\theta) &= \langle \hat{b}^2 \rangle - \langle \hat{b} \rangle^2 \\ &= N_s (\eta N_s + N_B + 1) \\ &\quad + (N_s + 1) (\eta N_s + N_B + 1) \\ &\quad - 2 (\eta N_s (N_s + 1)) \cos 2\theta - 4 (\eta N_s (N_s + 1)) \cos^2 \theta \end{aligned} \quad (5.10)$$

### 5.3.3 2x2 OPTICAL HYBRID RECEIVER BASED JOINT RECEIVER



**Figure 5.4:** Receiver configuration of a  $2 \times 2$  optical hybrid based joint balanced detection receiver.



In this section, we describe a practical receiver design using a 2x2 optical hybrid for EA communication. An optical hybrid-based joint detection scheme is suitable for EA communication since it can be directly implemented in integrated optics and quantum nanophotonics. For a two-dimensional constellation, a 2x2 optical hybrid receiver may be used as shown in Figure 5.4. A detailed discussion of optical hybrid receiver design can be found in (Djordjevic, June 2021, Article ID: 7500114) where Gaussian modulation has also been discussed. The scattering matrix  $\mathcal{S}$  of 2x2 optical hybrid is described by

$$\mathcal{S} = \begin{bmatrix} e^{j\phi_1} \sqrt{1-\kappa} & \sqrt{1-\kappa} \\ \sqrt{1-\kappa} & e^{j\phi_2} \kappa \end{bmatrix} \quad (5.11)$$

with  $\kappa$  being the power-splitting ratio of Y-junction in a 2x2 optical hybrid. Return and idler at the receiver is transformed based on the scattering matrix

$$\begin{bmatrix} \hat{A}_R \\ \hat{A}_I \end{bmatrix} = \mathcal{S} \begin{bmatrix} \hat{a}_R \\ \hat{a}_I \end{bmatrix}. \quad (5.12)$$

With equal power splitting  $\kappa = 0.5$ , we can write

$$\begin{bmatrix} \hat{A}_R \\ \hat{A}_I \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{j\phi_1} & 1 \\ 1 & e^{j\phi_2} \end{bmatrix} \begin{bmatrix} \hat{a}_R \\ \hat{a}_I \end{bmatrix} \quad (5.13)$$

For BPSK,  $\hat{a}_R = \hat{a}_{R'} e^{j\theta}$  with  $\theta \in \{0, \pi\}$ . The photocurrent operator is given by

$$\begin{aligned} \hat{i}_{\text{OH}} &= \frac{1}{2} e^{-j\theta} (e^{-j\phi_1} - e^{j\phi_2}) \hat{a}_{R'}^\dagger \hat{a}_I \\ &+ \frac{1}{2} e^{j\theta} (e^{j\phi_1} - e^{-j\phi_2}) \hat{a}_I^\dagger \hat{a}_{R'} \end{aligned} \quad (5.14)$$

The expectation of photocurrent is given by

$$\begin{aligned} N_{\text{OH}} = \langle \hat{i}_{\text{OH}} \rangle &= \frac{1}{2} e^{-j\theta} \sqrt{\eta N_s (N_s + 1)} (e^{-j\phi_1} - e^{j\phi_2}) \\ &+ \frac{1}{2} e^{j\theta} \sqrt{\eta N_s (N_s + 1)} (e^{j\phi_1} - e^{-j\phi_2}) \end{aligned} \quad (5.15)$$

In this chapter, we consider a special case of 2x2 optical hybrid receiver where  $\phi_1 = 0$  and  $\phi_2 = \pi$ , for which,  $N_{\text{OH}} = 2\sqrt{\eta N_s (N_s + 1)} \cos \theta$ . The variance of the photocurrent operator

is given by

$$\begin{aligned}
\sigma_{\text{OH}}^2 &= \langle \hat{i}_{\text{OH}}^2 \rangle - \langle \hat{i}_{\text{OH}} \rangle^2 \\
&= \frac{1}{4} |e^{j\phi_1} - e^{-j\phi_2}|^2 (2N_R N_I + N_R + N_I) \\
&\quad + \frac{\eta N_s (N_s + 1)}{4} \left[ \left( \langle e^{-2j\theta} \rangle - e^{-2j\theta} \right) (e^{-j\phi_1} - e^{j\phi_2})^2 \right] \\
&\quad + \frac{\eta N_s (N_s + 1)}{4} \left[ \left( \langle e^{2j\theta} \rangle - e^{2j\theta} \right) (e^{j\phi_1} - e^{-j\phi_2})^2 \right] \\
&\quad - \frac{\eta N_s (N_s + 1)}{2} e^{-j\theta} e^{j\theta} |e^{j\phi_1} - e^{-j\phi_2}|^2
\end{aligned} \tag{5.16}$$

For equi-prior BPSK symbols,  $\langle e^{\pm 2j\theta} \rangle = (e^{\pm 2j\pi} + e^{\pm 2j \cdot 0})/2 = 1$ . For non-equi prior symbols with priors  $p_0$  and  $p_1$ ,  $\langle e^{\pm 2j\theta} \rangle$  is calculated as  $p_0 e^{\pm 2j\pi} + p_1 e^{\pm 2j \cdot 0}$  which is still 1. Further, regardless of phase value  $\theta \in \{0, \pi\}$  for BPSK symbols,  $e^{\pm 2j\theta} = \cos 2\theta$ . Putting these values in Equation (5.16), we can rewrite variance of photocurrent for BPSK as

$$\begin{aligned}
\sigma_{\text{OH}}^2 &= \frac{1}{4} |e^{j\phi_1} - e^{-j\phi_2}|^2 (2N_R N_I + N_R + N_I) \\
&\quad + \frac{\eta N_s (N_s + 1)}{4} \left[ \left( 1 - \cos 2\theta \right) (e^{-j\phi_1} - e^{j\phi_2})^2 \right] \\
&\quad + \frac{\eta N_s (N_s + 1)}{4} \left[ \left( 1 - \cos 2\theta \right) (e^{j\phi_1} - e^{-j\phi_2})^2 \right] \\
&\quad - \frac{\eta N_s (N_s + 1)}{2} |e^{j\phi_1} - e^{-j\phi_2}|^2
\end{aligned} \tag{5.17}$$

For the special of  $\phi_1 = 0$  and  $\phi_2 = \pi$ , the variance for BPSK is

$$\begin{aligned}
\sigma_{\text{OH}}^2(\theta) &= (2N_R N_I + N_R + N_I) \\
&\quad + 2\eta N_s (N_s + 1) (1 - \cos 2\theta) - 2\eta N_s (N_s + 1)
\end{aligned} \tag{5.18}$$

where  $N_R = \eta N_s + N_B$  and  $N_I = N_s$ .

## 5.4 EVALUATION OF ENTANGLEMENT-ASSISTED COMMUNICATION RECEIVERS

### 5.4.1 ERROR PROBABILITY CALCULATION

The probability of error of state discrimination for the case of BPSK using OPA is given by

$$P_E = p_0 P_{\text{OPA}}\left(n < N_{\text{th}} | \theta = 0; M\right) + p_1 \left[1 - P_{\text{OPA}}\left(n < N_{\text{th}} | \theta = \pi; M\right)\right]. \quad (5.19)$$

An optimum value of  $N_{\text{th}}$  can be found by equating individual error term in Equation (5.19) which, for case of equi-probable symbols gives us  $N_{\text{th}}(\theta) = \frac{M(\sigma(\pi)\bar{N}(0) + \sigma(0)\bar{N}(\pi))}{(\sigma(\pi) + \sigma(0))}$ . However, for unequal priors, the optimum threshold  $N_{\text{th}}$  is the one that satisfies the condition

$$p_0 P_{\text{OPA}}\left(n < N_{\text{th}} | \theta = 0; M\right) = p_1 \left[1 - P_{\text{OPA}}\left(n < N_{\text{th}} | \theta = \pi; M\right)\right]. \quad (5.20)$$

We solve Equation (5.20) for  $N_{\text{th}}$  using grid search procedure and plug into Equation (5.19) to calculate the error probability.

The joint detection can either be made at the idler output port or signal output port (i.e. return port). The error probability of discrimination is higher at the return port compared to detection made at the idler port, as shown in Figure 5.5b. As a result, our further analysis solely focuses on making joint detection at the idler port. We find out that for the case of non-equal priors, the mean threshold photon for BPSK discrimination is higher for any detection made at the return output port than at the idler output port (see Figure 5.6). Note that even though the error probability  $P_E$  in Equation (5.19) is a convex function of  $N_{\text{th}}$ , it is monotonic function of prior  $p_0$ , as shown in Figure 5.7. Hence, there doesn't exist an optimum prior that minimizes the probability of error of state discrimination.

For the case of the OPC receiver, we calculate the error probability by taking Gaussian approximation of photodetection statistics as we measure the difference of photocurrent obtained at two arms of the beamsplitter at the detection side (Figure 5.3). The Gaussian approximation yields the probability of error formula given by Equation (5.21)

$$P_E = p_0 \mathcal{F}_{\text{OPC}}\left(N_{\text{th}}, M \cdot N_{\text{OPC}}(0), \sqrt{M} \cdot \sigma_{\text{OPC}}(0)\right) + p_1 \left[1 - \mathcal{F}_{\text{OPC}}\left(N_{\text{th}}, M \cdot N_{\text{OPC}}(\pi), \sqrt{M} \cdot \sigma_{\text{OPC}}(\pi)\right)\right] \quad (5.21)$$

where  $N_{\text{OPC}}(\theta)$  and  $\sigma_{\text{OPC}}$  are given by Equations (5.9) and (5.10) respectively, and  $\mathcal{F}_{\text{OPC}}$  is cumulative distribution function of Gaussian distribution with mean  $M \cdot N_{\text{OPC}}(\theta)$  and standard deviation  $\sqrt{M} \cdot \sigma_{\text{OPC}}$ . Similar to the OPA receiver, we can calculate optimum  $N_{\text{th}}$

by equating two terms of Equation (5.21). From Figure 5.5a, we see that the performance of the OPC receiver in terms of error probability in discriminating BPSK symbols is better than that of the OPA receiver. However, for a low number of modes  $M$ , OPA receivers with non-equi priors still perform better than OPC receivers with equal priors and perform similar to OPC receivers with non-equal priors. Our evaluation suggests that lower complexity receivers like OPA receivers with fewer optical components can provide superior information retrieval with a suitable choice of prior.

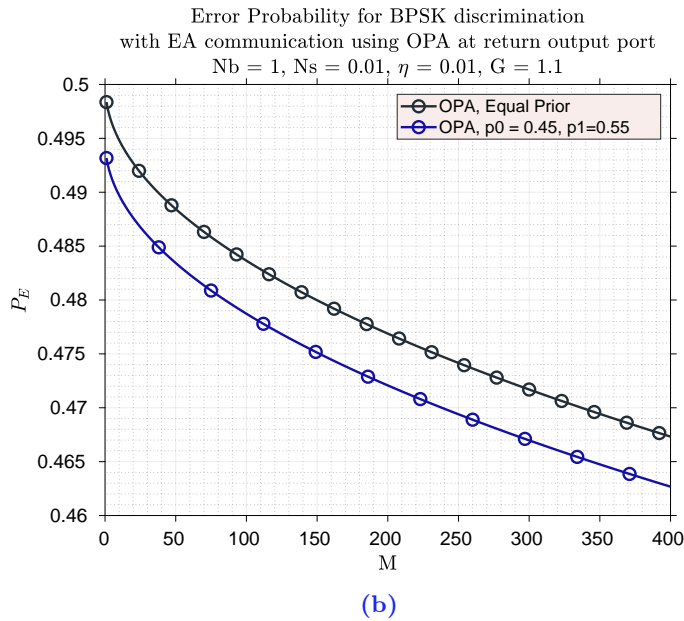
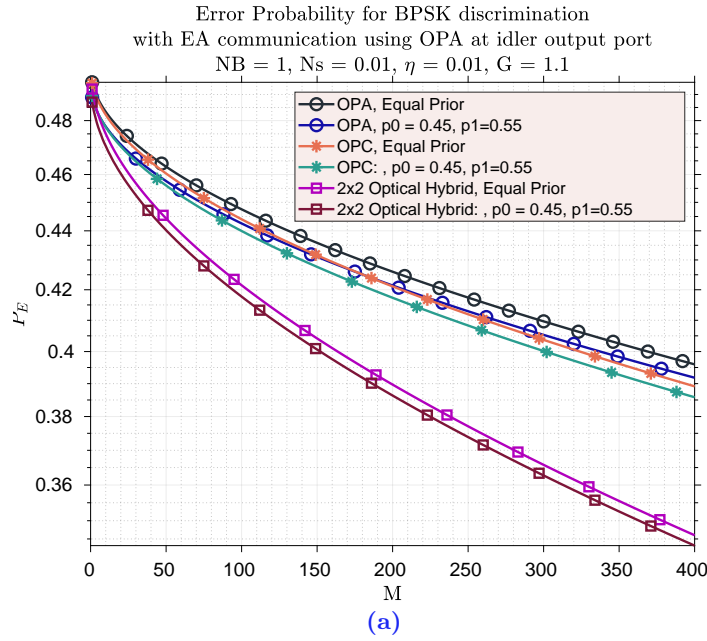
The error probability of 2x2 optical hybrid can be calculated using a formula similar to one in Equation (5.21) with mean and variance from Equations (5.15) and (5.18) respectively. From the error probability plot in Figure 5.5a, we see that the 2x2 optical hybrid offers roughly 10% improvement in terms of BPSK state discrimination as compared to OPC receiver.

#### 5.4.2 MUTUAL INFORMATION CALCULATION

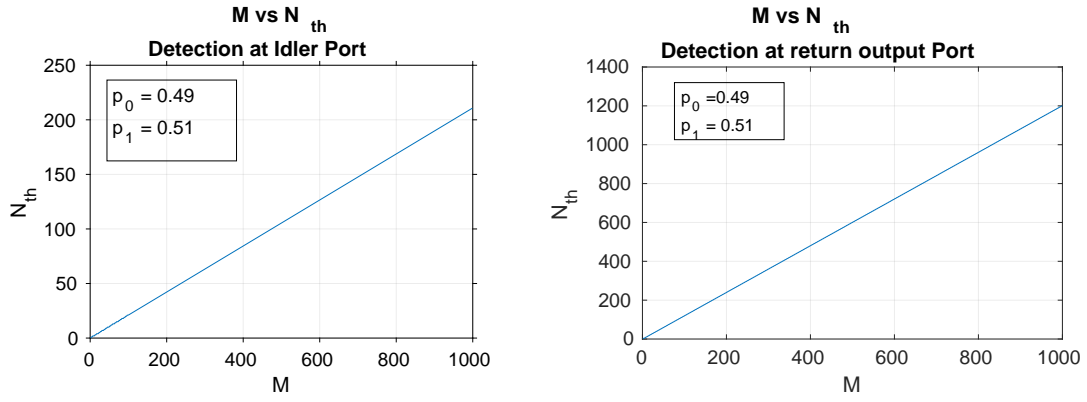
Holevo capacity (Holevo and Werner, 2001; Holevo, 2002) for classical communication that doesn't require entanglement assistance is given by

$$C = g(\eta N_s + N_B) - g(N_B) \quad (5.22)$$

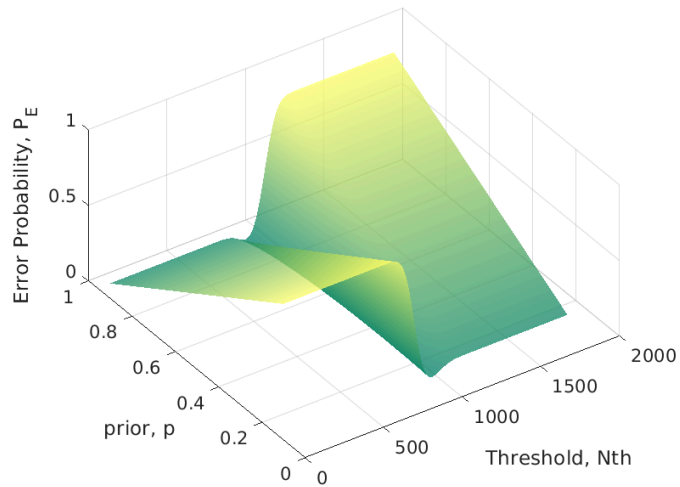
where  $g(n) = (n + 1) \log_2(n + 1) - n \log_2(n)$  is the entropy of the thermal state with mean photon number  $n$ . To write mutual information and in turn capacity for entanglement-assisted classical communication requiring symbol-by-symbol joint detection, we are required to calculate conditional probability distribution. Assume that the random variable  $X$  is used to denote the received symbols, and  $Y$  is used to denote the detected symbols. We calculate the mutual information as follows. We first calculate conditional probabilities to complete the transition matrix. Using conditional probabilities we can calculate posteriors. Posteriors are used to calculate conditional entropies followed by the calculation of mutual information. The overall set of steps is provided in Equation (5.23).



**Figure 5.5: Top:** Symbol-by-symbol (separable) minimum error-probability measurement on each return-idler mode pair at idler output port. We find that unequal priors have lower error probability as compared to BPSK symbols with equal prior. **Bottom:** Symbol-by-symbol (separable) minimum error-probability measurement on each return-idler mode pair at return output port of OPA receiver. As compared to measurement made at idler output port of the OPA receiver, error probability is higher at the return output port of the OPA receiver.



**Figure 5.6:** Optimal threshold for hypothesis testing at the output port of OPA as a function of number of modes. Higher threshold is required when detection is made at the return output port compared to the detection made at idler output port of OPA receiver.



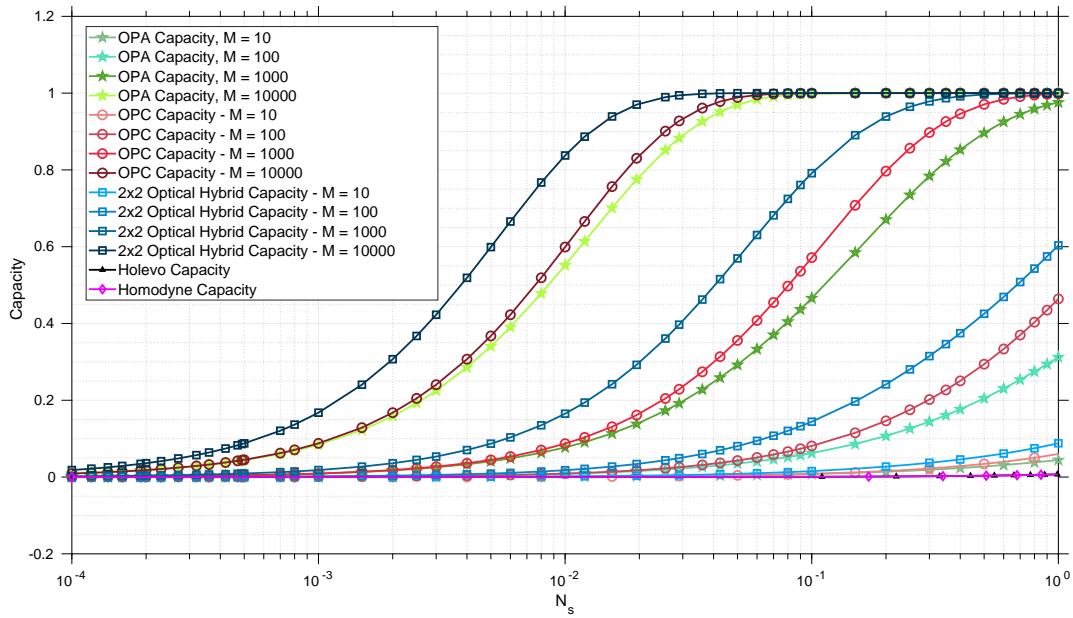
**Figure 5.7:** Surface plot of  $P_E$  as a function of prior  $p_0$  and threshold mean photon number  $N_{th}$  from Equation (5.19) for photodetection at idler output port for OPA receiver.

$$\begin{aligned}
p_{y|x}(Y = 0|X = 0) &= 1 - P_{\text{OPA}}(n < N_{\text{th}}|\theta = 0; M) \\
p_{y|x}(Y = 1|X = 1) &= P_{\text{OPA}}(n < N_{\text{th}}|\theta = \pi; M) \\
p_{y|x}(Y = 0|X = 1) &= 1 - P_{\text{OPA}}(n < N_{\text{th}}|\theta = \pi; M) \\
p_{y|x}(Y = 1|X = 0) &= P_{\text{OPA}}(n < N_{\text{th}}|\theta = 0; M) \\
p_y(Y = 0) &= p_0 p_{y|x}(Y = 0|X = 0) + p_1 p_{y|x}(Y = 0|X = 1) \\
p_y(Y = 1) &= p_0 p_{y|x}(Y = 1|X = 0) + p_1 p_{y|x}(Y = 1|X = 1) \\
H(Y|X = 0) &= -p_{y|x}(Y = 0|X = 0) \log_2(p_{y|x}(Y = 0|X = 0)) \\
&\quad - p_{y|x}(Y = 1|X = 0) \log_2(p_{y|x}(Y = 1|X = 0)) \\
H(Y|X = 1) &= -p_{y|x}(Y = 0|X = 1) \log_2(p_{y|x}(Y = 0|X = 1)) \\
&\quad - p_{y|x}(Y = 1|X = 1) \log_2(p_{y|x}(Y = 1|X = 1)) \\
H(Y|X) &= p_0 H(Y|X = 0) + p_1 H(Y|X = 1) \\
H(Y) &= -p_y(Y = 0) \log_2(p_y(Y = 0)) - p_y(Y = 1) \log_2(p_y(Y = 1)) \\
I(X; Y) &= H(Y) - H(Y|X)
\end{aligned} \tag{5.23}$$

The Shannon's capacity for transmitting classical information with our EA receivers can be calculated by taking the maximum of mutual information over prior  $p$  and threshold mean photon  $N_{\text{th}}$ , i.e.

$$C_{\text{EA}} = \max_{p, N_{\text{th}}} I(X; Y) \tag{5.24}$$

We find that symbols with equal priors maximize the mutual information, as expected. We conducted a simulation study with varying number of modes  $M$  to optimize the mutual information as a function of the signal mean photon number transmitted over noisy Bosonic channel with  $N_B = 1$  and transmittivity of Bosonic channel  $\eta = 0.01$ . In Figure 5.8, we present a comparison of the capacity of various receiver designs proposed for the BPSK constellation using Equation 5.24. At the same time, we also plot the capacity of the Homodyne receiver where an average number of photons received is  $4\eta N_s$  and the average number of noisy photons is  $2N_B + 1$ . The capacity of a Homodyne receiver is given by  $C_H = 0.5 \log_2[1 + 4\eta N_s / (2N_B + 1)]$ . As a reference, we also plot the Holevo capacity given by Equation (5.22). Note that for achieving Holevo capacity we require coherent states with Gaussian modulation. For EA communication with the BPSK constellation, we find that all three joint receivers proposed in this chapter outperform the Holevo capacity even for a number of modes as low as  $M = 10$ . From our analysis and results shown in Figure 5.8, we conclude that for the proposed EA receiver design employing a joint-detection scheme, a large number of signal-idler modes is not required. The number of modes as low as  $M = 10$  is sufficient.



**Figure 5.8:** Channel Capacity for BPSK state discrimination using different receiver schemes. We see that entanglement assistance offers advantage in terms of increasing capacity of the channel and beats the classical capacities such as Holevo capacity and Homodyne Capacity. We chose transmittivity of Bosonic channel as  $\eta = 0.01$  and mean background photon as  $N_B = 1.0$ . In our numerical study, classical capacity stays below 0.07 bits per channel use for mean signal photon  $N_s < 1.0$ .



Additionally, we also plot per mode communication rate  $R$  normalized by Holevo capacity for classical communication  $C$  in Figure 5.9 where  $R$  is given by Equation (5.25).

$$R = \frac{1 + P_e \log_2(P_e) + (1 - P_e) \log_2(1 - P_e)}{M} \quad (5.25)$$

We find that in terms of normalized communication rate, OPA and OPC receivers perform almost three times better in the photon-starved regime when BPSK symbols with non-equal priors are used compared to when BPSK symbols are equally likely. At the same time, 2x2 optical hybrid receivers for non-equal priors perform roughly 2.5 times as compared to BPSK with equal priors in a photon-starved regime. Further, compared to OPA-based receiver, 2x2 optical hybrid receiver can outperform by as much as 30% in terms of information rate.

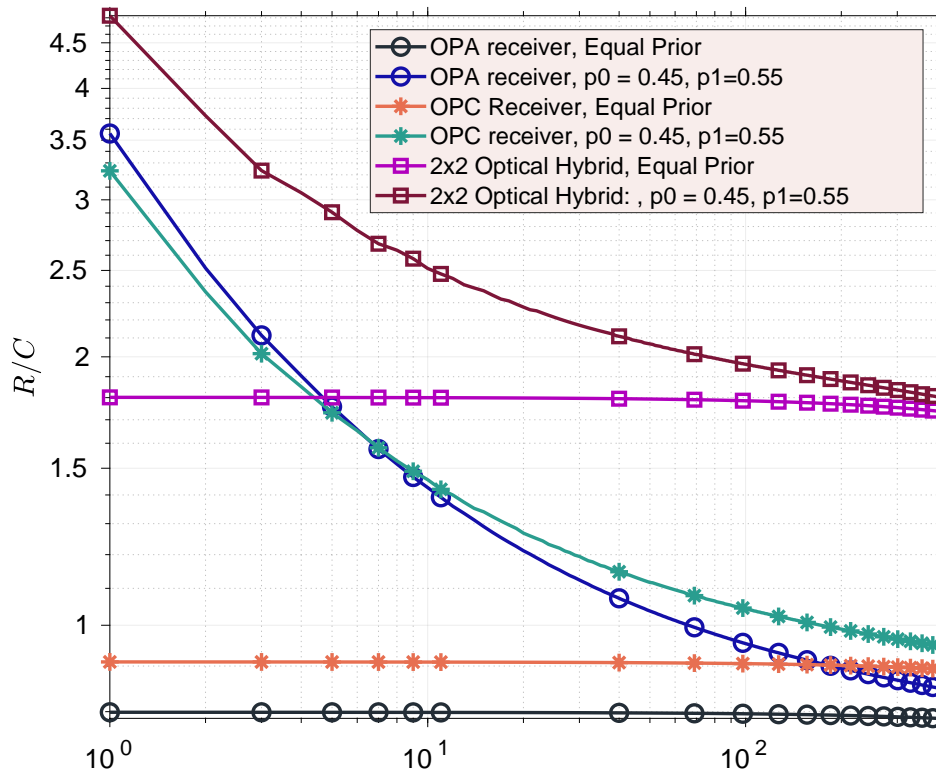


Figure 5.9: Information rate as a function of number of modes  $M$  for EA receivers.

## 5.5 DISCUSSION

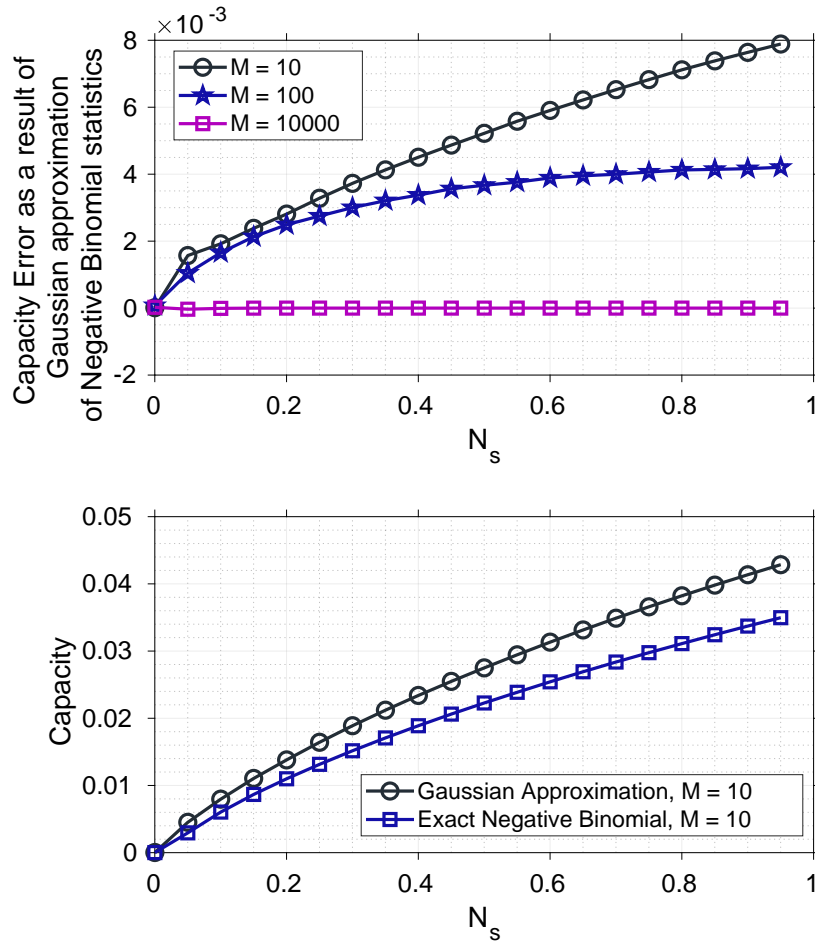
### 5.5.1 GAUSSIAN APPROXIMATION TO NEGATIVE BINOMIAL PHOTON STATISTICS

Although the photodetection statistics given by OPA receivers in Equations (5.7) is negative binomial in nature, they are computationally expensive to calculate. For a large value of  $M$ , we can approximate the statistics to be Gaussian distribution. However, we should be aware of how we may misinterpret the true performance of receivers due to approximation. In Figure, we plot the  $C_{\text{Gaussian}} - C_{\text{NB}}$ .  $C_{\text{Gaussian}}$  is the Capacity of OPA receiver discussed in Section 5.3.1 by approximating photodetection statistics as Gaussian.  $C_{\text{NB}}$  is the capacity by using exact negative binomial distribution from Equation (5.7). Based on our calculation, we make the following observations: (i) the error of approximation increases as the signal mean photon  $N_s$  increases; (ii) with Gaussian approximation, the capacity of the channel is over-estimated than its true value; (iii) as the number of modes increases, the error of approximation vanishes. Our observations are presented in Figure 5.10. Even though Gaussian approximation over-estimates the capacity, the error is in the order of  $10^{-3}$  that is small compared to the value of capacity and allows faster numerical calculation.

## 5.6 CONCLUDING REMARKS AND FUTURE WORKS

Entanglement is a unique phenomenon in quantum information science that can be leveraged to design new types of sensors allowing computing devices to solve problems that are intractable by conventional computers. In communication systems, the use of entanglement assistance offers a unique advantage in terms of providing a better communication rate in a low photon-number regime. Pre-shared entanglement can be used to surpass the performance of classical capacity and Holevo capacity in highly noisy and low-brightness conditions. However, there are several challenges in terms of practical realization of entanglement such as (i) the transmission of entanglement over long-distance; and (ii) optimum quantum receiver to achieve entanglement assisted channel capacity has not been derived yet. Nevertheless, simulation results indicate that even when entanglement is not perfect, EA communication based on signal-idler pair outperforms Holevo capacity and capacity of classical channels.

In this chapter, we analyzed several low-complexity receiver designs employing optical hybrids and balanced detectors. We demonstrated that for BPSK modulation, 2x2 optical hybrid-based joint detection can outperform the OPA and optical phase-conjugation receivers. Numerical results demonstrate that we don't need a large number of signal-idler modes to outperform Holevo and Homodyne capacity.



**Figure 5.10: Top:** Capacity error in the case of OPA receiver as a result of approximating negative binomial photodetection statistics to Gaussian. **Bottom:** Capacity of OPA receiver with the number of modes  $M = 10$ . We observe that with Gaussian approximation, we overestimates the shannon's capacity of OPA receiver for EA communication while discriminating BPSK states.



---

## CONCLUSION

---

This thesis discusses the importance of parameter choices while designing a receiver for state discrimination when information is encoded using quantum states. The approach for detection uses a semi-classical approach with on-off photo-detection made at the receiver end. The first novel result of the thesis includes optimal receiver design using coherent states. Coherent states are non-orthogonal states that are building blocks of semi-classical quantum communication as well as a precursor for fully quantum communication. Our first result tells us that receiver needs to be tuned based on the photon number regime and properties of optical elements used in the communication system. A practical extension to this work can be a realization of such receivers in practice. Our receiver design uses on-off detectors, however, photon-number resolving detectors may be used to further improve the performance of such receiver design. In addition to that, the use of non-classical ancillary states may deliver a lower probability of error than classical states (Nair et al., 2012).

In Chapter 4, we introduce squeezing as a non-Gaussian operation while encoding information with phase-shift keying modulation. However, for displacement-style receivers (e.g. Kennedy’s receiver), employing squeezing while transmitting information doesn’t provide any additional advantage since squeezing effectively increases the mean photon being transmitted. However, we see some improvement in terms of increased mutual information for the low photon number regime when squeezing is used on the receiver side. Based on our study, we hypothesize that a displacement-style receiver may not be an optimal choice when squeezing operation needs to be used. There may be some other receiver design that can perform superior as compared to displacement-style receivers.

Finally, in Chapter 5, we explored entanglement for classical communication. Pre-shared entanglement facilitates many applications such as quantum-secured communication, quantum-enhanced sensing, and quantum illumination. Pre-shared entanglement increases the reliable transmission rate of classical information and surpasses the performance of classical capacity and Holevo capacity in the noisy and low-brightness regime. Further, as compared to previous work, Chapter 5 provides low-complexity receiver designs for EA communication that are practical and easier to implement. The communication protocol in EA communication uses SPDC and beamsplitters with integrated photonics for joint detection. We show that to surpass the classical capacity, the number of modes can be as low as 10. Finally, even though optimum encoding for achieving EA channel capacity is known for decades (Holevo and Werner, 2001; Holevo, 2002), very little progress has been made in the design of optimum quantum receivers for EA communication. We have provided optimal receiver design for EA communication in this thesis but an experimental demonstration of such receiver

design is yet to be explored.

We believe that our results would pave a path to new avenues in designing receivers to improve communication performance in conditions that involve substantial loss of photons and noise such as covert sensing, deep-space communication, and non-invasive imaging. A natural extension of this paper can be exploring optimality conditions for quantum receivers which is still an open problem.

# Appendices





---

## PRELIMINARIES

---

### A.1 RANDOM VARIABLES AND RANDOM PROCESSES

A random variable (r.v.) usually denoted by capital letters say  $X$  is a variable whose value denotes the possible value of a random phenomenon. There are two types of random variables

1. **Discrete random variables:** Discrete random variables only take countable number of discrete values such as  $0, 1, 2, 3, \dots, N$ . For example, discrete random variables include the number of balls in a basket, number of players in a game, number of envelopes for letters, etc. The probability distribution of a discrete random variable is a list of probabilities associated with each of its possible values. It is also sometimes called the probability function or the probability mass function (pmf). The probability law of a discrete random variable can be described by the function defined as

$$p(x) = P(X = x) \tag{A.1.1}$$

where  $P(\bullet)$  is the probability of obtaining  $x$ . Properties of discrete random variables:

- $\sum_{k=0}^{\infty} p_k[k] = 1$
- Mean is calculated as  $\mathbb{E}[K] = \sum_{k=0}^{\infty} k p_k[k]$
- Variance is calculated as  $\mathbb{V}[K] = \sum_{k=0}^{\infty} (k - \mathbb{E}[K])^2 p_k[k]$

An important family of distribution that we are going to encounter in the context of photon and light-detection is **Poisson distribution**. A pmf of Poisson distribution is written as

$$p(k) = P(K = k) = \frac{e^{-\lambda} \lambda^k}{k!} \tag{A.1.2}$$

For Poisson distribution,  $\mathbb{E}[K] = \mathbb{V}[K] = \lambda$ .

2. **Continuous random variables:** A continuous random variable takes an infinite number of possible values. Continuous random variables are usually measurements. Examples include height, weight, the amount of sugar in orange, the time required to run a mile. A continuous random variable is not defined at specific values. Instead, it is defined over an interval of values and is represented by the area under a curve (in advanced mathematics, this is known as an integral). The probability of observing any single value is equal to 0 since the number of values that may be assumed by the

random variable is infinite. The curve function denoted by  $p(x)$  is called a probability density function or (pdf). Properties of discrete random variables:

- $\int_{-\infty}^{\infty} p_X(x)dx = 1$
- Mean is calculated as  $\mathbb{E}[X] = \int_{-\infty}^{\infty} xp_X(x)dx$
- Variance is calculated as  $\mathbb{V}[X] = \int_{-\infty}^{\infty} (x - \mathbb{E}[X])^2 p_X(x)dx$

The most common continuous random variable encountered in physical processes is gaussian random variable. A pdf of Gaussian random variable is written as:

$$p_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (\text{A.1.3})$$

For Gaussian distribution,  $\mathbb{E}[K] = \mu$  and  $\mathbb{V}[K] = \sigma^2$ .

For a rigorous treatment on random variables, interested readers may refer to [Casella and Berger \(2002\)](#).

## A.2 RANDOM PROCESSES

Random processes also known as stochastic processes helps in modeling phenomena that evolve in time in an uncertain manner, for example, the trajectory of a finite body, stock market index, oil prices, etc. In this section, we introduce a mathematical tool to develop the aptitude to understand such phenomena.

Before we move forward, we define the probability space. A *probability space* is a triplet  $(\Omega, \mathcal{F}, P)$ . The first component,  $\Omega$ , is a nonempty set. Each element  $\omega$  of  $\Omega$  is called an outcome and  $\Omega$  is called the sample space. The second component,  $\mathcal{F}$ , is a set of subsets of  $\Omega$  called events. The set of events  $\mathcal{F}$  is assumed to be a  $\sigma$ -algebra<sup>1</sup>.

### A.2.1 DEFINITION OF RANDOM PROCESSES

A random process  $X$  is an indexed collection  $X = (X_t : t \in \mathbb{T})$  of random variables, all on the same probability space  $(\Omega, \mathcal{F}, P)$ . In many applications,  $\mathbb{T}$  is a set of times. If  $\mathbb{T} = \mathbb{Z}$ , or more generally, if a set consists of integers then,  $X$  is a discrete-time random processes. If  $\mathbb{T} = \mathbb{R}$  or constitutes of an interval of  $\mathbb{R}$ , then  $X$  is considered to be a continuous-time random process. We can view random process in one of the following three ways:

1. If  $t$  is fixed, then  $X_t$  is a function of sample space  $\Omega$ .
2.  $X$  is a function of  $\mathbb{T}$  with a value of  $X_t(\omega)$ ,  $t \in \mathbb{T}$  and  $\omega \in \Omega$ .
3. For each  $\omega$  fixed with  $\omega \in \Omega$ ,  $X_t(\omega)$  is a function of  $t$ , called the sample path corresponding to  $\omega$ .

<sup>1</sup>See [Casella and Berger \(2002\)](#) for more details on  $\sigma$ -algebra.

### A.2.2 RANDOM PROCESSES DESCRIBING DISCRETE EVENTS IN CONTINUOUS TIME AND/OR SPACE

Given the independent (time) variable set  $\mathbb{T}$ , whose elements usually represent time, and the set of possible outcomes  $\mathbb{S}$ , called the state space, a random process also known as a stochastic process is defined as a collection of random variables  $\{X(t), t \in \mathbb{T}\}$  on the same probability space. Random processes can be divided into four categories depending on the continuous or discrete-nature of time variable and random variables:

1. **Discrete-time, discrete-state random processes:** Time variable and the state space both are discrete. If we assume time  $t_i$  to be an increasing sequence, then  $X(t_i)$  is a random sequence. If the process is *Markovian*, then  $X(t_i)$  is a Markov chain. Simulation techniques in stochastic chemical kinetics usually belong to this class.
2. **Continuous-time, discrete-state random processes:** In this case, the state space is discrete but time variable assumes continuous range in  $(-\infty, \infty)$ . A Markovian process with these features is called a continuous-time Markov chain.
3. **Discrete-time, continuous-state random processes:**  $X(t)$  assume a continuous range of values but time variable  $t$  is discrete.
4. **Continuous-time, continuous-state random processes:** In this case, both the state space and time variables are continuous.

In this thesis, we only focus on random processes with the discrete state (or discrete events) in continuous time (and continuous space) as photon detection is discrete even in continuous time and/or space.

Let arrival process is denoted by  $I(t)$  and counting process is denoted by  $N(t)$ .  $I(t)$  is considered to be random arrivals while  $N(t)$  is the number of occurrences before time  $t$ . Then,

$$N(t) = \int_0^t I(t)dt \quad (\text{A.2.1})$$

Pictorially it has been illustrated in A.1.

If arrival rate is  $\lambda(t)$ , then mean number of arrivals is  $N = \int_0^T \lambda(t)dt$ . For a constant arrival rate  $\lambda$ , mean number of arrivals in  $T$  time (unit) is  $N = \lambda T$ .

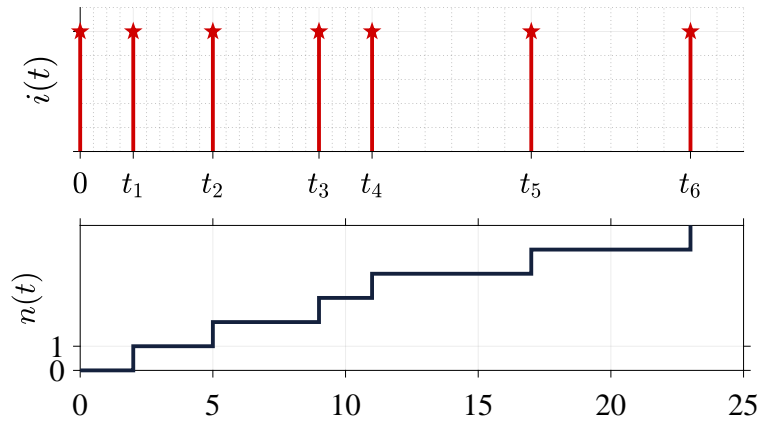


Figure A.1: Arrival and Counting Process

## BIBLIOGRAPHY

---

- D. Alsina and M. Razavi. Absolutely maximally entangled states, quantum maximum distance separable codes, and quantum repeaters. *arXiv preprint arXiv:1907.11253*, 2019. ↑ Cited on [33]
- R. Asif. Quantum secure routing for future internet. In *2020 International Conference on Information Networking (ICOIN)*, pages 121–125. IEEE, 2020. ↑ Cited on [33]
- S. J. Axler. *Linear algebra done right*, volume 2. Springer, 1997. ↑ Cited on [8]
- C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem. *IEEE Transactions on Information Theory*, 48(10):2637–2655, 2002. ↑ Cited on [67]
- R. S. Bondurant. Near-quantum optimum receivers for the phase-quadrature coherent-state channel. *Optics letters*, 18(22):1896–1898, 1993. ↑ Cited on [32]
- G. Cariolaro. *Quantum communications*. Springer, 2015. ↑ Cited on [2, 39, 40, 60]
- G. Casella and R. L. Berger. *Statistical inference*, volume 2. Duxbury Pacific Grove, CA, 2002. ↑ Cited on [92]
- A. Chefles and S. M. Barnett. Quantum state separation, unambiguous discrimination and exact cloning. *Journal of Physics A: Mathematical and General*, 31(50):10097, 1998. ↑ Cited on [40]
- A. Christ, A. Fedrizzi, H. Hübel, T. Jennewein, and C. Silberhorn. Chapter 11 - parametric down-conversion. In A. Migdall, S. V. Polyakov, J. Fan, and J. C. Bienfang, editors, *Single-Photon Generation and Detection*, volume 45 of *Experimental Methods in the Physical Sciences*, pages 351–410. Academic Press, 2013. doi: <https://doi.org/10.1016/B978-0-12-387695-9.00011-1>. URL <https://www.sciencedirect.com/science/article/pii/B9780123876959000111>. ↑ Cited on [23]
- S. Das, S. Bäuml, M. Winzewski, and K. Horodecki. Universal limitations on quantum key distribution over a network. *arXiv preprint arXiv:1912.03646*, 2019. ↑ Cited on [33]

- I. Djordjevic. Discretized Gaussian Modulation-Based Continuous Variable (CV)-QKD. In *2019 IEEE Photonics Conference (IPC)*, pages 1–2. IEEE, 2019a. [↑ Cited on \[33\]](#)
- I. B. Djordjevic. *Physical-Layer Security and Quantum Key Distribution*. Springer, 2019b. [↑ Cited on \[33\]](#)
- I. B. Djordjevic. Quantum-key distribution (qkd) fundamentals. In *Physical-Layer Security and Quantum Key Distribution*, pages 211–265. Springer, 2019c. [↑ Cited on \[18\]](#)
- I. B. Djordjevic. *Quantum Communication, Quantum Networks, and Quantum Sensing*. Elsevier/Academic Press, 2022. [↑ Cited on \[20\]](#)
- I. B. Djordjevic. Quantum receivers for entanglement assisted classical optical communications. *IEEE Photonics Journal*, 13(3):1–14, June 2021, Article ID: 7500114. doi: 10.1109/JPHOT.2021.3075881. URL [10.1109/JPHOT.2021.3075881](https://doi.org/10.1109/JPHOT.2021.3075881). [↑ Cited on \[65, 68, 75\]](#)
- J. Dolinar. A near-optimum receiver structure for the detection of m-ary optical ppm signals. *The Telecommunications and Data Acquisition Progress Report*, 42(72), 1982. [↑ Cited on \[33\]](#)
- S. J. Dolinar. *Optical communication over a non-direct path through the atmosphere*. PhD thesis, Massachusetts Institute of Technology, 1973a. [↑ Cited on \[33\]](#)
- S. J. Dolinar. An optimum receiver for the binary coherent state quantum channel. *Research Laboratory of Electronics, MIT, Quarterly Progress Report*, 11:115–120, 1973b. [↑ Cited on \[28, 33\]](#)
- S. J. Dolinar. *A class of optical receivers using optical feedback*. PhD thesis, Massachusetts Institute of Technology, 1976. [↑ Cited on \[32, 33\]](#)
- Y. C. Eldar and G. D. Forney. On quantum detection and the square-root measurement. *IEEE Transactions on Information Theory*, 47(3):858–872, 2001. [↑ Cited on \[17\]](#)
- J.-P. Gazeau. *Coherent states in quantum physics*. Wiley, 2009. [↑ Cited on \[33, 35, 37\]](#)
- C. Gerry, P. Knight, and P. L. Knight. *Introductory quantum optics*. Cambridge university press, 2005. [↑ Cited on \[2\]](#)
- V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen. Classical capacity of the lossy bosonic channel: The exact solution. *Physical Review Letters*, 92(2):027902, 2004. [↑ Cited on \[31\]](#)
- R. J. Glauber. The quantum theory of optical coherence. *Physical Review*, 130(6):2529, 1963a. [↑ Cited on \[51\]](#)
- R. J. Glauber. The quantum theory of optical coherence. *Physical Review*, 130(6):2529, 1963b. [↑ Cited on \[33\]](#)

- K. Goda, O. Miyakawa, E. E. Mikhailov, S. Saraf, R. Adhikari, K. McKenzie, R. Ward, S. Vass, A. J. Weinstein, and N. Mavalvala. A quantum-enhanced prototype gravitational-wave detector. *Nature Physics*, 4(6):472–476, 2008. [↑ Cited on \[52\]](#)
- R. K. Goodrich. A riesz representation theorem. *Proceedings of the American Mathematical Society*, 24(3):629–636, 1970. [↑ Cited on \[9\]](#)
- D. J. Griffiths and D. F. Schroeter. *Introduction to quantum mechanics*. Cambridge University Press, 2018. [↑ Cited on \[13\]](#)
- S. Guha. Receiver design to harness quantum illumination advantage. In *2009 IEEE International Symposium on Information Theory*, pages 963–967. IEEE, 2009. [↑ Cited on \[68, 70\]](#)
- W. W. Hager. Lipschitz continuity for constrained processes. *SIAM Journal on Control and Optimization*, 17(3):321–338, 1979. [↑ Cited on \[47\]](#)
- S. Hao, H. Shi, W. Li, J. H. Shapiro, Q. Zhuang, and Z. Zhang. Entanglement-assisted communication surpassing the ultimate classical capacity. *Physical Review Letters*, 126(25):250501, 2021. [↑ Cited on \[65, 67\]](#)
- P. Hausladen and W. K. Wootters. A ‘pretty good’ measurement for distinguishing quantum states. *Journal of Modern Optics*, 41(12):2385–2390, 1994. [↑ Cited on \[17\]](#)
- P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters. Classical information capacity of a quantum channel. *Physical Review A*, 54(3):1869, 1996. [↑ Cited on \[31\]](#)
- C. Helstrom and R. Kennedy. Noncommuting observables in quantum detection and estimation theory. *IEEE Transactions on Information Theory*, 20(1):16–24, 1974. [↑ Cited on \[33\]](#)
- C. W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969. [↑ Cited on \[17\]](#)
- C. W. Helstrom, J. W. Liu, and J. P. Gordon. Quantum-mechanical communication theory. *Proceedings of the IEEE*, 58(10):1578–1598, 1970. [↑ Cited on \[33\]](#)
- A. S. Holevo. On entanglement-assisted classical capacity. *Journal of Mathematical Physics*, 43(9):4326–4333, 2002. [↑ Cited on \[67, 68, 78, 87\]](#)
- A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic gaussian channels. *Physical Review A*, 63(3):032312, 2001. [↑ Cited on \[67, 78, 87\]](#)
- S. Izumi, M. Takeoka, M. Fujiwara, N. Dalla Pozza, A. Assalini, K. Ema, and M. Sasaki. Displacement receiver for phase-shift-keyed coherent states. *Physical Review A*, 86(4):042328, 2012. [↑ Cited on \[32, 38, 41, 52\]](#)

- S. Izumi, M. Takeoka, K. Ema, and M. Sasaki. Quantum receivers with squeezing and photon-number-resolving detectors for m-ary coherent state discrimination. *Physical Review A*, 87(4):042328, 2013. [↑ Cited on \[52\]](#)
- R. S. Kennedy. A near-optimum receiver for the binary coherent state quantum channel. *Quarterly Progress Report*, 108:219–225, 1973. [↑ Cited on \[25, 32, 52\]](#)
- P. Liu, Z. Pan, and J. Lei. Parameter identification of reed-solomon codes based on probability statistics and galois field fourier transform. *IEEE Access*, 7:33619–33630, 2019a. [↑ Cited on \[33\]](#)
- Q. Liu, Y. Yang, and Z. Liu. Adaptive modulation coding method based on minimum packet loss rate in aos communication system. *International Journal of Performability Engineering*, 15(4), 2019b. [↑ Cited on \[33\]](#)
- M. Loncar and M. G. Raymer. Development of quantum interconnects for next-generation information technologies. *arXiv preprint arXiv:1912.06642*, 2019. [↑ Cited on \[33\]](#)
- D. Lopez-Mago. *Implementation of a two-photon michelson interferometer for quantum optical coherence tomography*. PhD thesis, 2012. [↑ Cited on \[23\]](#)
- W. Mauerer, M. Avenhaus, W. Helwig, and C. Silberhorn. How colors influence numbers: Photon statistics of parametric down-conversion. *Physical Review A*, 80(5):053815, 2009. [↑ Cited on \[70\]](#)
- P. W. Milonni and J. H. Eberly. *Lasers physics*, 2010. [↑ Cited on \[13\]](#)
- C. R. Müller and C. Marquardt. A robust quantum receiver for phase shift keyed signals. *New Journal of Physics*, 17(3):032003, 2015. [↑ Cited on \[38, 52\]](#)
- R. Nair, B. J. Yen, S. Guha, J. H. Shapiro, and S. Pirandola. Symmetric m-ary phase discrimination using quantum-optical probe states. *Physical Review A*, 86(2):022306, 2012. [↑ Cited on \[87\]](#)
- R. Nair, S. Guha, and S.-H. Tan. Realizable receivers for discriminating coherent and multicopy quantum states near the quantum limit. *Physical Review A*, 89(3):032318, 2014. [↑ Cited on \[32\]](#)
- T. Ninacs, B. Matuz, G. Liva, and G. Colavolpe. Short non-binary low-density parity-check codes for phase noise channels. *IEEE Transactions on Communications*, 67(7):4575–4584, 2019. [↑ Cited on \[33\]](#)
- M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha. Routing entanglement in the quantum internet. *npj Quantum Information*, 5(1):1–9, 2019. [↑ Cited on \[33\]](#)



- Z. Qu and I. B. Djordjevic. High-speed free-space optical continuous variable-quantum key distribution based on kramers–kronig scheme. *IEEE Photonics Journal*, 10(6):1–7, 2018. [↑ Cited on \[33\]](#)
- M. S. Sadeghi-Zadeh, M. Houshmand, H. Aghababa, M. H. Kochakzadeh, and F. Zarmehi. Bidirectional quantum teleportation of an arbitrary number of qubits over noisy channel. *Quantum Information Processing*, 18(11):353, 2019. [↑ Cited on \[33\]](#)
- C. Shannon. The lattice theory of information. *Transactions of the IRE professional Group on Information Theory*, 1(1):105–107, 1953. [↑ Cited on \[3\]](#)
- C. E. Shannon. A mathematical theory of communication. *The Bell System Tech*, 27: 379–423, 623–656, 1948. [↑ Cited on \[31\]](#)
- H. Shi, Z. Zhang, and Q. Zhuang. Practical route to entanglement-assisted communication over noisy bosonic channels. *Physical Review Applied*, 13(3):034029, 2020. [↑ Cited on \[65, 67, 68, 72\]](#)
- P. W. Shor. Capacities of quantum channels and how to find them. *arXiv preprint quant-ph/0304102*, 2003. [↑ Cited on \[32, 40\]](#)
- B. A. Smith, L. A. Soderblom, D. Banfield, A. Basilevsky, R. Beebe, K. Bollinger, J. Boyce, A. Brahic, G. Briggs, R. Brown, et al. Voyager 2 at neptune: Imaging science results. *Science*, 246(4936):1422–1449, 1989. [↑ Cited on \[33\]](#)
- M. Takeoka and S. Guha. Capacity of optical communication in loss and noise with general quantum gaussian receivers. *Physical Review A*, 89(4):042309, 2014. [↑ Cited on \[40\]](#)
- M. Takeoka and M. Sasaki. Discrimination of the binary coherent signal: Gaussian-operation limit and simple non-gaussian near-optimal receivers. *Physical Review A*, 78(2):022320, 2008. [↑ Cited on \[19, 26, 32\]](#)
- H. Vahlbruch, S. Chelkowski, B. Hage, A. Franzen, K. Danzmann, and R. Schnabel. Demonstration of a squeezed-light-enhanced power-and signal-recycled michelson interferometer. *Physical review letters*, 95(21):211102, 2005. [↑ Cited on \[52\]](#)
- V. Vilnrotter and C. Lau. Quantum detection theory for the free-space channel. *The InterPlanetary Network Progress Report 42-146, April–June 2001*, pages 1–34, 2001. [↑ Cited on \[33\]](#)
- V. Vilnrotter and E. Rodemich. A generalization of the near-optimum binary coherent state receiver concept (corresp.). *IEEE transactions on information theory*, 30(2):446–450, 1984. [↑ Cited on \[32\]](#)
- R. Yuan, M. Zhao, S. Han, and J. Cheng. Kennedy receiver using threshold detection and optimized displacement under thermal noise. *IEEE Communications Letters*, 2020. [↑ Cited on \[32\]](#)

- H. Yuen, R. Kennedy, and M. Lax. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Transactions on Information Theory*, 21(2):125–134, 1975. [↑ Cited on \[33\]](#)
- H. P. Yuen. Two-photon coherent states of the radiation field. *Physical Review A*, 13(6):2226, 1976. [↑ Cited on \[51\]](#)
- Z. Zhang, S. Mouradian, F. N. Wong, and J. H. Shapiro. Entanglement-enhanced sensing in a lossy and noisy environment. *Physical review letters*, 114(11):110506, 2015. [↑ Cited on \[67\]](#)
- Q. Zhuang. Quantum ranging with gaussian entanglement. *arXiv preprint arXiv:2103.11054*, 2021. [↑ Cited on \[67, 68\]](#)