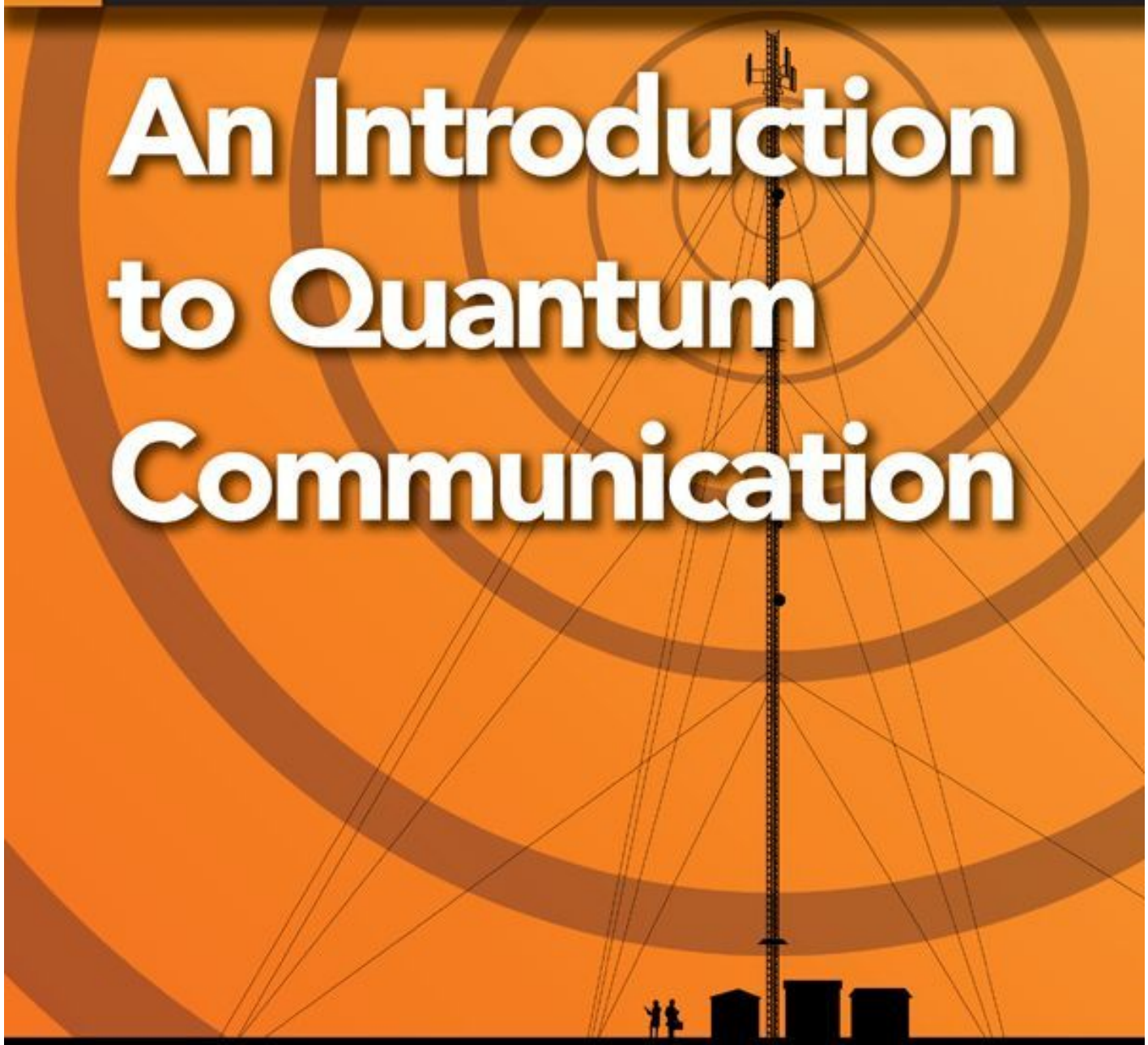
COMMUNICATIONS AND SIGNAL PROCESSING COLLECTION

Orlando R. Baiocchi, Ph.D., *Collection Editor*

An Introduction to Quantum Communication



Vinod K. Mishra

MOMENTUM PRESS
ENGINEERING

AN INTRODUCTION TO QUANTUM COMMUNICATION

AN INTRODUCTION TO QUANTUM COMMUNICATION

VINOD K. MISHRA

An Introduction to Quantum Communication

First published in 2016 by
Momentum Press, LLC
222 East 46th Street, New York, NY 10017
www.momentumpress.net

ISBN-13:978-1-60650-556-4 (print)
ISBN-13:978-1-60650-557-1 (e-book)

Momentum Press Communications and Signal Processing Collection

Cover and interior design by S4Carlisle Publishing Service Private Ltd.
Chennai, India

10 9 8 7 6 5 4 3 2 1

DEDICATION

I dedicate this book to the sacred memory of my parents and teachers, to my wife Kamala, and to my curious daughters Meenoo, Aparajita, and Ankita.

ABSTRACT

Quantum mechanics is the most successful theory for describing the microworld of photons, atoms, and their aggregates. It is behind much of the successes of modern technology. It has deep philosophical implications to the fundamental nature of material reality. A few decades ago, it was also realized that it is connected to the computer science and information theory. With this understanding were born the new disciplines of quantum computing and quantum communication.

The current book introduces the very exciting area of quantum communication, which lies at the intersection of quantum mechanics, information theory, and atomic physics. The relevant concepts of these disciplines are explained, and their implication for the task of unbreakably secure communication is elucidated. The mathematical formulation of various approaches has been explained. An attempt has been made to keep the exposition self-contained. A senior undergraduate with good mathematics and physics background should be able to follow the current thinking about these issues after understanding the material presented in this book.

KEYWORDS

Information Theory, Quantum Mechanics, Shannon Entropy, Quantum Coding, Entanglement, Quantum Information

CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENT

I deeply thank Dr. Ashok Goel for being the impetus behind writing this book and Dr. Kurt Jacobs for going through the manuscript.

CHAPTER 1

WHY QUANTUM COMMUNICATION?

Communication in the form of written and spoken languages is a hallmark of human societies. Even lower life-forms and nonliving entities communicate non-linguistically. The basic building blocks of matter consist of quarks and leptons, and they communicate by exchanging the force quanta of gluons and photons respectively. Among the living entities, cells communicate via biochemical molecules. Languages are the most important communication tools on which our distinctive human societies are based. They also include nonverbal varieties like sign languages, semaphores, etc.

Still when we speak of communication in the context of technology, we actually mean telecommunication. It started with telegraphs based on Morse code, progressed through radio and wireless, and finally transformed into the Internet. Technically, communication involves transmission and reception of messages using electromagnetic waves in free space, photonic pulses in optical fiber, or currents in copper wires. Several of their attributes like currents, voltages, amplitudes, frequencies, etc., are used for carrying messages of importance to both machines and humans.

1.1 CLASSICAL COMMUNICATION AND ITS LIMITS

Efforts to develop a theoretical understanding of telecommunications started quite early. A very important problem was to determine the maximum amount of information that could be sent over an information channel in presence of noise. It took the genius of Claude Shannon (Shannon 1948) to solve this problem, and as a result, launch Information Theory as a distinct area of knowledge. He has earned the distinction of being “the Einstein of communication.” Before Shannon, the definition of information applicable to telecommunication was very qualitative. He made

it more precise and quantitative using Boolean algebra and basic thermodynamic principles.

CONCEPT OF PROBABILITY DISTRIBUTION

Let us assume that there is a discrete random process in which the basic event takes a finite number of values. Tossing a coin, where there are only two outcomes of either heads or tails, exemplifies such a process. The probability of obtaining k successes (heads for our example) out of n tosses is the binomial coefficient,

$$B(n,k) = \frac{n!}{k!(n-k)!} \tag{1.1}$$

This is also known as Bernoulli process. For $n \rightarrow \infty$, Sterling's asymptotic formula for factorials can be used to show that this process gives rise to a Gaussian distribution. In this limit the discrete variables (n, k) change into a continuous variable denoted by x.

INFORMATION OR SHANNON ENTROPY

We associate a probability $p(x)$ ($0 \leq p(x) \leq 1$) for a random variable x($0 \leq x \leq \infty$). Shannon defined information content of a random variable as a "surprise" function. It is a measure of how surprised we will be to find that a random variable has value x. It is defined as:

$$h[p(x)] = \log \frac{1}{p(x)} = -\log p(x). \tag{1.2}$$

The logarithm can be in any base depending on the number of distinct and discrete values x can take. The base is 2 for the process of coin tossing. Then the Shannon entropy or information entropy is defined as the average value of the surprise function,

$$H[X] = E[h(X)] = -\sum_{x} p(x) \log p(x). \tag{1.3}$$

The notation E [.] denotes an estimated value,which is similar to the mean value. H [X] is a measure of "disorder" in the random process $p(x)$, and the summation is over all of its possible values. For a binary random variable (head or tail in the coin example), the summation is over probability p and it's complimentary $(1–p)$. This is analogous to a digital value taking value 0 or 1. Then the Shannon entropy is:

$$H[X] = E[h(X)] = -p \log p - (1-p)\log(1-p). \qquad (1.4)$$

Here, the logarithm is taken to the base 2, and this entropy is measured in the units of "bits." The word *bit* is a shortened form of binary digit. This function has mathematical properties expected from an entropy-like function well-known in Statistical Mechanics.

SHANNON-HARTLEY THEOREM

A given information channel is a physical medium through which information travels from source to destination in presence of noise. Capacity C (in Hz or bits/s) of such a channel is defined as the maximum rate at which this information can be transmitted. Let us assume the following about this channel.

- B = Bandwidth of the channel (in Hz or bits/s)
- The channel noise is Additive White Gaussian Noise (AWGN)
- S/N = Signal (S) to noise (N) ratio (SNR), where S and N are signal and noise powers (in Watts or Volts^2) respectively

The Shannon-Hartley theorem then states that

$$C = B\log_2\left(1+\frac{S}{N}\right) \qquad (1.5)$$

Usually SNR is given in decibels (dB) so a conversion is required between the two units. For example, if SNR is given as X dB then ratio is $10^{X/10}$. This theorem is one of the most fundamental results of information theory and has many applications is both communication and data storage technologies. For a given bandwidth B and signal-to-noise ratio S/N, a way

to transmit data with arbitrarily low BER can always be found as long as R < C. Similarly for R > C, it will be very hard to achieve lower BER.

To rewrite this theorem in an alternative and useful form, let us assume the following.

- E_b = Energy in a bit (in Joules/bit)
- $N_0/2$ = 2-sided AWG Noise Power Spectral Density (in Watts/Hz)

Then, for data rate R, we have $N = BN_0$ and $S = RE_b$[v2] andso we get:

$$\frac{R}{B} \leq \log_2\left(1+\frac{E_b R}{N_0 B}\right). \tag{1.6}$$

The combination R/B is called bandwidth efficiency (in bits/sec/Hz) and E_b/N_0 is the normalized average energy per bit (in sec.Hz/bit). After some algebra, the above expression can be rewritten as the following:

$$\left(\frac{E_b}{N_0}\right)_{\min} \geq \frac{2^{R/B}-1}{R/B}. \tag{1.7}$$

This gives the minimum possible normalized average energy per bit satisfying Shannon-Hartley theorem.

NOISY-CHANNEL CODING THEOREM

Given a noisy channel, we are interested in the efficiency of error-correcting methods in overcoming the channel capacity limitations due to the noise. Let us assume that information is transmitted at a rate R. There are two possibilities.

- $R < C$: This is the usual situation. Then this theorem states that there exist error correcting codes such that the probability of error at the receiver, or equivalently the difference $C - R$, can be made arbitrarily small. The theorem only proves the existence of such codes and does not give a way to find them. Finding such codes is an important endeavor of Applied Mathematics. At present time, some of the known

codes like Reed-Solomon codes, Low Density Parity Check (LDPC) codes, and Turbo codes come arbitrarily close to the Shannon capacity limit.

- $R > C$: In this case, error will increase; so increasing R beyond C does not serve any useful purpose.
- $R = C$: The theorem does not address this possibility.

LIMITS OF CLASSICAL COMMUNICATION

In theoretical terms, Shannon-Hartley theorem says that for greater capacity, one needs appropriately large bandwidth and SNR. The limits arise because of the capabilities of the physical layer.The physical medium with the highest capacity right now is optical fiber, with 100 Gbps rate common and 400 Gbps demonstrated in lab settings. Noise in optical fiber channels is the result of many complex physical processes and they become increasingly dominant at higher data rates. But, many clever signal coding and modulation techniques have been developed to overcome the capacity loss due to noise. Real limitations come from the transmitter and receiver architectures and their underlying operating physical principles, e.g., lasers, amplifiers, etc.

There are other characteristics of communication like reliability, security, energy efficiency, and others, which are based on non-physical layer considerations. Questions about optimal network architectures and protocols need to be answered to solve these problems.

1.2 ROLE OF QUANTUM COMMUNICATION

Classical communication is based on the properties of electromagnetic waves like frequency, phase, and polarization, which do not involve considerations of Quantum Mechanics. The achievable error-free rate for transmission of digital information is given by Shannon's theorem. So improvements consist in discovering better error-correction codes and higher information processing techniques. In principle, ever-increasing higher-speed communication is limited mainly by advances in computer processing and communication devices.

Security is another aspect of communication that is as important as speed and in some contexts more so. Many cryptography schemes and protocols

have been devised over the years but none is totally secure.

Interest in utilizing quantum phenomena for communication came after it was realized that quantum communication was immune to tampering and eavesdropping. A new area of science called quantum cryptography was born after quantum mechanical principles were applied to communication. We will go into more details about these developments in the rest of the book.

CHAPTER 2

PHYSICAL BASIS OF QUANTUM COMMUNICATION

The quantum communication depends on the basic physical principles of Quantum Mechanics (QM). The QM arose from the need to explain some very unusual results in classical physics like black-body radiation, spectral emission lines, photoelectric effect, etc., in the early 20th century. Results of experiments done with atoms and light could not be explained using ideas of classical physics. For understanding them, some revolutionary and radical ideas like notion of "Quantum" and Special Theory of Relativity (STR) were introduced. The final synthesis of these approaches during the 1920–1930 time period by Albert Einstein, Erwin Schrödinger, Paul Dirac, Enrico Fermi, Wolfgang Pauli, Satyendra Nath Bose, and others created an edifice of new physics called Quantum Mechanics.

In this chapter we will describe essential QM and explain some experimental facts and concepts needed for understanding Quantum Communication (QC).

2.1 BASIC QUANTUM MECHANICS FOR QC

QM operates in the micro-world of atoms and photons. Atoms have electrons and a nucleus, though the latter will be ignored here. Light is a stream of photons. Photons are the particles associated with the electromagnetic waves. The formalism of QM requires some new concepts described below.

WAVE FUNCTION

Wave function describes the quantum state of an object. Consider it similar to the notion the position of a particle in the classical physics. For example, the quantum state of a harmonic oscillator in its ground state is given as

$$\psi_0(x) = \left(\frac{m\omega}{\pi h}\right)^{1/4} \exp\left(-\frac{m\omega}{2h}x^2\right). \qquad (2.1)$$

Here, the subscript *0* denotes the ground state. The object under discussion (in this case, a harmonic oscillator) can also assume higher state wave functions, in which case the mathematical expression will be different. In general,the wave function is a complex object with both real and imaginary parts.

SCHRÖDINGER'S EQUATION

The wave function obeys an equation called Schrödinger's equation (SE), named after its discoverer Erwin Schrödinger, one of the early pioneers of QM. The wave function $\Psi(x)$ of a particle with mass m moving in a potential energy $V(x)$ obeys the time-independent SE,

$$\left[-\frac{\hbar^2}{2m}\frac{d^2}{dx^2} + V(x)\right]\Psi(x) = E\Psi(x). \qquad (2.2)$$

Here, $\hbar$ is Planck's constant h divided by 2π. In general, there are many solutions of this equation and each eigenvalue E_n has a corresponding eigenfunction $\Psi_n(x)$ and for corresponding "eigenvalues". For harmonic oscillators, Hydrogen atom, and few other cases, the solutions are known in analytic form, but in general one has to resort to numerical techniques.

There is also a time-dependent SE given by:

$$\left[-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x)\right]\Psi(x,t) = i\hbar\frac{\partial\Psi(x,t)}{\partial t}. \qquad (2.3)$$

This equation describes the time evolution of the wave function.

BRA AND KET

Dirac introduced a convenient notation to represent general wave functions. A wavefunction is denoted by a *ket* written as $|\Psi>$. Any reference to the underlying argument is not written. Its complex transpose is called a *bra* and is denoted by $<\Psi|$. The two words together remind one of another word *bracket*, which is the origin of this notation.

PROBABILITY FUNCTION:

The wave function is amplitude and not a directly observed physical entity. Its absolute square is the probability of finding the associated particle at any given space-time point,

$$P(x) = \Psi^{*}(\mathrm{x})\Psi(\mathrm{x}) = |\Psi(\mathrm{x})|^{2}. \qquad (2.4)$$

SUPERPOSITION PRINCIPLE

If a quantum entity has many allowed states, then the superposition principle states that it will exist in a state which is an arbitrary combination of all those states. The amount by which the general state has a given allowed state is specified by a complex number. As an example, a qubit is a quantum system and it has two logical states denoted by $|0>$ and $|1>$. It should be remembered that these logical states can be realized in many different physical systems of qubits. Then the superposition principle (SP) implies that it will be in a general state given by their linear combination as:

$$|\Psi> = c_0|0> + c_1|1>. \qquad (2.5)$$

Here the complex numbers c_0 and c_1 denote the "amount" of the allowed states contained in the general state. The absolute squares of these coefficients are interpreted as probabilities, so there is a relation among them,

$$|c_0|^2 + |c_1|^2 = 1. \qquad (2.6)$$

A measurement of a physical property in the general state projects one of the basic states, and it is known as the “collapse of wave function”. The SP follows from the fact that Schrödinger’s equation is a linear one and a superposition of its solutions is also a solution. The above discussion can also be extended to any number of allowed states.

2.2 EINSTEIN–PODOLSKY–ROSEN PARADOX

Albert Einstein, one of the towering figures of theoretical physics was very uncomfortable with the non-classical nature of quantum mechanics. Together with Boris Podolsky and Nathan Rosen (all three together known as EPR), he demonstrated in a famous 1935 paper [1] that QM is incomplete. They described a thought (“gedanken”) experiment on two correlated particles in which a measurement is performed on one particle. Due to quantum correlations, the property of the second particle can be inferred without any measurement on it. Assuming that the first measurement has no influence on the second, it implies an instantaneous “spooky action at a distance”. This is not allowed in classical mechanics since the maximum speed of any inter-particle communication is limited by the finite speed of light and cannot be infinite. Based on this analysis, the EPR paper claimed that QM is incomplete and it was lacking an “element of reality” in its basic structure, and there are “hidden variables” (HV) which QM was ignoring. Afterwards, a discussion started among physicists, philosophers, and mathematicians about the true meaning of EPR paper without any resolution.

In 1964, John Bell [2] proposed experiments to distinguish between QM and so-called hidden variable theories. According to these experiments, HV theories and QM led to different predictions. Since then, many such experiments [3] have been performed and they all vindicate QM. HV theories are understood as not describing the reality and the debate has centered on the correct interpretation of QM in light of these experiments.

The basic EPR thought experiment used continuous variables like position and momentum. The experiments become easier if discrete variables like spin and polarizations are used.This choice does not affect the outcome. The quantum states used in this analysis have come to be known as *entangled state*. The property of *entanglement*, which was seen as

showing the deficiencies of QM, has now become the foundation on which the discipline of quantum information science rests.

The analysis presented by Bell involved discrete quantum variable spin in contrast to continuous variables like position and momentum used by EPR.

Bell's experiment starts with preparation of two electrons in a state having total spin zero (so called "singlet" state),

$$|\psi>_{singlet} = \frac{1}{\sqrt{2}}\left[|\uparrow>_A|\downarrow>_B - |\downarrow>_A|\uparrow>_B\right]. \qquad (2.7)$$

Let one electron fly to Alice and the other to Bob, who is in opposite direction at the same distance. Both Alice and Bob have set their polarization analyzers to random angles for measuring the spin direction of the received particle.

A statistical quantity called correlation (C) is calculated from the measurements made by Alice and Bob. It is defined as two times the probability of equal outcomes after measurements of the spin values minus one.

For some polarizer angles, the correlations are easy to calculate.

(i) Anti-parallel
(the relative angle between Alice and Bob's polarizer angles is 180°):

$$C(180^\circ) = 1 \qquad (2.8)$$

(ii) Parallel (the relative
angle between Alice and Bob's polarizer angles is 0°):

$$C(0^\circ) = -1 \qquad (2.9)$$

(iii) Orthogonal (the relative angle between
Alice and Bob's polarizer angles is 90°):

$$C(90^\circ) = 0 \qquad (2.10)$$

For intermediate angles θ, there are two predictions:

(i) If quantum mechanics is correct, then $C(\theta) = -\cos\theta$.
(ii) If there are hidden variables, then $C(\theta)$ is proportional to θ.

All the experiments done so far are consistent with quantum mechanics. It implies that local hidden variable theories as advocated by EPR and others is an incomplete description of reality at the fundamental level. Even after the experimental vindication of quantum mechanics, the debate over the philosophical meaning of locality and causality implied by it,continues.

2.3 SOME INEQUALITIES

Bell's ideas are mathematically presented in terms of some inequalities.

(i) Bell's Inequality:

Let there be three variables a,b, and c which can take either one of the two allowed discrete values, for example, up or down spins. Then Bell's inequality states that:

$$C(a,c) - C(b,a) - C(b,c) \leq 1. \qquad (2.11)$$

It holds true for local hidden variable theories but is violated by quantum mechanics. All the experiments show that this inequality is violated.

(ii) CHSH (Clauser–Horne–Shimony–Holt) Inequality:

It is another form of Bell's inequality more suitable for experiments. Let Alice measure random variables *a, a'* and Bob measure *b* and *b'*. All of the variables take either one of the two allowed values. Then the CHSH inequality is a relation among the correlations given by:

$$-2 \leq C(a,b) - C(a,b') + C(a',b) + C(a',b'). \qquad (2.12)$$

Again it is violated by quantum mechanics.

2.4 IDEA OF ENTANGLEMENT

Let us start with a 2-qubit state given as:

$$|\psi> = \frac{1}{\sqrt{2}}\left[|0>_A|0>_B + |1>_A|1>_B\right]. \qquad (2.13)$$

Here, |0> and |1> refer to a photon in horizontally and vertically polarized states and subscripts *A* and *B* refer to separate particles respectively.This state has an interesting property that it cannot be expressed as a product state of two single photon states. Such a state is called *entangled state* after Erwin Schrödinger, who coined the phrase ("verschräkung" or entanglement in German). The state above is one of four similar ones called Bell states and they are maximally entangled states for two qubits.

These and other entangled states have the property that the measurement of the first photon's polarization will allow one to infer the second photon's polarization without measuring it. Einstein did not like it as it implied instantaneous communication of some kind between the two photons. This violates the special theory of relativity according to which any the velocity of any signal cannot exceed the velocity of light. Later experiments on qubit systems have proved that quantum mechanics describes the system correctly.

2.5 QUANTUM ZENO EFFECT

A property which distinguishes quantum systems from their classical counterpart is the collapse of wave function on measurement. The act of measuring a quantum particle brings it to one of its eigenstates.

It was discovered [3] that it is possible to prevent this collapse by very fast continuous measurement. This effect has been named quantum Zeno effect (QZE) after the famous Greek philosopher of antiquity. Zeno had argued that logically, motion cannot take place because in order for an object to reach its destination, it has to reach the midpoint, and the midpoint of the distance to the midpoint, and so on. This results in an infinite series and thus movement cannot be possible. This is also known as Zeno's

paradox and was not resolved to satisfaction till the advent of the theory of infinite sequences and series.

The original scope of QZE has been enlarged so that apart from fast measurement, environmental factors, stochastic fields, etc., have also been found to inhibit the time evolution of a quantum state. The practical uses of QZE have been found in atomic magnetometer and optical networking.

2.6 DECOHERENCE

Let us start with a pure quantum state. However hard one tries, the state cannot be made totally isolated from the surrounding environment. Due to this interaction between the quantum state and the environment, the purity of the original state will be diluted. Very soon, the state will evolve in a mixed state or a superposition of many pure states, ultimately assuming a classical character. This phenomena is called *quantum decoherence*.

The interaction between a quantum state and the surrounding environment can be modeled by a heat bath. As time progresses, the quantum state subsystems evolve in such a manner that starting phase relations among them are lost. The temporally evolved subsystems cannot be put together to reproduce the original relationship among the relative phases of the system components. So the original coherence, that is, the phase relation among subsystems, is lost and the system becomes more classical and less quantum.

Quantum decoherence has a negative effect on the persistence of "quantumness" of a system and leads to a loss of starting information of the quantum state. Vigorous research effort is needed to solve this problem for realizing the promises of quantum communication and computing.

2.7 PROPAGATION OF LIGHT IN AN OPTICAL FIBER

In optical fibers, light pulses are encoded to carry information using some scheme and travel through the fiber to the receiver where they are decoded.

Optical fiber can be thought of as a long cylinder in which a glass core is surrounded by a glass shell of lower refractive index. The inner and outer regions are called core and cladding respectively. The light propagating through this medium consists of many modes of electromagnetic waves

propagating simultaneously. These modes are associated with different energies and can be arranged as atomic energy levels. Each mode is associated with a definite fiber diameter needed for it to propagate. In general, higher energy modes need larger diameters.

The total number of modes a given fiber can support depends on its diameter. Practically speaking, there are two versions in use:

(i) Single Mode Fiber (SMF) supports a single mode. The core diameter is typically 8–12 μm (microns) and the total diameter is about 125 μm.

(ii) Multimode Fiber (MMF) supports many modes. The core diameter is typically 50–200 μm and the total diameter is about 125–400 μm.

The qubits in optical fiber consist of a single mode of light as a pulse but with horizontal and vertical polarizations moving simultaneously. The propagation is described using Helmholtz equation for electric and magnetic fields $\vec{E}$ and $\vec{H}$ respectively) as a function of position vector,

$$\left[\nabla^2 + k^2\right]\begin{bmatrix}\vec{E}\\ \vec{H}\end{bmatrix}(\vec{r}) = 0. \qquad (2.14)$$

Here, k^2 is the square of the momentum vector, which depends on the light wave frequency and material properties of the glass. Solutions of this equation are called modes. Helmholtz equation is derivable from Maxwell's equations. For practical purposes, the lowest modes, known as transverse electric (TE) and transverse magnetic (TM), are used. SMF can accommodate a single mode and MMF more than one.

The light pulses for quantum communication are usually transformed into qubits by utilizing the two orthogonal polarization modes simultaneously. Their qubit properties can be lost very soon due to physical processes like birefringence and polarization mode dispersion (PMD). Many experimental techniques have been developed to counter them. Modeling and simulation using numerical calculations are tools used to predict the physical behavior of optical pulses in presence of these linear and nonlinear effects.

CHAPTER 3

INFORMATION THEORY FOR QUANTUM COMMUNICATION

In this chapter, we will describe some results from information theory (Stone 2015) useful for quantum communication (QC). Information theory is a branch of mathematics concerning the mathematical foundations of computing and communication. Shannon's theorem for classical communication is one example of such an approach. Similar results for QC are not a straightforward generalization of this theorem as many subtleties are involved. Finding answers to some of the questions regarding QC are still under intensive investigation.

3.1 MATHEMATICAL REPRESENTATION OF A SINGLE QUBIT

The points on the Poincaré sphere has been used to represent classical polarization states but it can be adapted to also represent a general qubit.

The general qubit can be represented by

$$|\psi>= sin\frac{\theta}{2}|0>+e^{i\phi}cos\frac{\theta}{2}|1>. \qquad (3.1)$$

Here, (θ, ϕ) denote the angular coordinates of the qubit state, and the complex coefficients are such that the sum of their squares represented by the length of the qubit state vector equals unity. The different angular values denote many qubits in common use,

(i) ($\theta = \phi = 0$) and ($\theta = 180°$, $\phi = 0$) points denote horizontal and vertical polarizations respectively. They form two orthogonal basis states for a qubit.

(ii) ($\theta = \phi = \pi/2$) and $(\theta = \frac{\pi}{2}, \phi = 3\pi/2)$ points denote left and right polarizations |L> and |R> respectively.

(iii) Any point on the sphere is a pure qubit.

(iv) Any point inside the sphere is a mixed qubit and its radial length is less than unity.

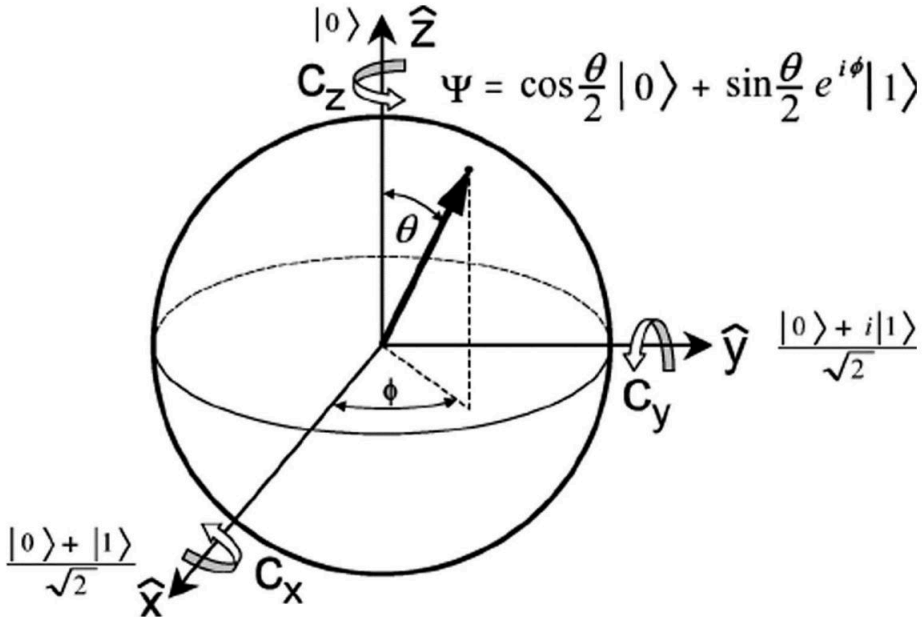


Figure 3.1. The spherical representation of a qubit (source: www.research-gate.net/figure/228581169_fig2_FIG-2-Bloch-sphere-representation-of-the-qubit-state-Control-vector-c-c-x-c-y). The surface points represent pure states and interior points represent mixed states.

3.2 ENTROPIES FOR INFORMATION

The concept of entropy originated in classical thermodynamics and it measures the disorder in a system. It is denoted by S and is defined as:

$$S = k \log W. \qquad (3.2)$$

The overall state or "macrostate" of a system is characterized by the values of some thermodynamic variables, for example, pressure,

temperature, etc. This macrostate can be generated by many "microstates", or the configurations of system components. The number of microstates for a given macrostate is denoted by *W*.

Entropy has many unique properties, like it will always increase if the system changes. After its initial discovery by Ludwig Boltzmann, it has been generalized to various other fields of inquiry like cosmology, economics, social sciences, etc. Some classical and quantum versions of this concept being used currently are described below.

VON NEUMANN ENTROPY

The von Neumann entropy is its quantum version and is defined by:

$$H(X) = -Tr(\rho ln \rho). \tag{3.3}$$

Here, ρ is the density matrix.

SHANNON ENTROPY

It is the version of entropy concept applied to classical information and is very similar to von Neumann entropy.

Let us start by measuring the value of a random variable. Then the Shannon entropy can be interpreted in two ways.Before measurement, it measures the amount of uncertainty about the value of the random variable.After measurement, it measures the amount of information that was gained.The Shannon entropy for a random variable X taking values x is defined as

$$H_S(X) = -\sum_x p(x) log_2 p(x). \tag{3.4}$$

RENYI ENTROPY

Alfred Renyi (*1961*) generalized the Shannon definition of information entropy. He searched for the most general case compatible with axioms of probability and applicable to information. For a discrete random variable $X = \{x_1, x_2, \ldots, x_N\}$ with different probabilities $\{p_1, p_2, \ldots, p_N\}$, the Renyi entropy is defined as:

$$H_\alpha(X) = \frac{1}{1-\alpha} log_2 \left(\sum_{k=1}^{N} p_k^\alpha \right), \tag{3.5}$$

for $\alpha > 0$, $\alpha \neq 1$. Shannon entropy is its special case in the $\boldsymbol{\alpha \to 1}$ limit,

$$H_1(X) = H_S(X). \tag{3.6}$$

COLLISION ENTROPY

The $\alpha = 2$ value of Renyi entropy is known also as collision entropy and has been used extensively in many areas of science. It is given by:

$$H_2(X) = -log_2 \left(\sum_{k=1}^{N} p_k^2 \right). \tag{3.7}$$

MIN-ENTROPY

The $\boldsymbol{\alpha \to \infty}$ value of Renyi entropy is known also as min-entropy. It is the smallest entropy measure out of all Renyi entropies, given by:

$$H_\infty(X) = -log_2 \max p_i. \tag{3.8}$$

TSALLIS ENTROPY

It is a generalization of Boltzmann-Gibbs entropy given earlier. For a parameter *q* also called entropic index, it is defines as:

$$S_q = \frac{1}{q-1} \left(1 - \sum_i p_i^q \right). \tag{3.9}$$

In the limit $\boldsymbol{q \to 1}$, it gives the usual Boltzmann-Gibbs entropy. For continuous probability distribution *p(x)*, it takes the following form:

$$S_q = \frac{1}{q-1}\left(1 - \int((p(x))^q\, dx\right). \qquad (3.10)$$

SHARMA-MITTAL ENTROPY

It unifies both thermodynamic and information entropies in a single expression by using two parameters.

$$S_{\alpha\beta} = \frac{1}{1-\beta}\left(\left(\int(p(x)^\alpha\, dx\right)^{\frac{1-\beta}{1-\alpha}} - 1\right), \alpha > 0, \alpha \neq 1, \beta \neq 1 \qquad (3.11)$$

This expression has the following limits: (i) $\boldsymbol{\beta \rightarrow 1}$ gives Renyi entropy, (ii) $\boldsymbol{\beta \rightarrow \alpha}$, gives Tsallis entropy, and (iii) $\boldsymbol{\beta \rightarrow 1}$, $\boldsymbol{\alpha \rightarrow 1}$ gives Shannon entropy.

3.3 SHANNON-LIKE CAPACITY THEOREMS FOR QC

Many questions arise when starting to think about QC capacity theorems. Is it possible to assume that the original Shannon results will apply to QC channels unmodified? Or, does one have to rethink the whole chain of logical steps? It turns out that there are many ways in which QC capacity can be defined. The possible combinations identified so far are given in the table below.

Channel nature	Information nature	Noise characteristic	Capacity theorem
Classical	Classical: Bits	Noiseless	Shannon
		Noisy, AWGN	Shannon
Quantum	Classical: Bits encoded as qubits (entanglement-assisted classical information)	Noiseless	Holevo
		Noisy	Holevo-Schumacher-Westmoreland (HSW)
	Quantum: Arbitrary superposition of sequences of quantum states	Noiseless	Schumacher and Josza
		Noisy, Decoherent	Lloyd-Schumacher-Devetak (LSD)

Any channel that can be used to transmit quantum information can be used for classical information as well, but the converse is not true. Let us look at different capacity theorems and their differences from Shannon's.

The capacity theorems for Quantum Channel (Q-CH) with quantum information are not straightforward generalizations of their classical counterparts. There are many new considerations complicating the derivations, like entanglement, classical bits as assisting quantum communication, single use or many uses, and others. Essentially, there are four types of information transmissions.

(i) Classical

This bound treats the transmission of classical information over quantum channels given as an ensemble of quantum states. The information is encoded over this finite ensemble in which the probability of the j-th member Q_j is given as p_j. Then the Holevo upper bound (Holevo, 1973) for transmitting classical capacity over this noiseless quantum channel is defined as:

$$\chi = H\left(\sum_j p_j \rho_j\right) - \sum_j p_j H\left(\rho_j\right). \tag{3.12}$$

The bound implies that the capacity cannot exceed χ. The *H*-function is the von Neumann entropy, which for a general density matrix *Q* is defined as:

$$H(\varrho) = -Tr(\varrho \log_2 \varrho). \tag{3.13}$$

Using this definition, χ can be rewritten as:

$$\chi = -Tr\left\{\left(\sum_j p_j \rho_j\right) log_2 \left(\sum_j p_j \rho_j\right)\right\} + \sum_j p_j Tr(\rho_j \log_2 \rho_j). \tag{3.14}$$

In simpler language, the bound means that it is impossible to send *n* classical bits using *n* qubits alone. The capacity for sending classical bits on noisy quantum channel then is bounded by Holevo upper bound:

$$C(N) \geq \chi(N). \tag{3.15}$$

Classical Information over Noisy Quantum Channel: Holevo-Schumacher-Westmoreland (HSW) Theorem

The Holevo bound was generalized by Schumacher and Westmoreland for noisy channel (*Schumacher and Westmoreland 1997)*. They showed that the Shannon capacity theorem for classical information can be generalized to the quantum channel. In that case, the Holevo bound can be proven to be asymptotically achievable.

$$C_{HSW}(N) = max_{p_j, \rho_j}\left[H\left(\sum_j p_j \rho_j\right) - \sum_j p_j H(\rho_j)\right] \tag{3.16}$$

Here, the maximum is over all ensembles $\{p_j, \rho_j\}$ for the chosen quantum channel, and *N* denotes noisy quantum channel.

(ii) Private Classical

Let *P(N)* denote the private capacity for sending classical bits on a noisy quantum channel so that only the receiver knows the message. Then it obeys the following bound:

$$P(N) \geq max_{p_j,\rho_j} I(X,B) - I(X,E). \qquad (3.17)$$

Here *I(X,B)* and *I(X,E)* are the mutual information functions for Bob (receiver *B*) and environment *E*. This is in some ways a generalization of the wire-tap channel capacity for classical information.

(iii) Quantum

The quantum capacity *Q(N)* for sending quantum states on a noisy quantum channel is bounded as given below.

$$Q(N) \geq max_{p_j,\rho_j} \{H(X) - H(E)\} \qquad (3.18)$$

The von Neumann entropies relate to the quantum states and environment.

(iv) Entanglement-Assisted Quantum:

Let *E(N)* be the capacity for sending quantum states on a noisy quantum channel with both Alice and Bob possibly using entangled quantum states. Then, its bound is given by:

$$E(N) \geq max_{p_j,\rho_j} I(B), \qquad (3.19)$$

where *I(B)* is the mutual information at the receiver.

3.4 NO-GO THEOREMS FOR QUBITS

Qubits obey laws implied by Heisenberg uncertainty relation. According to this law, it is impossible to measure two canonically conjugate observables with the same precision at the same time. Some examples of such pairs are position and momentum, and energy and time. So if the position is known with some precision, the momentum will be known with a precision that is lesser. It has implications for qubits in form of various “theorems”.

(a) No-cloning theorem:

This fundamental result about qubits was first given by Wootters and Zurek (1982). It states that an arbitrary unknown quantum state cannot be copied. When applied to mixed states, it is called *no-broadcast theorem* and its time-reversed version is known as *no-deleting theorem*. A simple proof of no-cloning theorem is given below.

Let us assume the existence of a cloning operator $U_{cloning}$ that can clone a given state

$$|\varphi> = \alpha|0> + \beta|1>. \tag{3.20}$$

Let $|\varphi>$ be the state we wish to clone. The $U_{cloning}$ operator operating on our initial states has that effect.

$$\begin{aligned} U_{cloning}(|\varphi>|0>) &= |\varphi>|\varphi> = (\alpha|0> + \beta|1>)(\alpha|0> + \beta|1>) \\ &= \alpha^2|00> + \beta^2|11> + \alpha\beta(|01> + |10>) \end{aligned} \tag{3.21}$$

It should also work if we just operate on the expansion of $|\varphi>$.

$$U_{cloning}(|\varphi>|0>) = U_{cloning}(\alpha|0> + \beta|1>)|0> = \alpha|00> + \beta|11> \tag{3.22}$$

The two expressions are very different. In particular, the cross terms are missing in the second one. So our earlier assumption about the existence of $U_{cloning}$ is false.

(b) No-teleportation theorem:

It states that complete accuracy of measurement is impossible for an arbitrary quantum state. If it was possible, then a qubit could be converted to classical bits.

(c) No-communication theorem:

Suppose Alice measures subsystem of an entangled state and wants to send this information to Bob. This theorem states that this communication is impossible.

3.5 A GENERAL MODEL FOR QUANTUM COMMUNICATION

Any digital communication process including quantum communication can be broken down into the following obvious steps: (i) pre-processing and encoding of information before transmission by sender by Alice, (ii) propagation of information carrier across the communication channel, and (iii) decoding and post-processing of received signals Bob.

These ideas when applied to quantum communication translate into the following stages:

(i) Information and channel encoding: Alice encodes classical bits in the attributes of a physical particle or a system in general. An obvious example will be two orthogonal polarization states of a photon. For quantum communication, the bits are encoded in the quantum states. Afterwards, she pre-processes the physical signal attributes to compensate for the noise present in the communication channel.

(ii) Channel evolution: The channel encoded quantum state evolves to a new state after propagation in the quantum channel. The transformed state should not be too different from the original one if the channel encoding was done properly. A general Q-CH transforms the original pure quantum state into a mixed quantum state.

(iii) Measurement: Bob measures the output quantum state and decodes it to recover the information sent by Alice. He uses error correction to remove the noise induced by the Q-CH.

An ideal Q-CH will be an identity so that the original quantum state is unchanged. The Q-CHs in many ways are similar to stochastic classical channels so the channel capacity is always less than that due to the ideal case. In addition to Shannon channel capacity, many new possibilities emerge for them. A new and emerging area of information theory concerned with investigating these questions is called Quantum Shannon Theory.

So far, two major new results about Q-CH capacity have been found.

(i) Classical capacity of Q-CH (Holevo, Schumacher, and Westmoreland) is given by HSW theorem. In this approach, Quantum Mutual Information (see Appendix 3B) is maximized.

(ii) Quantum Capacity of Q-CH (Lloyd, Shor, and Devetak) is given by LSD theorem. In this approach, Quantum Coherent Information (QCI) is maximized. Let

A and B be input and output states respectively,
ρ (A) and ρ (B) be corresponding density matrices of A and B respectively,
$S_{vN}(B)$ be von Neumann entropy of B, and
$S_{vN}(A \mid B)$ be joint von Neumann entropy of B and purification of A.

Then, QCI is given by:

$$I(A,B) = H(B) - H(B \mid A),$$
$$\mathrm{I}(\mathrm{A} > \mathrm{B}) = S_{vN}(B) - S_{vN}(A \mid B). \tag{3.23}$$

3.6 ENTANGLEMENT MEASURES

In this section, a few important quantifiable measures of entanglement are described.

(i) Fidelity

It is one of the measures of the closeness of the original quantum state to the changed one after it has propagated in a noisy environment. Given two density matrices ρ (starting state) and σ (ending state), fidelity is defined as:

$$F(\rho,\sigma) = \left(tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right)^2. \tag{3.24}$$

Here, the square root of density matrix is the matrix with entries as square root of its eigenvalues. This is interpreted as probability. There is an alternate definition without square as well. Here we use the convention used by Jozsa.

The density matrix for a pure state $|\Psi\rangle$ is given as:

$$\rho = \sqrt{\rho} = |\psi><\psi|, \tag{3.25}$$

and so the fidelity for a pure state remains unchanged after time evolution and reduces to:

$$F = <\psi|\rho|\psi>. \tag{3.26}$$

(ii) Concurrence

It is another measure of entanglement and easy to calculate for 2-qubit states. It is defined as in the following.

We recall that under a spin flip operation, we have

$$\sigma_y|0> = i|1>, \sigma_y|1> = -i|0>. \tag{3.27}$$

For pure 2-qubit state, we form a new state by complex conjugation and spin flip operations.

$$|\tilde{\psi}> = \sigma_y|\psi^*>. \tag{3.28}$$

The concurrence of the state is defined as:

$$C(|\psi>) = |<\psi|\sigma_y|\psi^*>| = |<\psi|\tilde{\psi}>|. \tag{3.29}$$

For a general 2-qubit state given as the density matrix $\rho = |\Psi><\Psi|$, we form another matrix $\tilde{\rho} = |\tilde{\psi}><\tilde{\psi}|$. Then it can be proved that the concurrence in terms of its eigenvalues is given as:

$$C(\rho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}. \tag{3.30}$$

Here, λ_i's are the square roots of the eigenvalues of the matrix $(\rho.\tilde{\rho})$ in descending order. A general 2-qubit state is given by

$$|\psi>= a|00> +b|01> +c|10> +d|11> \qquad (3.31)$$

We will also denote this state in short as [*a, b, c, d*]. The concurrence is calculated to be

$$C = 2|ad - bc| \geq 0. \qquad (3.32)$$

It can be verified that for a product state, for example, (1/2) [1, 1, 1, 1], it is zero as expected. For an entangled state, it should be nonzero, and that can be seen in the following example.

Let us generate an entangled state by operating on the earlier product state by an entangling gate close to CNOT.

$$|\psi> = (1/2)\ [1, 1, c-, c+] \qquad (3.33)$$

Here $c_- = \cos\frac{\varphi}{2} - \sin\frac{\varphi}{2}$ and $c_+ = \cos\frac{\varphi}{2} + \sin\frac{\varphi}{2}$. Then the concurrence can be calculated as

$C = 2 \sin \frac{\varphi}{2}$. This is nonzero for nonzero φ and has correct behavior for $\varphi = 0$.

(iii) Entanglement of Formation

It is yet another measure of entanglement and is defined for a 2-qubit state as in the following.

$$E_F(\rho) = H\left(\frac{1+\sqrt{1-C^2}}{2}\right) \qquad (3.34)$$

Here, *H* is the Shannon entropy function defined as:

$$H(x) = -x\log_2 x - (1-x)\log_2(1-x), \qquad (3.35)$$

and C is the concurrence as defined earlier. If the argument of H in the definition of $E_F(\rho)$ is denoted as y, then it satisfies $y^2 - y + (C^2/4) = 0$.

Let us try to form a general 2-qubit state and express it in some basis. The 2-qubit state space is four dimensional, and so we choose an orthonormal basis in this space, which is given by:

$$|e_1> = \frac{1}{2}(|00> + |11>) \tag{3.36}$$

$$|e_2> = \frac{i}{2}(|00> - |11>) \tag{3.37}$$

$$|e_3> = \frac{i}{2}(|01> + |10>) \tag{3.38}$$

$$|e_1> = \frac{1}{2}(|01> - |10>) \tag{3.39}$$

Sometimes this choice is called “Magic” basis because of its special properties. Now, a pure 2-qubit state in this basis can be given by:

$$|\psi> = \sum_{n=1}^{4} \alpha_n |e_n>. \tag{3.40}$$

Then the entanglement of formation of this state is given by:

$$E_F(|\psi>) = H\left(\frac{1+\sqrt{1-\sum_{n=1}^{4}|\alpha_n|^2}}{2}\right). \tag{3.41}$$

3.7 ENTANGLEMENT PROCESSING

In quantum communication, sometimes we need to process a given entangled state for effective transmission of information. Some useful ones

are described in this section.

(i) Entanglement Swapping

It is an operation in which the entanglement state of a qubit pair is transferred to another qubit pair without direct interaction. Let us start with two SPDC sources each of which emits an entangled qubit pair (AB) and (CD). The first source sends the individual qubits in opposite directions, A to sender and B to an intermediate point. The second source sends C to the intermediate point and D to the receiver. At this stage, the qubits A at the sender and D at the receiver are not entangled. At the intermediate place, Bell state measurement is performed on qubits B and C. Through this projective measurement,qubits A and D then become entangled. It is one of the most basic operations for quantum repeaters.

(ii) Entanglement Distillation and Purification

The starting entanglement states become less entangled after propagation in a noisy environment. It is possible to transform the starting states using local unitary operations in such a way that they are reduced to a smaller number of maximally entangled states or Bell-pairs. It should be recalled that the maximally entangled states are a special kind of 2-qubit states. This operation is called entanglement distillation. It effectively replaces noisy communication with a noiseless one using local operations.

One starts from a large number of low-fidelity EPR states. Their low fidelity is a result of environmental noise. In the purification process, local unitary operations are applied on this collection and this improves their fidelity. At the end, a smaller number of desired high-fidelity states are extracted. Local operations consist of Pauli rotations and CNOT gate operations. An arbitrary mixed state can be turned into Werner states to which Pauli operation σ_y and CNOT gate are applied. It can be proved that the resulting state has higher fidelity value.

APPENDIX 3A: SPECIAL 3-QUBIT QUANTUM STATES

In 3-qubit states, the classification of entangled states has led to two configurations with special entanglement properties. Their 2-qubit system part cannot be separated. These are known as GHZ and W states as named after their discoverers.

(i) Greenberg-Horne-Zeilinger (GHZ) States

A GHZ state is a 3-qubit state defined as:

$$GHZ = \frac{1}{\sqrt{2}}\left(|000> + |111>\right). \tag{3.42}$$

It is an entangled state and so cannot be decomposed into any simpler states. The GHZ state has some interesting properties.

- A GHZ state is maximally entangled. For such a state, the trace over the square of density matrix is less than one ($Tr(\rho^2)<1$).
- If partial trace is taken over one of the 3-qubits, an unentangled 2-qubit state is obtained.

The idea can be generalized to any number of qubits, in which case a GHZ state is defined as a superposition of all qubits being in |0> state with all of them being in |1> state.

(ii) Werner States

A Werner state is another special 3-qubit state defined as:

$$W = \frac{1}{\sqrt{3}}\left(|001> + |010> + |100>\right). \tag{3.43}$$

It is a symmetric combination of 3-qubit states and is invariant under their permutations. Any given state is represented by an 8×1 column vector.

The definition can be generalized to any number of states. In such a case, a Werner state is a sum of all states obtained by permutations. In other words, Werner states are invariant under any particular single qubit unitary operation acting on all states. Werner states have been found useful in theoretical investigations of noisy quantum channels.

APPENDIX 3B: PERES-HORODECKY CRITERION

It is a mathematical test to ascertain whether a given mixed qubit state is entangled. It is both necessary and sufficient criteria for 2-qubit states. For higher number qubit states, it is a necessary condition but not sufficient. To

make Peres-Horodecky Criterion sufficient for higher number qubit states, it needs to be supplemented with extra conditions.

Given a 2-qubit state represented by a density matrix ϱ, let us form a "partial transpose" or PT-matrix and find its eigenvalues. If none of them is negative, then the starting state is entangled, otherwise it is separable. We will illustrate it below by an example.

Let the starting state be a mixture of a Bell state and constant matrix.

$$\rho = p\left|\Psi^{-} >< \Psi^{-}\right| + \frac{1}{4}(1-p)I \tag{3.44}$$

Here, I is the 4×4 identity matrix. The density matrix is expanded as:

$$\rho = p\frac{1}{\sqrt{2}}(|01> - |10>)\frac{1}{\sqrt{2}}\left(<01| - <10|\right) + \frac{1}{4}(1-p)I. \tag{3.45}$$

Using the column vector representation of the states, we get,

$$|01> = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix},\ |10> = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix},\ |\Psi^{-}> = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}. \tag{3.46}$$

Now the density matrix is calculated as:

$$\rho = \frac{1}{4}\begin{bmatrix}1-p & 0 & 0 & 0\\ 0 & 1+p & -2p & 0\\ 0 & -2p & 1+p & 0\\ 0 & 0 & 0 & 1-p\end{bmatrix}. \tag{3.47}$$

The PT matrix with respect to B-system is obtained by transposing the upper-right and lower-left 2×2 parts.

$$\rho^{T_B} = \frac{1}{4}\begin{bmatrix} 1-p & 0 & 0 & -2p \\ 0 & 1+p & 0 & 0 \\ 0 & 0 & 1+p & 0 \\ -2p & 0 & 0 & 1-p \end{bmatrix}. \qquad (3.48)$$

It has three eigenvalues: $\frac{1+p}{4}, \frac{1+p}{4}$, and $\frac{1-3p}{4}$. The last one is the smallest eigenvalue. So the criterion for entanglement gives these possibilities:

- $p < 1/3$, system is separable
- $p > 1/3$, system is entangled

APPENDIX 3C: VON NEUMANN ENTROPY

Let us start with a general quantum state as a superposition of its eigenstates.

$$|\Psi> = \sum_i a_i |i> \qquad (3.49)$$

Then the expectation value of an observable O (or a quantum mechanical operator) is

$$<O> = <\Psi|O|\Psi> = \sum_{i,j} a_i^* a_j <i|O|j> \qquad (3.50)$$

Define the density matrix as;

$$<j|\rho|i> = a_j a_i^*. \qquad (3.51)$$

Then we can write,

$$<O> = \sum_{i,j} <j|\rho|i><i|O|j> = \sum_j <j|\rho O|j> = Tr(\rho O). \qquad (3.52)$$

It can now be seen that von Neumann entropy is given by

$$S_{vN}(X) = -<ln\rho> = -Tr(\rho ln\rho). \qquad (3.53)$$

APPENDIX 3D: OTHER INFORMATION ENTROPIES

Let us start with random variables *X* and *Y* which take values from the set [0,1]. The probability of obtaining a specific value from the set is given by the probability distributions *p(x)* and *p(y)*. The conditional probability distributions give probabilities of a chosen random variable if the other one is already known. They are denoted by *p(x|y)* and *p(y|x)*. Finally, the joint probability distribution *p(x,y)* gives probabilities for both random variable selected together.

The joint and conditional probability distributions are related in the following way:

$$p(x,y) = p(y)\,p(x|y) = p(x)\,p(y|x). \qquad (3.54)$$

The entropies are measures of knowledge about the information in the probability distributions. They are defined as:

(i) Marginal entropies: Shannon entropy is a famous example.

$$H(X) = -\sum_x p(x) log_2 p(x) \qquad (3.55)$$

$$H(Y) = -\sum_y p(y) log_2 p(y) \qquad (3.56)$$

Here, the sum is over all the values taken by the random variable. For our example, they are 0 and 1.

(ii) Conditional entropies:

$$H(X|Y) = -\sum_y p(y)\left(\sum_x p(x|y) log_2 p(x|y)\right) \qquad (3.57)$$

$$H(Y \mid X) = -\sum_{x} p(x) \left(\sum_{y} p(y \mid x) log_2 p(y \mid x) \right) \tag{3.58}$$

(iii) Joint entropy:

$$H(X,Y) = -\sum_{x} \sum_{y} p(x,y) log_2 p(x,y) \tag{3.59}$$

(iv) Mutual information:

$$I(X,Y) = -\sum_{x} \sum_{y} p(x,y) log_2 \frac{p(x,y)}{p(x)\,p(y)} \tag{3.60}$$

These entropies are not independent. Their relationship can be found by applying the relation between joint and conditional probability distributions.

$$I(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

$$I(X,Y) = H(X) + H(Y) - H(X,Y) \tag{3.61}$$

$$I(X,Y) = H(X,Y) - H(X|Y) - H(Y|X)$$

CHAPTER 4

QUANTUM ERROR CORRECTION CODING AND CRYPTOGRAPHY

In this chapter, we will present one of the most important applications of Quantum Communication (QC), namely, quantum coding and cryptography. In analogy with classical communications, errors at the qubit level occurring during QC can be corrected by quantum error correction codes. Their discovery has led to some very interesting developments in general coding theory. One of the most obvious advantages of QC is the fact that it is unbreakable.

We will present the reasons for such thinking and describe very widely used protocols.

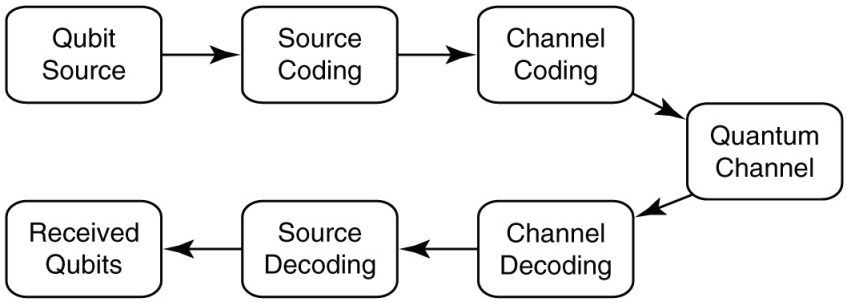


Figure 4.1. Sequence of coding action during quantum communication

4.1 NEED FOR CODING IN COMMUNICATION

Classical data communication process undergoes two kinds of coding as shown in Figure 4.1.

SOURCE CODING (CLASSICAL)

Source coding is also known as data compression and aims at removing redundancies in the data stream to prepare it for more efficient transmission. Zip data compression used on the Internet to make files smaller is a well-known example.

Suppose we have a data source with redundancy in which the individual bits are random and occur according to some probability distribution. Then Shannon's Noiseless Source Coding Theorem states that there exists a reliable compression scheme with a rate R such that

$$R > H(P). \tag{4.1}$$

Alternatively, the optimal data compression rate for variable length codes for an arbitrary source with probability distribution $P(x)$ lies between Shannon entropy $H(P)$ and $H(P)+1$.

CHANNEL CODING (CLASSICAL)

Communication process introduces errors in the bit stream due to noise inherent in physical channels. Channel coding adds extra bits to the data to correct for imperfections of the channel. Reed-Solomon, Hamming, Turbo codes, etc., are some examples.

Quantum communication also needs such codes because ultimately the qubits need to be compressed for more efficient representation and travel through a noisy physical medium.

4.2 SOURCE CODING (QUANTUM)

There is a quantum version of source coding theorem with the following changes.

(i) The classical bit is a random variable and follows a probability distribution. In QC, its counterpart is the density matrix corresponding to a qubit. We recall that density matrix for state $|\boldsymbol{s}>$ is defined as $\boldsymbol{\rho} = |\boldsymbol{s}><\boldsymbol{s}|$.

(ii) The QC counterpart of the Shannon entropy is the von Neumann entropy.

Let there be a source of quantum states $|S>$ with probability distribution $P(s)$. A general quantum codeword composed of N such states is then given as:

$$\sigma = \sum_{n=1}^{N} P(s_n) \,|\, s_n >< s_n \,|. \tag{4.2}$$

With these changes, the Quantum Lossless Source Coding Theorem states (Schumacher)] that for all uniquely decodable quantum codes, the expected average length of the codeword is lower-bounded by von Neumann entropy S(σ):

$$l_{avg} \geq S(\sigma) = -Tr(\sigma log_2 \sigma). \tag{4.3}$$

4.3 ERROR CORRECTION CODING (QUANTUM): AN EXAMPLE

The Quantum Error Correction Codes (QECC) for correcting errors introduced by a noisy quantum channel have been found relatively recently. Steane code, surface code, toric code, etc., are some examples. The basic idea of QECC can be understood by looking at the case of single qubit bit flip error correction.

Alice executes the following steps to send qubit $|A> = a|0> + b|1>$ to Bob.

(i) (Alice) Step1. She adds two qubits in state |00> to the starting qubit to get

$$|A> = a|000> + b|100>. \tag{4.4}$$

(ii) (Alice) Step2. She applies CNOT operation to the to the first and second members of the qubits,

$$CNOT\ (1,2)\,|000> = |000>,\ CNOT(1,2)\,|100 = |110>. \tag{4.5}$$

(iii) (Alice) Step3. She applies CNOT operation to the to the first and third members of the result qubits in step 2,

$$CNOT\ (1,3)\,|\,000>=\left|000>,\ CNOT\,(1,3)\right|110>=|\,111>. \qquad (4.6)$$

(iv) (Alice) Step4. She releases the resulting qubits as inputs to the quantum channel,

$$|\,A_{in}>=a\left|000>+b\right|111>. \qquad (4.7)$$

Quantum channel adds noise, so the qubit changes. These changes are random and follow a probability distribution. For bit flip error, we assume that it is given by the following:

$$\begin{aligned}&\text{Probability of } (|\,0>\rightarrow|\,1>) = \text{Probability of } (|\,1>\rightarrow|\,0>) = p,\\ &\text{Probability of } (|\,0>\rightarrow|\,0>) = \text{Probability of } (|\,1>\rightarrow|\,1>) = 1-p. \qquad (4.8)\end{aligned}$$

Then the probabilities for the input qubit changing to any of the eight possibilities can be computed.

$$\begin{aligned}&\text{Prob } (|\,A_{in}>\rightarrow a\left|000>+b\right|111>) = (1-p)^3\\ &\text{Prob } (|\,A_{in}>\rightarrow a\left|100>+b\right|011>)\\ &\quad = \text{Prob } (|\,A_{in}>\rightarrow a\left|010>+b\right|101>)\\ &\quad = \text{Prob } (|\,A_{in}>\rightarrow a\left|001>+b\right|110>) = p(1-p)^2\end{aligned} \qquad (4.9)$$

$$\begin{aligned}&\text{Prob } (|\,A_{in}>\rightarrow a\left|110>+b\right|001>)\\ &\quad = \text{Prob } (|\,A_{in}>\rightarrow a\left|101>+b\right|010>).\\ &\quad = \text{Prob } (|\,A_{in}>\rightarrow a\left|011>+b\right|100>) = p^2(1-p)\\ &\text{Prob } (|\,A_{in}>\rightarrow a\left|111>+b\right|000>) = p^3\end{aligned} \qquad (4.10)$$

Bob does the following operations on the received qubits.

(i) (Bob) Step1. He uses CNOT operation on received qubits to generate two extra qubits called ancilla from the given eight possibilities.

$$
\begin{aligned}
&CNOT\left(a|000>+b|111>\right)\rightarrow \text{ancilla}\ |00>\\
&CNOT\left(a|111>+b|000>\right)\rightarrow \text{ancilla}\ |00>\\
&CNOT\left(a|001>+b|110>\right)\rightarrow \text{ancilla}\ |01>\\
&CNOT\left(a|110>+b|001>\right)\rightarrow \text{ancilla}\ |01>\\
&CNOT\left(a|010>+b|101>\right)\rightarrow \text{ancilla}\ |10>\\
&CNOT\left(a|101>+b|010>\right)\rightarrow \text{ancilla}\ |10>
\end{aligned}
\qquad (4.11)
$$

$$
\begin{aligned}
&CNOT\left(a|100>+b|011>\right)\rightarrow \text{ancilla}\ |11>\\
&CNOT\left(a|011>+b|100>\right)\rightarrow \text{ancilla}\ |11>
\end{aligned}
$$

(ii) (Bob) Step2. He measures the two ancilla bits in the {\0>, |1>} basis and takes the following actions:

- for |00>, does nothing,
- for |01>, |10> and |11>, applies Pauli operator $\boldsymbol{\sigma_x}$ to the third, second, or first qubit respectively.

After this, he obtains the following:

$$
\begin{aligned}
&\sigma_x(3rd\ qubit)\left(a|001>+b|110>\right)\rightarrow a|000>+b|111>\\
&\sigma_x(2nd\ qubit)\left(a|010>+b|101>\right)\rightarrow a|000>+b|111>\\
&\sigma_x(1st\ qubit)\left(a|100>+b|011>\right)\rightarrow a|000>+b|111>\\
&\sigma_x(3rd\ qubit)\left(a|110>+b|001>\right)\rightarrow a|111>+b|000>\\
&\sigma_x(2nd\ qubit)\left(a|101>+b|010>\right)\rightarrow a|111>+b|000>\\
&\sigma_x(1st\ qubit)\left(a|011>+b|100>\right)\rightarrow a|111>+b|000>
\end{aligned}
\qquad (4.12)
$$

(iii) (Bob) Step3. Bob applies CNOT from the first to the second qubit and from the first to the third qubit to obtain either $\left(a|0>+b|1>\right)|00>$ or $\left(a|1>+b|0>\right)|00>$. So Bob has either the correct qubit sent by Alice or her qubit changed by $\boldsymbol{\sigma_x}$ but with the probability of success greater than 1–p which is very good as long as p<1/2.

This method is such that as long as the channel introduces no error or only one qubit error, Bob will find the correct qubit with a very high probability.

4.4 GENERAL ERROR CORRECTION CODING (QUANTUM)

There have been many attempts to develop new approaches to quantum error correction. Due to no-cloning theorem, the input states cannot be copied, so an indirect approach is used. The general approach involves the following steps:

(i) Alice adds extra qubits to the input qubits and applies some gate operations;
(ii) The channel adds errors by flipping the bits and phases of the transmitted qubits;the latter means that the sign '+' changes to '–' and vice versa;
(iii) Bob applies a combination of suitable gate operations and unitary transformations to arrive at the correct qubits sent to him.

The basic challenge is to find proper qubit operations for maximizing the probability of correct decoding by Bob. A general solution is not available but many particular codes have been discovered. Finding powerful codes for quantum computing is a very active research area and many codes have been discovered.

A class of such codes is known as Calderbank-Steane-Shor (CSS) code. We introduce one of its special cases known as Steane code which can correct arbitrary single qubit errors. It is based on classical 7-bit Hamming code and so uses 7 qubits. For correcting qubit flip errors (also called X errors), it uses self-dual [7,4,3] Hamming code, and for correcting phase flip errors (also called Z errors), it uses the dual of [7,3,3] Hamming code. In the given notation, (i) 3 is the minimum number of changes in going from one code word to another, (ii) 7 is the block length, and (iii) 4 or 3 is the message length. Some of the other such codes are Toric code and Surface code.

Codes useful for quantum communication are somewhat different. Source coding remains the same but channel coding is different because of the requirement of being able to transmit qubits over long distances. When using optical fiber, photons are lost during transmission. This manifests itself as amplitude damping or attenuation of the initial photonic beam. Photon loss codes and parity codes have been developed to correct transmission errors for this purpose.

4.5 CRYPTOGRAPHY: CLASSICAL AND QUANTUM

Cryptography is a branch of mathematics concerned with secure communication of messages between two parties in the presence of a third party, for example, between Alice and Bob in presence of Eve (for an eavesdropper or third party adversary). The basic components of a classical cryptographic system are the following:

(i) Plaintext: The message to be coded

(ii) Encryption: It is the method by which Alice transforms plaintext into a ciphertext and usually involves operating on the plaintext by a sequence of mathematical operations like transposition, substitution, etc., and converting it to nonsense.

(iii) Key sharing: The method by which the secret decryption key is shared between Alice and Bob. It should be such that Eve is not able to intercept the key. This step is very important and the key sharing process must satisfy the requirements of confidentiality, integrity, authentication, and non-repudiation.

(iv) Transmission: The ciphertext is transmitted using a secure physical medium.

(v) Decryption: Bob decrypts the ciphertext to recover the intended plaintext.

Out of the many classical cryptographic algorithms, only one-time pad is known to be provably secure and unbreakable. At the same time, it is very hard to implement due to the requirement of generation and exchange of random secret code of the same length as that of the plaintext. For other approaches, in general, it is possible to make the decryption stage

computationally so demanding that Eve cannot break the code. But even then, the security of the code is not guaranteed against future advances in the mathematical and computational techniques.

A general QKD setup is depicted in Figure 4.2 in which Alice sends an encrypted message to Bob on a classical channel like optical or wireless network. She also sends the secret key for deciphering the message but on a quantum channel. The eavesdropper Eve has access to both channels and tries to intercept the quantum channel by measuring the secret key qubits. Quantum cryptography guarantees the security of ciphertext based on the laws of quantum mechanics. This comes from the fact that any attempt by Eve to intercept the message destroys the qubit which was carrying it.

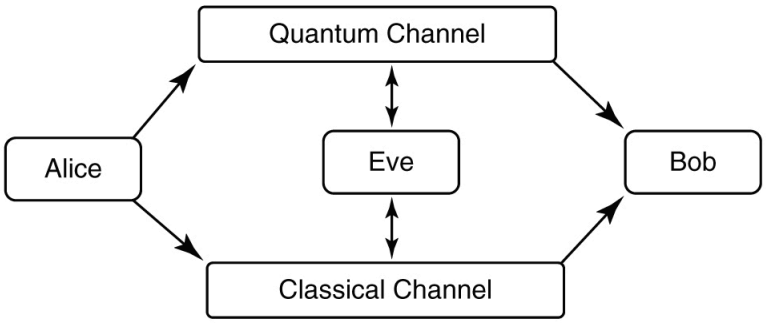


Figure 4.2. Standard QKD setup with possibility of interception by Eve

In this communication between Alice and Bob, the exchange of secret key is the crucial step. Once this is completed, the ciphertext can be sent on the classical channel. Many quantum key distribution (QKD) protocols have been developed to accomplishment this task efficiently. They are classified according to the principle of QM used.

(i) Heisenberg uncertainty principle
(ii) Entanglement

In general, the same protocols have two versions based on the above classification.

4.6 A QKD PROTOCOLS BASED ON HEISENBERG UNCERTAINTY PRINCIPLE

BB84 (Bennett and Brassard, 1984)was the first cryptographic algorithm based on the principles of quantum mechanics. This is the sequence of steps it follows:

(i) Alice converts the secret key to bits, and before sending them to Bob, encodes them randomly in four photon polarization states as follows: 0° as 0, 90° as 1 (called rectilinear basis), 45° as 0, 135° as 1 (called diagonal basis). She also records the bit values and corresponding polarization states.

(ii) Bob measures the received photons in rectilinear or diagonal basis chosen randomly and records them as well as resulting polarization states. Bob sends the sequence of basis used (and not the polarization states) to Alice.

(iii) Alice compares the received information with her records, identifies the smaller subset of the correct key, and sends it to Bob on a public channel. She also deletes the wrong identifications from her records thus generating a shorter key.

(iv) Bob receives the correct key.

It was found that even though the BB84 protocol is unconditionally secure because of its use of quantum mechanical principles; there are still some loopholes due to sources and detectors. Efforts were made to close those loopholes and BB84 was improved utilizing similar ideas. Currently all the loopholes have not been closed.

4.7 A QKD PROTOCOL BASED ON ENTANGLEMENT

BB84 uses photon polarization states which do not use entangled states. It was found that it is possible to modify existing protocols like BB84 by using them. This improves their security as well. This allows new versions of all the protocols of the BB84 family. Here we describe the first such protocol, known as E91 (Ekert, 1991), discovered by Artur Ekert in 1991 as the entanglement version of BB84.

Let us recall that in BB84, Alice creates the photons and sends them to Bob. In E91, there is a central source creating an entangled singlet state out of two spin-1/2 particles.

$$|\psi> = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow> - |\downarrow\uparrow>\right) \tag{4.13}$$

The source sends one particle to Alice and another to Bob. The spin-up or spin-down nature of individual particles are unknown and can be known only after a measurement. Alice and Bob measure the particle spins in the coplanar bases given by (0°, 45°, 90°) and (45°, 90°, 135°) with respect to x-axis respectively. Let us denote them as a_i and b_j with (i,j = 1,2,3).

There are nine combinations of the bases in which Alice and Bob can measure the particle spins. They can be divided in two groups: in the first group, the bases are compatible whereas in the second group, they are not. They exchange the information about the correlation coefficient for the second group on the public channel without revealing the measurement outcomes.

Define $P_{++}(a_i, b_j)$ as the probability of obtaining +1 along a_i axis and +1 along b_j axis. Then the correlation coefficient is defined as:

$$E\left(a_i, b_j\right) = P_{++}\left(a_i, b_j\right) + P_{--}\left(a_i, b_j\right) - P_{+-}\left(a_i, b_j\right) - P_{-+}\left(a_i, b_j\right). \tag{4.14}$$

Now define the quantity S as a combination of these correlation coefficients.

$$S = E\left(a_1, b_1\right) - E\left(a_1, b_3\right) + E\left(a_3, b_1\right) + E\left(a_3, b_3\right) \tag{4.15}$$

Bell proved that quantum mechanics implies that

$$S = 2\sqrt{2}. \tag{4.16}$$

A value lower than this indicates that Eve has tried to interfere with the transmission. In that case, Alice and Bob throw out all results and start anew. Once they are satisfied that there has been no interference, their observation can be trusted. Now they only keep the first group as they can be sure that they are anti-correlated and use it for the secret key.

4.8 PRACTICAL QKD

The number of variations on the two basic approaches of BB84 and E91 is large and many such protocols have been proposed and verified. So far, none of them are totally secure and have some loophole or the other. These mostly arise from the imperfect nature of the source, the channel, and the detector employed in a practical QKD setting. For example, the channel can be noisy or the detector can be inefficient. The market place has generated some solutions and some of those systems are being used in real life. MagiQ and IdQuantique are two pioneer companies which have built such systems. Most of the current theoretical and experimental work in this area is focused on trying to devise a practical and loophole-free implementation of QKD.

CHAPTER 5

QUANTUM COMMUNICATION NETWORK (QCN)

In this chapter, we will present the basic ideas behind future realization of Quantum Communication Network (QCN). Currently, researchers are trying to develop architectures, components, and protocols for QCN.

5.1 A REVIEW OF CLASSICAL COMMUNICATION NETWORK

The classical communication network is a layered structure according to the Open Systems Interconnection (OSI) model, as shown in Figure 5.1.

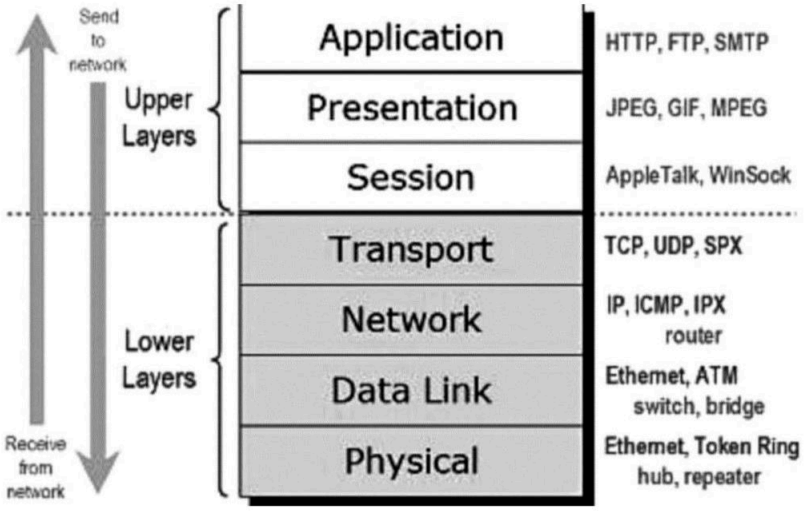


Figure 5.1. OSI model (source: compnetworking.about.com)

The full task of communicating data between two entities can be broken down into many simpler tasks taking place at a specific layer. The layers are logical abstractions and can be physically implemented in many ways. By convention, physical layer is considered to be the lowest layer.

Each layer supports specific protocols and performs the following generic tasks:

- it receives the packet header together with data payload from higher (or lower) layer;
- it adds new information as extra bytes at the beginning or end of the data payload to (or removes from) it according to the rules of the protocol; and
- it sends the packets to the protocols at the next layer.

The basic task of communication between two users (or applications) can be broken down into the following layer tasks, starting from the top:

(i) Application: It provides services to the software requiring network services. Software programs, for example,Microsoft Word or Microsoft Excel, are not part of the layer. Browsers, FTP clients, and mail clients exist at this layer.

(ii) Presentation: It takes care of data representation and formatting like graphics and video.

(iii) Session: It establishes and maintains session between sending and receiving computers.

(iv) Transport: It helps with assembly and dis-assembly of the data packets and makes sure that they are transported reliably.

(v) Network (also called Internet layer): It is concerned with routing and logical addressing for communications between local networks and lies at the heart of the Internet.

(vi) Data Link: It provides mechanism to move data in a local network and uses topologies like Ethernet.

(vii) Physical: At this layer, data is translated into physical signals, like electrical, optical, or wireless.

The OSI model is a very good logical framework but the real Internet is based on an alternative approach known as the US Department of Defense

reference model. The seven layers of OSI are compressed into four layers supported by the TCP/IP protocol suite as given in Figure 5.2 below. This was developed by the now famous DARPA project called ARPAnet by DOD.

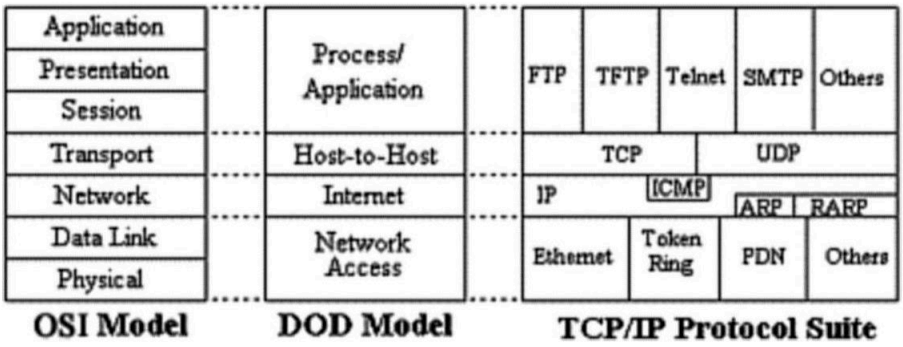


Figure 5.2. OSI and DOD models (source: infocellar.com)

The OSI layer model is at the foundation of the modern computer communications. As we will see, use of quantum mechanical principles will necessitate some changes in this model.

5.2 BASIC QCN ARCHITECTURE

There is no standard scheme of OSI-like layers for QCNs because we are at a very early stage of QCN evolution. The foremost use of quantum approach to communication has resulted in Quantum Key Distribution (QKD) protocols. They add unbreakable security, in principle, to point-to-point communication. Recently, there have been many efforts to extend this security to multi-node QKD networks. We will describe one of them as developed by a consortium of research labs led by Japan.

The Tokyo QKD network has three layers as given in Figure 5.3. A secure TV conference application was demonstrated over this network in 2012.

The layers have the following functions:

(i) Quantum Layer

This layer consists of point-to-point optical fiber quantum links between QKD devices. Each device generates a secure key in its own way and hands over the result to the higher key management layer.

(ii) Key Management (KM) Layer

This layer has KM Agent (KMA) devices at each site for receiving the key material from the Quantum Layer. KMAs resize and save this information. They also store Quantum Bit Error Rate (QBER) and key generation rate. The agents also implement advanced encryption standards in addition to one-time pad. The keys are relayed in a hop-by-hop fashion.

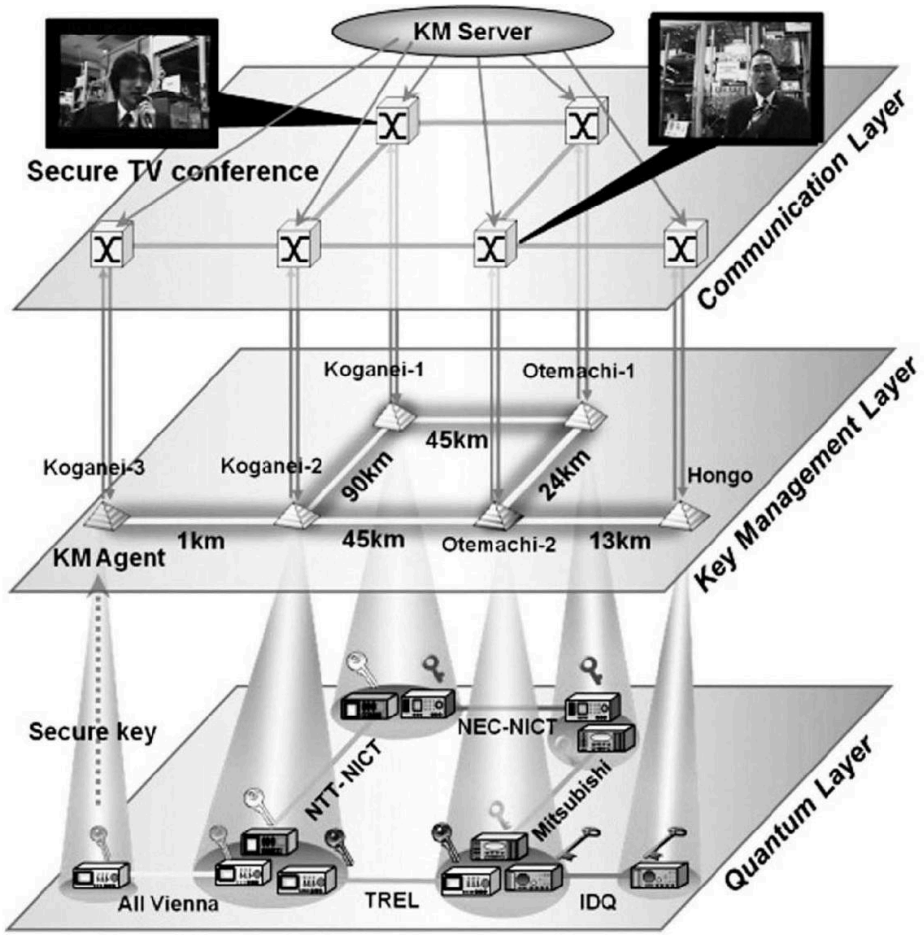


Figure 5.3. QKD network layers (source: www.uqcc.org/QKDnetwork/). Abbreviations: IDQ = IDQuantique, KMA = Key Management Agent, NICT = National Institute of Information and Communications Technology, NTT = Nippon Telegraph & Telephone, TREL = Toshiba Research Europe Ltd.

(iii) Communication Layer

In this layer, secure TV conferencing (the main application) and key downloading to mobile phones are performed. The video encryption rate is 128 kbps in a stored key mode.

Finally, a key management server (KMS) gathers link information from agents, organizes a routing table, and provisions secure paths to them. A very strong authentication code is implemented in KMSs and KMAs.

5.3 QUANTUM TELEPORTATION

Quantum teleportation is not teleportation in the sense of science-fiction books or movies. It solves the basic problem of transporting a quantum state across space without violating no-cloning theorem. Let us recall that according to this theorem, we cannot replicate a quantum state. This dilemma is solved by somehow being able to transport quantum state information without moving the physical particles themselves.

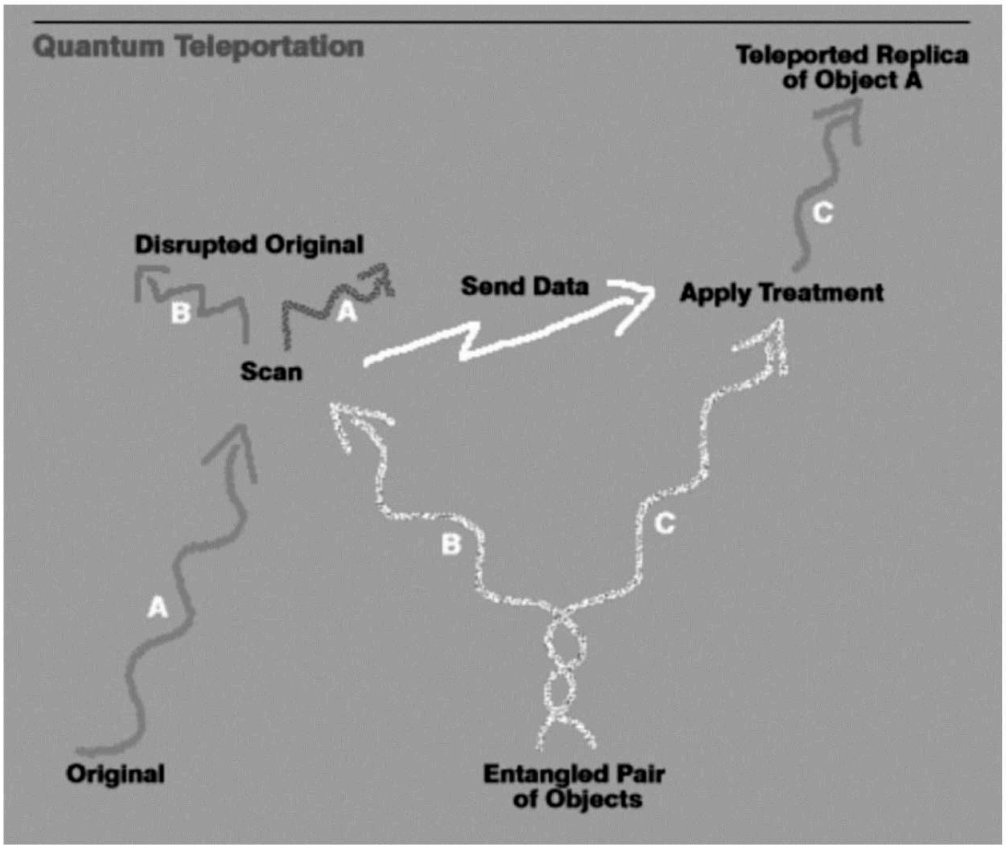


Figure 5.4. Quantum teleportation schematic (source: http://researcher.watson.ibm.com/researcher/view_group.php?id=2862)

The following steps describe how it works.

(i) We start with the qubit *A* in a given quantum state at location *A*. The task is to teleport this state to location *C*.

(ii) An EPR pair of qubits *B* in a particular Bell state (it will be different from the state to be transported in general) is also generated and the two member particles of the pair are sent to location *A* and *C*.

(iii) At location *A*, quantum states of partial qubit *B* and qubit at *A* are measured and then both qubits are discarded. The outcome is encoded as one of four possibilities into two classical bits.

(iv) The two classical bits are sent to location *C* via a classical communication channel and are decoded. Bob deduces the state of his qubit *B* based on this information.

a. He does not have to do anything if *B* is indicated as being in same state as that of the EPR qubit.
b. If it is different, then he can make unitary transformation to change the state of *B* to that of *A*. So effectively the state of *A* has been teleported to *C*.

The experimental confirmation for this came in 1998 and has been repeated many times since then. Currently, the research is focused on increasing the distance between *A* and *B*. Current record of 25 kilometers over optical fiber was reported in 2014 by an experimental physics group at University of Geneva, Switzerland.

5.4 QUANTUM SUPER-DENSE CODING

Suppose Alice wants to send classical bits using qubits. Then she can encode one classical bit in a qubit and send it to Bob who can then decode it. It is seen that use of a qubit does not provide any advantage. Question arises that is it possible to improve upon this bound.

In general it is not possible to send more than one classical bit of information using a qubit. But if Alice and Bob share an entangled state, then it is possible to send two classical bits using that single state. This is called *super-dense coding* protocol of quantum communication.

These are the steps in the execution of this protocol:

1. Alice and Bob share an entangled pair or a Bell-pair given by:

$$|\psi> = \frac{1}{\sqrt{2}}\left[|0>_A|0>_B + |1>_A|1>_B\right]. \qquad (5.1)$$

2. Alice now uses local operations on the Bell-pair to send two classical bits. These operations only affect her states. The table below shows the operations.

Classical bit to be sent	Operations on Bell-pair performed by Alice	Resultant State
00	No operation	$\|\psi> = \frac{1}{\sqrt{2}}\left[|0>_A|0>_B + |1>_A|1>_B\right]$
01	X gate	$\|\psi> = \frac{1}{\sqrt{2}}\left[|1>_A|0>_B + |0>_A|1>_B\right]$
10	Z	$\|\psi> = \frac{1}{\sqrt{2}}\left[|0>_A|0>_B - |1>_A|1>_B\right]$
11	XZ	$\|\psi> = \frac{1}{\sqrt{2}}\left[|0>_A|1>_B - |1>_A|0>_B\right]$

3. Bob decodes the received states by applying *H* unitary operation (also called Hadamard gate), thus finding out the information sent by Alice.

5.5 QUANTUM REPEATER NETWORK

It is well known that signal strength decreases exponentially with distance. In classical communication, this problem is solved by placing amplifiers along the communication path. In quantum communications, this strategy

does not work because quantum states cannot be copied (also known as the no-cloning theorem). Quantum Repeaters (QR) solve this problem.

Let us divide a communication path into many line segments. Let us choose two segments with nodes (1, 2) for the first and nodes (3, 4) for the second. Their lengths are such that the signals become very weak by the time they reach the end of the segment. We want to propagate entangled states from node 1 to node 4. For that, one uses the process of "entanglement swapping". We create entanglements between nodes 1 and 2 and also separately between nodes 3 and 4.A joint measurement for entanglement is performed between nodes 2 and 3 and this information is communicated using classical methods to nodes 1 and 4.

The entanglement swapping measurement is not one-shot and so many measurements have to be made. This collection follows a statistical distribution. Further, there is a need to store the measurements, so a quantum memory is needed. The device that makes this possible is called a Quantum Repeater (QR).

5.6 SOFTWARE DEFINED QUANTUM NETWORKING

Software Defined Networking (SDN) is a new way to organize network tasks in traditional classical networks. They consist of network devices which forward the data and also exercise control over it. In SDN, these two broad functions are separated in the so-called data plane and control plane. All control functions are exercised by a centralized controller and network devices just forward the data.

This paradigm when applied to QCN leads to Software Defined Quantum Communication (SDQC). It is a relatively new area of research and much needs to be developed.

CHAPTER 6

PHYSICAL REALIZATION OF QUANTUM COMMUNICATION NETWORK

In this chapter, we will present the basic ideas behind future realization of Quantum Communication Network (QCN). Like any far reaching idea in science, it has to be embodied in devices and systems. The most obvious example is the classical communication network built out of the receivers, transmitters, links, and information processing nodes in the intervening space. QCN is being modeled after such networks but there may be surprises as more progress is made. It may turn out that this approach to QCN may need to change in light of future advances. Currently, researchers are trying to develop architecture, components, and protocols for QCN.

Quantum Communication (QC) uses so-called "flying" qubit sources. These are photons propagating either in free space or in optical fibers. In addition, the qubits developed for quantum computing are stationary sources. They can be converted to flying ones for QC purposes.

6.1 FLYING QUBIT SOURCES

There are two basic methods to produce flying qubits.

(i) Photonic qubits in free space

A single photon is a quantum particle with many physical attributes having two distinct values so that they can be used to represent two quantum states needed to make a qubit. Possible attribute are polarization, phase, time, spatial modes, and frequency.

- Horizontal and vertical polarization modes of a photons can encode logical and respectively. Any orthogonal combination of these two

is another possibility.

- Orbital Angular Momentum (OAM) modes are spatial configurations of photon electromagnetic fields carrying angular momentum and can be used to encode qubits.
- Laser pulses separated in time such that it is difficult to tell them apart at the output is an example of time-based qubits. Same idea works for frequency separated pulses.

The source should emit single photons so they can be treated as quantum particles. A big research effort is on to find and perfect single-photon sources and detectors.

(ii) Photonic qubits from Spontaneous Parametric Down Conversion (SPDC)

SPDC is a physical process that takes place inside a uniaxial crystal when a pump laser light is incident on it. The crystalline medium is such that inside it, the dipole polarization induced by the light wave depends quadratically on the electric field of the light. This is called secondorder optical effect and is called parametric because it depends on the electric field and not on the light intensity. An example of such a crystal is β-Barium Borate (BaB_2O_4) also known as BBO crystal.

The incident photon gets converted into two photons inside the crystal and they are called signal and idler photons. They have opposite polarizations. Down conversion refers to the fact that their frequencies are lower than that of the incident photon. The directions of the outgoing photons can be thought to exist on the outer surface of two cones whose axes are the light rays of idler and signal lights. The intersection region of the two cones consists of photons whose polarization cannot be determined as they can be in any of the two orthogonal states. This is a hallmark of entanglement. The process is subject to energy and momentum conservation laws given by:

$$\begin{aligned} \omega_{pump} &= \omega_{signal} + \omega_{idler}, \\ \boldsymbol{k}_{pump} &= \boldsymbol{k}_{signal} + \boldsymbol{k}_{idler}. \end{aligned} \tag{6.1}$$

The SPDC process can be used to generate Bell pairs, which are maximally entangled photon pairs.

6.2 STATIONARY QUBIT SOURCES

Qubit is an abstract concept representing a two-state quantum entity, and it can be realized in many ways. The desired attributes of the source for quantum communication are the following:

- persistence of qubit properties over a long time,
- ability of preparing a given state repeatedly on demand,
- ability to evolve the qubit into any desired state, and
- efficient read-out capability.

Stationary qubit sources are better suited for quantum computing applications. For quantum communication, the sources have to be converted to photonic ones so they can cover longer distances. Optimum conversion methods also depend on the physical processes under consideration. This is a very active area of research. Many ideas based on different physical principles are being tried, some of which are described in the Appendix 6A.

6.3 QUBIT DETECTION AND MEASUREMENT

Qubits can be detected by measuring their physical properties, like spin, polarization, etc. It is important to realize that these properties cannot be measured at intermediate stages of quantum computation or quantum communication because of the no-cloning theorem. The detection of final qubit state can take place only at the end of processing, and that “read out” will give the result of computation or deliver the application-specific information.

The detection mechanism depends on different approaches for quantum computing. In ion trap systems, a resonant laser light is used to scatter off the qubit. The resulting photons are collected and interpreted to identify the qubit state. Other approaches use similar methods. The detection efficiency can be improved by suppressing counts due to non-qubit processes.

There are three measurement methods to determine the quantum states of a qubit.

(i) Bell's Inequality

This, or equivalently CHSH, inequality measurement allows one to determine the presence of entanglement in the prepared state. The *S*-parameter measurement distinguishes between local hidden variable theories and quantum mechanics. The range $2 < S \leq 2\sqrt{2}$ signifies an entangled state.

(ii) Bell State Measurement (BSM)

The unknown state is projected on the maximally entangled states (also called Bell states). For a two-particle qubit state, this means that the state is projected on the basis of the Hilbert space of four Bell states.

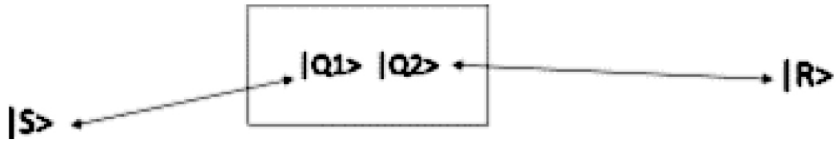
(iii) Quantum State Tomography

In this method, one measures the matrix elements of the full density matrix of the unknown quantum state. For a *d*-dimensional entangled qubit state, d^2-1 measurements are needed. For a two particle qubit, the density matrix is a 4×4 matrix, which means that we have to make 15 measurements to completely specify the unknown state. Similarly a three particle state needs 63 measurements. It can be easily seen that for more complicated states, the number of needed measurements becomes very large very soon. In general, methods of statistical analysis like maximum likelihood estimation are used to arrive at good estimates of the density matrix elements.

6.4 QUANTUM REPEATER (QR)

Free space or optical fiber limit the physical distance for transmission of quantum states. In free space,the limit is governed by attenuation due to inverse-square law, and in optical fiber, there are other physical processes which degrade the signal quality. In classical communications, this problem is solved by using amplifiers which remove the noise and retransmit the information. This is not possible in quantum communication due to no-cloning theorem. We recall that the degraded quantum signal will become useless as soon as it is measured for clean-up and restoration.

The idea of QR is a way around this limitation. The steps for QR operation are:



(i) Using physical techniques like SPDC, an entangled qubit pair is created by the sender who keeps one copy |S>. Another copy $|Q_1>$) is sent to the quantum repeater.

(ii) A second entangled qubit pair is created at the QR. One copy called $|Q_2>$) is retained at QR but another one called |R> is sent to the receiver. Note that at this stage, QR has two qubits which are parts of separate entanglement pairs.

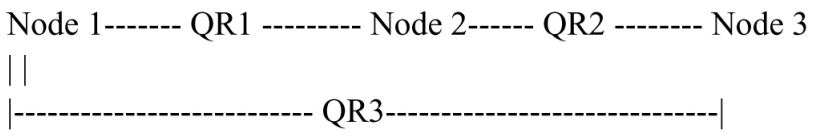
(iii) A Bell state measurement is performed at the QR so that qubits $|Q_1>$ and $|Q_2>$ become entangled. This can be accomplished by using linear optic elements like beam splitters, mirrors, etc. In this way, the quantum information in the first qubit pair is transferred to the second pair. In principle, the process can be repeated indefinitely across a chain of repeaters and so the range can be extended.

In practical terms, a working QR will need many components, many of which are still under development. Processes of entanglement swapping, purification, and distillation are also utilized in QR.

6.5 DISTRIBUTED QUANTUM NODES

There is no standard scheme of OSI-like layers for QCNs at this time. It is also not known if that framework is sufficient or needs to be replaced. New approaches like software defined networking (SDN) for network control and programming are under intense investigation. In limited application domain, like that of quantum cryptography, some scaled down QCN has been realized.

A basic framework for a 3-node distributed quantum network separated in space can be visualized as in the following.



The QRs are needed for exchanging qubit state information among the nodes. It is very straight forward to generalize this topology to higher number of nodes but it becomes very difficult to realize in practice. If it is possible to put the node and QR together in one box, then it may be easier to enlarge this kind of network.

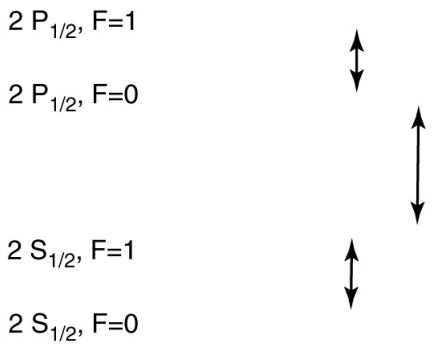
APPENDIX 6A: STATIONARY QUBIT SOURCE TECHNOLOGIES

As mentioned earlier, stationary qubits are very important for quantum computing. They are confined to very small spaces and undergo different quantum control operations depending on the algorithms involved. At the same time, they can be considered as intermediate steps in quantum communication before being converted to flying qubits. Some of the many different physical methods are described below.

(i) Trapped Ions

Atoms in ground state have electrons organized in allowed orbits called shells, which surround a tiny nucleus made out of protons and neutrons. The number of electrons is the same as that of protons in the nucleus, and so the total charge is zero. Such atoms are called neutral atoms. When they are involved in collisions and other kinds of interactions, they acquire extra electrons and become negatively charged. They may also lose electrons and become positively charged. These entities are called negative or positive ions. Many such ions have discovered by researchers over the years. Some of them, like $^{9}Be^{+}$ and $^{171}Rb^{+}$, have been found to have energy levels such that they can be used as qubits.

Let us look at the energy level diagram of $^{171}Rb+$ ion near ground state.



The hyperfine interaction of inner-shell electrons with nucleus splits the energy levels slightly. The new levels are indicated by the quantum number *F*. The next energy level is separated by 369.5 nm photon energy gap. In principle, there are two kinds of qubits possible in this ion.

- Hyperfine qubits are formed using the two lowest levels with $F = 0$ and $F = 1$ quantum numbers.
- Optical qubits include the ground state ($F = 0$) and the next excited state with $F = 0$.

Both qubits have their own challenges. As the name suggests, optical qubits are formed using optical frequency lasers. When a laser of that wavelength is applied, the electron absorbs that energy and is transferred to a higher energy state. The lower level can thus represent the state |0> and the higher |1>. The ion can thus represent a qubit with proper application of laser.

Now, one needs a stable source of qubits and the positively charged ions need to be trapped somehow. They cannot be trapped by just using static electromagnetic fields according to Earnshaw's theorem. Paul and Dehmelt (Physics Nobel prize winners of 1989) discovered that supplementing them with an oscillating and rotating radio frequency field leads to a trapping potential in three dimensions. One of the simplest traps of this kind is the Paul trap in which atomic ions are kept in place using a clever combination of static magnetic field and oscillating electric field. The qubits are formed using laser pulses which entangle the electronic energy levels of the ions. The laser

induced changes in the physical qubits correspond to various unitary transformations of the logical qubits.

Trapped ions are one of the most promising candidates for quantum computing as they represent stationary qubits. For quantum communication, those qubits need to be transferred to photons to make them flying qubits. This is a very active area of research.

(ii) Trapped Neutral Atoms

Energy levels of some atoms contain hyperfine states. They arise due to the interaction between spin of the nucleus and orbital angular momentum of the electron. For purposes of generating qubits, one chooses neutral atoms in which the energy difference between these levels is quite small. Additionally, one has to make sure that these states do not decay to lower states. Laser beams are used to excite the atoms to the hyperfine states. Neutral atom traps are also special configurations of electromagnetic field known as optical lattices. They hold neutral atoms in place through atomic dipoles interaction.

(iii) Josephson Junction

There is no rule that qubits must be formed from microscopic objects like photons, atoms, or ions. It was realized early on that macroscopic systems like quantum integrated circuits can be also used for this purpose. In particular, Josephson tunnel junctions are a very good alternative.

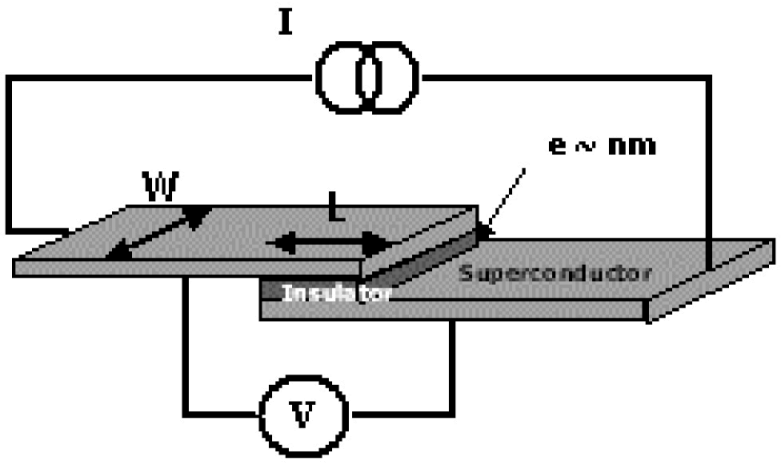


Figure 6.1. Schematic of a Josephson junction (source: www-inst.eecs.berkeley.edu/~cs191/projectreports/Superconductors.doc)

Josephson junction is a nonlinear device made from a thin insulating metal oxide layer sandwiched between superconducting metal electrodes. It has been found that Aluminum (Al) and its oxide Alumina (Al_2O_3) are ideal for this purpose. The whole setup is cooled down to temperature below 1K using cooling equipment like dilution refrigerators. In presence of a voltage source, a current flows through the junction due to quantum tunneling and is nondissipative due to superconductivity. The resulting energy states are such that there is a large separation between them and so the junction can be used as a qubit. Configuration changes can be used to generate three different kinds of qubits related to phase, flux, and charge.

The nonlinear junction current can be modeled as,

$$I(t) = I_0 \sin[\frac{2\pi}{\Phi_0}\Phi(t)]. \qquad (6.2)$$

The current and flux are related nonlinearly as expressed by the sine function. It should be contrasted with the usual linear relation,

$$I(t) = [I_0 \frac{2\pi}{\Phi_0}]\Phi(t). \qquad (6.3)$$

The universal flux quantum is related to Planck's constant and electrical charge,

$$\Phi_0 = \frac{h}{2e}. \qquad (6.4)$$

Three different types of quantum circuits can be realized depending on how the circuit parameters are controlled. These are known as Cooper pair box, the RF-SQUID, and current-biased junction.

The energy levels of the Josephson junction are such that the lowest levels are sufficiently separated from the higher ones and thus can be used for qubits. In that case, the photons from the controlling laser light induce transition just between two lowest levels needed for qubit formation.

Due to the macroscopic nature of the superconducting qubits, the fluctuations in control parameters due to fabrication process need to be taken into account. One drawback of these qubits is the need for very low temperatures.

(iv) Quantum Dots (QD)

QD are nano-scale version of semiconductors and they exhibit quantum properties like energy levels. They can be modified to have a predefined energy level structure to emit desired wavelengths of light. Their quantum properties lie somewhere between those of bulk semiconductors and those of molecules. Their quantum properties originate from Excitons, which are bound electron-hole systems. They can be engineered as one, two, or three-dimensional systems and then known as QD, quantum wires, or quantum wells.

Qubits can be realized by the spin states of extra electron in a QD. Currently, they are mostly used for realization of quantum logic gates needed for quantum computing. It is not difficult to also use them for quantum communication.

(v) NV Centers (Diamond Lattice with Nitrogen Vacancies)

Diamond lattice is a regular arrangement of carbon atoms in a hexagonal lattice. Lattices can have many possible types of defects. One of them is lattice vacancy, which is the absence of a required carbon atom at a lattice site. If the nearest carbon atom to the vacancy is then substituted by a nitrogen atom, an NV center is created. Such a pair has well separated energy levels which can be manipulated by optical and microwave radiation. They can be also used to create entangled qubits at room temperature. NV centers are generated by irradiating diamond by light or particle beams. Nitrogen can be inserted by a particle beam.

REFERENCES

Bell, J.S. 1964. “On the Einstein Podolsky Rosen Paradox.” *Physics* 1, no. 3, pp. 195–200.

Bennett, C.H. and G. Brassard. 1984. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175, New York, NY: IEEE, p. 8.

Einstein, A., B. Podolsky, and N. Rosen. 1935. “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” *Physical Review* 47, no. 10,pp.777–780.

Ekert, A.K. 1991. “Quantum Cryptography Based on Bell’s Theorem.” *Physical Review Letters* 67, pp. 661–663.

Facchi, P., D.A. Lidar, and S. Pascazio. 2004. “Unification of Dynamical Decoupling and the Quantum Zeno Effect.”*Physical Review A* 69, no. 3, p. 032314.

Holevo, A.S.1973. “Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel.”*Problems of Information Transmission* 9, pp. 177–183.

Rényi, A.1961. “On measures of information and entropy.”*Proceedings of the fourth Berkeley Symposium on Mathematics, Statistics and Probability, 1960.* Berkeley, CA: University of California Press, pp. 547–561.

Schumacher, B. 1995. “Quantum Coding.” *Physical Review A* 51, pp. 2738–2747.

Schumacher, B., and M.D. Westmoreland. 1997. “Sending Classical Information Via Noisy Quantum Channels.” *Physical Review A* 56, pp. 131–138.

Shannon, C.E. 1948. “A Mathematical Theory of Communication.” *Bell System Technical Journal* 27, pp.379–423, 623–656.

Stone, J.V. 2015. *Information Theory: A Tutorial Introduction*. Sheffield, England: Sebtel Press.

Wootters, W.,and W. Zurek. 1982. “A Single Quantum Cannot Be Cloned.” *Nature* 299, pp. 802–803.

INDEX

OTHER TITLES IN OUR COMMUNICATIONS AND SIGNAL PROCESSING COLLECTION

Orlando Baiocchi, University of Washington, Tacoma, *Editor*

Elements of Algebraic Coding Systems by Valdemar Cardoso da Rocha

Information Theory by Marcelo S. Alencar

Probability Theory by Marcelo Sampaio de Alencar and Raphael Tavares de Alencar

Momentum Press is one of the leading book publishers in the fi eld of engineering, mathematics, health, and applied sciences. Momentum Press offers over 30 collections, including Aerospace, Biomedical, Civil, Environmental, Nanomaterials, Geotechnical, and many others.

Momentum Press is actively seeking collection editors as well as authors. For more information about becoming an MP author or collection editor, please visit http://www.momentumpress.net/contact

---

• free trials

The **Momentum Press** digital library is very affordable, with no obligation to buy in future years.

For more information, please visit **www.momentumpress.net/library** or to set up a trial in the US, please contact **mpsales@globalepress.com**.

An Introduction to Quantum Communication

Vinod K. Mishra

Quantum mechanics is the most successful theory for describing the micro-world of photons, atoms, and their aggregates and is behind much of the successes of the modern technology. It has deep philosophical implications to the fundamental nature of material reality. A few decades ago it was also realized that it is connected to the computer science and information theory. With this understanding was born the new disciplines of quantum computing and quantum communication.

This book introduces the very exciting area of quantum communication which lies at the intersection of quantum mechanics, information theory, and atomic physics. The relevant concepts of these disciplines are explained and their implication for the task of unbreakably secure communication is elucidated. Mathematical formulation of various approaches are explained and attempt has been made to keep the exposition self-contained.

Vinod K. Mishra received his PhD in physics from State University of New York (SUNY) at Stony Brook. His area of focus was in theoretical nuclear physics. He was a post-doctoral researcher at various universities and research institutions before joining Lucent Technology Bell Labs. He worked on projects in many areas of optical and wireless networking. Later he joined Defense Information Systems Agency (DISA) focusing on advanced networking technologies. Currently he is a team leader at US Army Research Laboratory (ARL) conducting research in software defined networking, dynamic optical networking, and quantum communication. Outside of work his interests lie in travel, music, languages, and reading.

MOMENTUM PRESS
ENGINEERING

ISBN 978-1-60650-556-4
90000
9 781606 505564