Quantum Information, Algorithms and ProtocolsQuantum Information, Algorithms and Protocols A Textbook for Computer Science and Engineering

Students

A Textbook for Computer Science and Engineering Students

First Edition

Yuan John Jiang
City, Country

Self Publishers Worldwide

This book was typeset using LaTeX software.

Preface

Quantum computing and communication are hot topics. Software development kits (SDKs) including IBM Qiskit and Google Cirq have been made available to software engineers. However, quantum algorithms and protocols have been described as mysterious and incomprehensible – requiring software and communication engineers to take a graduate course in quantum physics to understand them. In reality, quantum physics is about waves at the minuscule scale, in which they cannot be divided smaller. The principles of using waves have already been established by existing theories on communication and optical computing. The quantum algorithms and protocols are easy to understand when explained in the framework of these theories. Applying the principles of the theories, software and communication engineers may even be able to invent new quantum algorithms and protocols.

Table of Contents

Chapter 1

Introduction

The advantage of quantum computing lies in the possibility of parallel computing. The use of quantum communication has been in key distribution.

1.1 The power of parallel computing

Maze problems are hard because there are too many paths to explore from the entrance to the exit. If changing the question of the problems from pinpointing the actual paths to finding the number of good paths, although seemingly dumb down, the challenge is as hard as the original. One still needs to explore all the possible paths to reach the conclusion.

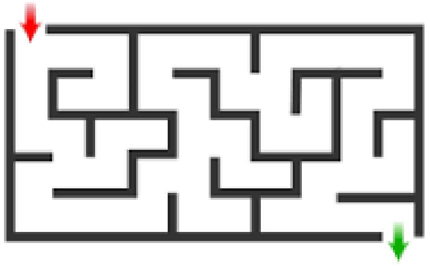

Figure 1.1: Maze

Computer scientists have long known parallel computing is the way to speed up solutions to such problems. But how to realize parallel computing needs the help of physicists. Indeed, a physicist would suggest the following experiment to attack the problem: run water into the entrance and observe what's coming out of the exit. If we see water out of the exit, we know the maze has at least one good path. Of course, this is not the ultimate answer. But at least it shows the power of using water for parallel exploration.

We can obtain more information if we explore the water experiment further: put one big drop of water into the entrance and observe how many drops of water coming out. If three drops coming out of the exit, we can conclude that the maze has at least three good paths. We can also conclude the relative lengths of the paths by measuring the time delays of the three drops assuming water runs through all the paths at the same speed. One problem left is whether we can determine for sure that each of the three drops corresponds to one or more paths. Water is not good medium to reach precise solutions.

From the above water experiment, to build a parallel computer, a medium must possess the following characteristics:

- it must be able to spread and to explore all possible solutions
- it must have one or more parameters, such as the time delay of a water drop, that can carry information
- it can be broken up into one or more smallest drops.

Many media possess the first two characteristics. But only quantum waves possess all three.

1.2 The quantum power

Quantum physics tells us that all waves have their smallest drops – the quanta, which cannot be divided further. This is the so-called particle nature of waves. Quantum physics also says that all matters including electrons and protons are waves. Physicists refer the two concepts as the particle and wave dual-natures of matters. They are the essence of quantum physics. Their truthfulness are proven all the physics experiments plain or wonderful. They are behind the power of quantum computing and communication.

The first hint of quantum power for parallel computing came by the proposal of Deutsch's algorithm[1] although the shock of the power did not come until the publication of Shor's algorithm in 1997. The hint of quantum application to secure communication came a year early in 1984 by the publication of the BB84 protocol[2]. The fact that the smallest drop of a quantum wave cannot be divided prevents it from being partially tapped for eavesdropping.

1.2.1 The particle nature

To most people, particles have the image of point-like things with negligible sizes. This image excludes the wave nature from the picture and cause all the misunderstandings when learning quantum physics. The particle nature really refers to the fact that all matters have the smallest drops when measured by their energy, mass or charge. For electrons and protons, measuring their mass or charge shows the smallest drops. For lights or electromagnetic waves, measuring their energy shows the smallest drops, and each drop is called a photon. Through out this book, we avoid using the mis-leading term particle and use ”quantum” to refer to the smallest drop of photons, electrons and protons.

The quantum nature of waves gives us the precision needed for parallel computing. But on the other hand, a quantum of a wave can only be measured once. A measurement requires energy to be extracted from the wave to the measurement device. And the phase, the conjugate variable of energy, becomes uncertain, and any information carried by it is lost forever.

1.2.2 The wave nature

When talking about waves, we often visualize ripples in a lake or the surges in oceans and seas. We observe water being pushed up and then pulled down by gravity. When we shake one end of a string as show in Fig. 1.2, we also see the vibration of each section of the string and the propagation of the vibration. Our perception of a wave includes something vibrating and the vibration propagating. But can we consider the vibration of a guitar string a wave? Indeed, we can. The reason we don’t perceive the vibration propagating is because it gets reflected back by the two fixed ends of the string. Therefore, propagation or spatial spread remains a defining characteristic of waves, even if their propagation or spread is constrained.

Quantum computing and communication use only electromagnetic waves and electron waves, whose vibrations are not visible as a wave of a string. But they behave similarly.

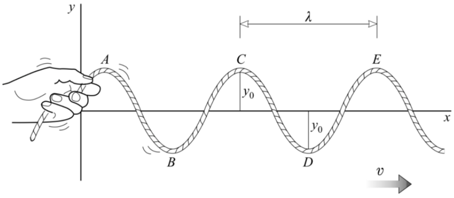

Figure 1.2: Wave arisen from shaking or vibrating one end of a string.

Types of waves by propagating characteristics

Radio-frequency (RF) electromagnetic waves are used for mobile communications including Wi-Fi. They can spread to everywhere if not being blocked by reflective matters. Light waves – electromagnetic waves with wavelength ranging from sub-micron to a few microns – are used for optical communications. They can be channeled by optical waveguides such as optical fibers to explore different paths. They are confined in two dimensions – the lateral dimensions – but propagate in the dimension along the axes of the waveguides or fibers.

Quantum communication can use only propagating waves, of course. But some of them may also be used in quantum computing.

If a wave is confined in three dimensions, e.g. an electromagnetic wave in a microwave oven, the wave cannot propagate anywhere other than being reflected back and forth. Only standing waves of specific frequencies can exist within such confinements. The allowed frequencies are discrete. Standing waves are good for storing information. Superconductor qubits are built by standing waves of electrons as we will discuss below. Standing waves may be best visualized and understood by the vibrations of a guitar string. When we pluck a string, the propagation of the vibrations are stopped and reflected by the two fixed ends. Only the waves whose phases coincide after a complete round trip of reflection survive while the other waves cancel each other and die off.

Another type of waves, which we may call trapped waves, are not confined with clear boundaries but are trapped by forces extending to infinity. Electrons in an atom are trapped waves by the electric force of the nucleus' positive charges. The waves extend to infinity but are concentrated within a nanometer around the nucleus. Trapped waves are also good for storing information. Trapped-ion qubits are built by trapped electron waves.

Information representation by wave characteristics

Fig. 1.2 shows several characteristics of a wave including its period, amplitude and phase. Shown but not labeled in the figure is the polarization of the vibration, which is in the y direction and is perpendicular to the propagation direction. Vibration is a periodic motion, and in the time dimension, can be characterized by frequency and phase. Fig. 1.3 shows the period (the inverse of the frequency), phase and amplitude of a sinusoidal vibration when depicted in the time dimension. All these characteristics wavelength, amplitude, frequency, period and polarization can be modulated to represent information. But wavelength, frequency and period are related, and only frequency is used for modulation.

In radio wave communication, which includes mobile or cellphone communication we use everyday, the modulation of frequency, phase, and amplitude serves as the primary methods for information representation. In optical communication, combination of polarization and phase modulation is mostly used. In subsequent sections, we will find that quantum devices use all of them and others for information modulation.

Information is represented by numbers, which can in turn mapped to the parameters of waves such as their amplitudes, frequencies, phases and polarizations. For guided waves, modes are another useful wave parameter.

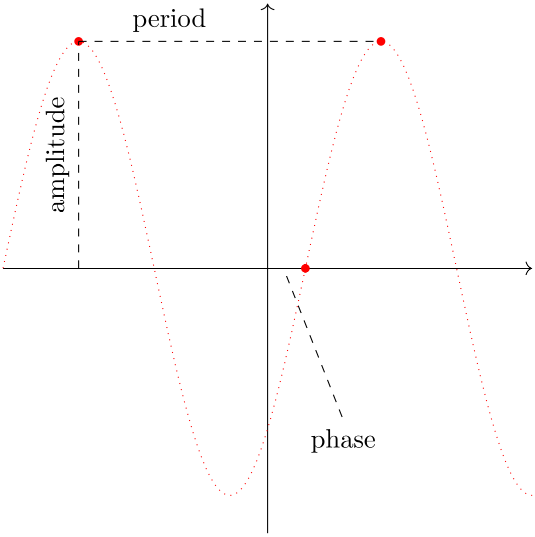

Figure 1.3: Characteristics of wave vibration

The quantum nature of waves

Optical waveguide quantum computing chip

If we take a look at the Xanadu.ai M-8 quantum computing chip, we see it very much ressembles a maze. The optical waveguides are the paths that light waves traverse. Its couplers and splitters ressemble the junctions of maze. A coupler merge two light paths into one, and a splitter split one into two. The chip has 8 entrances and 8 exits and can build 8^8 possible paths.

Quantum physics tells us that all matters are waves and in addition, they all have the smallest drops, which cannot be divided finer when measured in their energy or mass. A wave, like water, can spread in space and propagate in time through all possible paths and give us the power of parallel computing. The drop-like behavior gives us the needed precision. Physicists refer the drop-like behavior the particle nature of matters. But the term particle unavoidably suggests minuscule in size and clarity in trajectory, and leads to avoidable puzzles and paradoxes with waves' spread in space and propagation in time. We should imagine or interpret electrons and electromagnetic waves like water drops: they can spread in space and propagate in time, may be subjected to constraints such as reflective objects, but show the smallest drops when measured by energy or mass.

1.3 Quantum measurement

The quantum nature is not shown until a wave is measured. The concept is simple, but leads to profound differences between measure a quantum wave and a classical wave. The most profound difference is that one quantum of a wave can only be measured once. After measurement, the quantum of wave is no longer the same as it once was. This is the so-called Bohr quantum collapse theory. Another difference is the possible values of measurement are limited to the eigen-values, which may be a concept foreign to engineering students. The differences are natural results of von Neumann's projection theory of measurement – a highly abstract mathematical theory. To engineers, however, quantum measurement may be better understood as demodulation and resonance as described in the next chapter.

1.4 Quantum circuits and programming

When implementing the algorithms and protocols in software, we first draw out them as quantum circuit diagrams. Our software programs would call out qubits for input and output as well as the gates for processing according to the circuit diagrams. Qubit stands for quantum bit. For quantum computing, a qubit is the data memory device that typically stores a bit of information to be processed. The storage medium is a drop of wave, and the device includes hardware that contain the wave. For quantum communication, a qubit is the channel uses one drop of wave to carry one bit of information. It is no difference from a radio wave or optical wave communication channel except it uses one drop of wave at a time. Appendix 8 explains the physics behind the construct and operation principles of several types of qubit devices. In Chapter 3 on quantum information, we will revise the notion that a qubit can stores or carries only one-bit of information. Before that, we will stay with the qubit definition implied by its name and repeated in literature.

Conventional computers have no resemblance to quantum computers. Even before the appearance of modern computer, the not widely known subject of optical computing has explored the parallel computing capability of optical waves with Fourier transformation. But its application is limited and has not become a subject of learning by many. On the other hand, quantum devices have much in common with radio and optical communication devices because they all work with waves. Radio-wave communication including mobile communication and Wi-Fi is the dominating way for everyone connecting to the wired world. Mobile devices already take advantage of waves' parallel exploration capability for transmitters and receivers to find each other. The backbone of the wired world, on the other hand, is all optical fibers. The knowledge of wave communication reaches more engineering students than quantum physics and is most relevant not only to quantum communication but also to quantum computing. This chapter reviews some of the relevant subjects of communication theories especially on modulation before delving into the following chapters on the specifics of quantum communication and computing.

At the top level, a communication system has an information sender, a channel and a receiver. The sender contains modulators that transfer information in the form of numbers to characteristics of waves and send the waves to the channel. The receiver has demodulators that translate wave characteristics back to information. In a quantum system, the modulators and demodulators are quantum gates. The information bits carried in a quantum channel are called qubits – short for quantum bits.

An ideal channel maintains the form and shape of the waves so that no information is lost. The equivalent in a computing system is a memory device, which receives bits of information from a writer and conveys them to the reader. Channels and memory devices, which work with quantum waves, are all qubit devices and may often be loosely referred as qubits.

Quantum gates are modulators and demodulators, and are not the same as transistor gates in a conventional computer. They convert information from one form of wave to another. A circuit of quantum gates would turn a maze of data (information) to an obvious form for easy extraction and achieve the task of computation. Or a circuit can turn the data (information) to an obscure form and achieve the task of secure communication.

When we talk about quantum computers, we should understand that we don't have entire computers made of all quantum devices. They will only have some chips or co-processors be replaced by chips of integrated circuits of quantum devices. Even our conventional computers have graphic processor units (GPU) in addition to the central processing units (CPU) to help speed up the processing of video display data.

Chapter 2

Using waves to represent information

2.1 Waves and modulation

2.2 Information, numbers and modulation

When we get our blood pressure measured in a doctor's office, the height of the mercury in a glass column represents the information of our blood pressure. The height of mercury in the column is what we actually measure and is what we use the height of a mercury in a cylinder to represent the information of our blood pressure. We see that physical characteristics, which can be measured in numbers, can be used to represent information. Information theory assumes all information can be presented as numbers. In turn, engineers and physicists use physical characteristics that can be measured in numbers to represent the information. The whole process is Information -¿ Numbers -¿ Wave characteristics. The first step is called encoding, and the second step is modulation.

In the study of communication, modulation is the subject devoted to how information or numbers being represented by physical characteristics of waves. The wealth of knowledge can be applied to not only quantum communication protocols but also to quantum computing.

Radio broadcasts first used radio waves' amplitudes to represent the volume of one's voice. This is the so called amplitude modulation (AM). Later, fre-

Table 2.1: Information represented by physical characteristics

Information	Represented numbers	Physical characteristics
Blood pressure	real number	height of mercury in a cylinder
Picture	pixel 0 or 1	Radio wave phase and amplitude (QAM)

quency modulation (FM) was found less prone to noise in the airways. That is why we now have both AM and FM on the panels of our radios. Modern communication also use phase modulation (PM) and quadrature amplitude modulation (QAM), which is a combination of phase and amplitude modulation.

Quantum devices, working with the smallest drops of waves, typically use two wave characteristics in their modulation scheme. Understanding how modulation works in quantum devices is the critical link for engineers to understand quantum technologies.

2.2.1 Phase modulation

Phase modulation uses a carrier wave's phase to represent information. By varying the phase while keep the wave's frequency and amplitude constant, the real numbers in the $[0, 2\pi)$ domain can be represented. In communication textbooks, we use the points in constellation diagrams to depict the amplitudes and phases of waves – the distance of a point to the origin is the amplitude of the wave, and the angle to the x-axis ϕ is the phase. So, the numbers that PM can represent fall all onto a circle in a constellation diagram as in Fig. 2.1. Communication textbooks refer the numbers symbols. The range or set of the symbol is called the symbol constellation or symbol set. For example, the symbol constellation of PM in set notation is $phiin[0, 2\pi)$. (Constellation diagrams are most useful for understanding QAMs, in which both amplitudes and phases are used to represent information.)

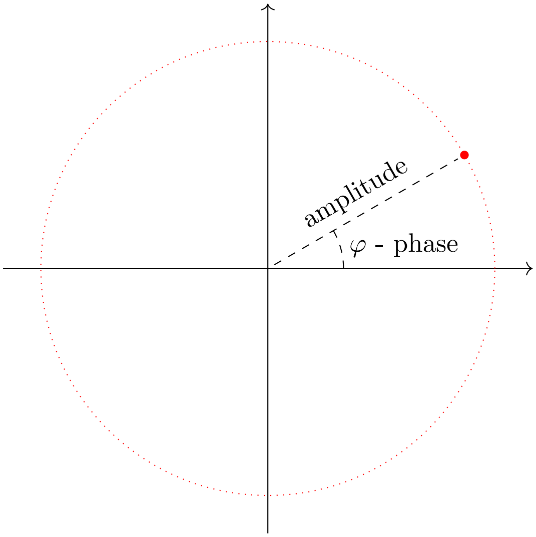

Figure 2.1: Constellation diagram of phase modulation

2.2.2 Digital modulation

In theory, we can measure a wave's amplitude, frequency and phase precisely and use them to represent real numbers. In really, communication channels and information processing devices have noises and errors. We are best to have the systems working with only integer numbers. Using integer numbers to represent information is what we call digital technology. Further, using binary integers instead of decimals makes computer and communication components much simpler. And nowadays digital technology is almost the synonym of binary technology. Technologies of dealing with real numbers are called analog technologies.

All computers use digital technology if we ignore the history of the slide rule calculators. Even abacuses are digital calculators. Communication systems are slow to convert to digital technology. For a long time, communication was mostly about voice communication – radio broadcast and telephones – and used analog technologies. For digital information, modulations such as AM, FM and PM often carry different names, e.g. amplitude-shift keying (ASK), frequency-shift keying (FSK) and phase-shift keying respectively (PSK).

2.2.3 Channel capacity and Hartley's law

Channel capacity measures the maximum possible bits per second of a communication channel. When modulation is the only limitation, Hartley's law gives the channel capacity to be

$$C = flnM \tag{2.1}$$

where f being the channel used rate and M being the number of modulation points.

2.3 Quadrature phase-shift keying

Quadrature phase-shift keying (QPSK) uses carrier waves of phases 90 degree apart, for example of phases 0, 90, 180, 270 degrees, to represent 2-bit numbers – 0, 1, 10, or 11 in binary. A wave with 90 degree phase is called the quadrature wave while the wave with zero phase is called the in-phase wave. (The significance of using waves with phases 90 degree apart is that every two waves of such phase difference are orthogonal to each other. Therefore, when receiving a wave of phase 180 degree representing "10", which has zero measurement overlap with waves of 90 or 270 degree phases, and has zero probability of being demodulated as "1" or "11". waves are orthogonal to each other. Measurement of orthogonal waves is least prone to noise or errors because they have zero overlap.)

The constellation diagram is shown in the diagram in 2.2.

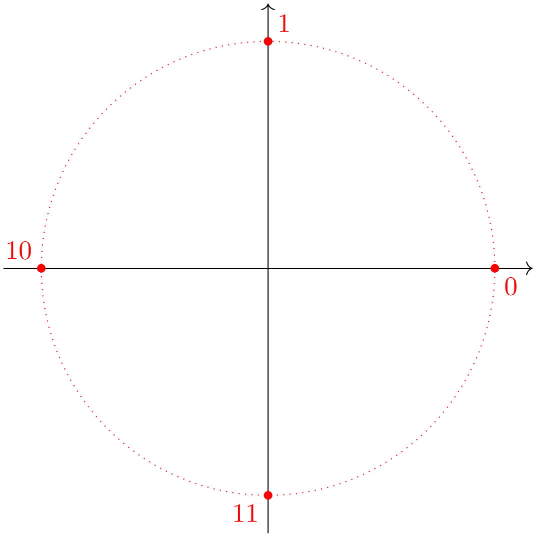

Figure 2.2: QPSK constellation diagram

2.3.1 Symmetric QPSK

For simpler modulator circuitry, the QPSK modulation scheme shown in the constellation diagram Fig. 2.3 is more widely used in practice.

2.3.2 Modulator, demodulator and superposition

A practical QPSK modulator circuit is shown in Fig. 2.4. It uses one carrier wave generator and splits the carrier wave into two waves of equal amplitudes. One of the half becomes the quadrature wave after a 90-degree phase shifter while the other half remains as the in-phase wave. modified scheme: in every time slot, 2 bits are fed into the modulator. Each bit is used to modulate a base carrier wave's phase. The two base carrier waves are orthogonal, one of zero phase and the other of 90-degree in phase. If the input to a carrier is "0", its phase is shifted another 180 degrees. The combined or summed up wave of the two carriers is the output of the modulator going into the communication channel. The constellation diagram this scheme is shown in Fig. 2.2.

We see that one wave from the source can be divided up into two waves, which can then be combined into one after modulation. In fact, all waves can be combined into one and may be regarded as one wave if they are coherent with each other – their phases are correlated. Combination, mixing or composing several waves into one is the same concept as superposition in quantum physics although the latter refers to combination, mixing or composition of waves with equal number of drops.

Figure 2.5 shows a demomulator circuit, which reverses the modulation: the received signal wave is divided into two waves to be resonated with two local oscillators, which are from the same local source but are orthogonal to each other. The the proportions of the two resonations determine the phase angle of the incoming wave. Bit numbers are output according to the phase angle.

2.4 Quadrature amplitude modulation

Quadrature amplitude modulation (QAM) is a combination of amplitude modulation and phase modulation. Modern radio communication such as Wi-Fi and mobile communications all use the digital forms of QAMs.

2.5 Polarization modulation

Polarization modulation is used in optical fiber communication. For example, dual polarization quadrature phase shift keying (DP-QPSK) modulation is a widely used.

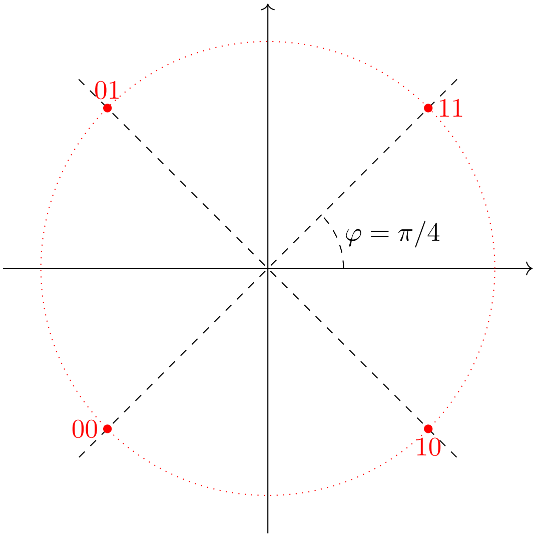

Figure 2.3: Practical QPSK constellation diagram

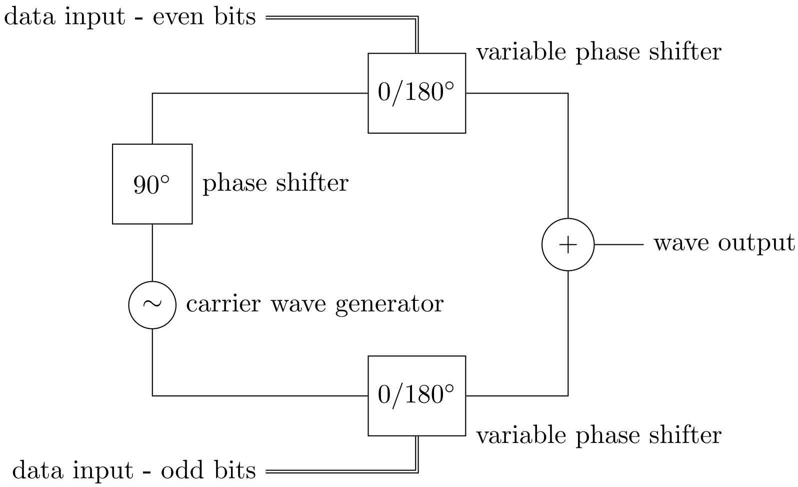

Figure 2.4: QPSK modulator circuit

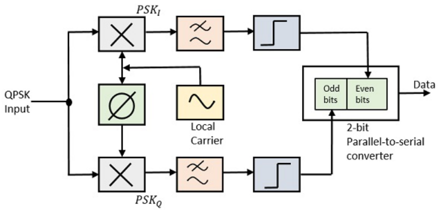

Figure 2.5: QPSK demodulator circuit

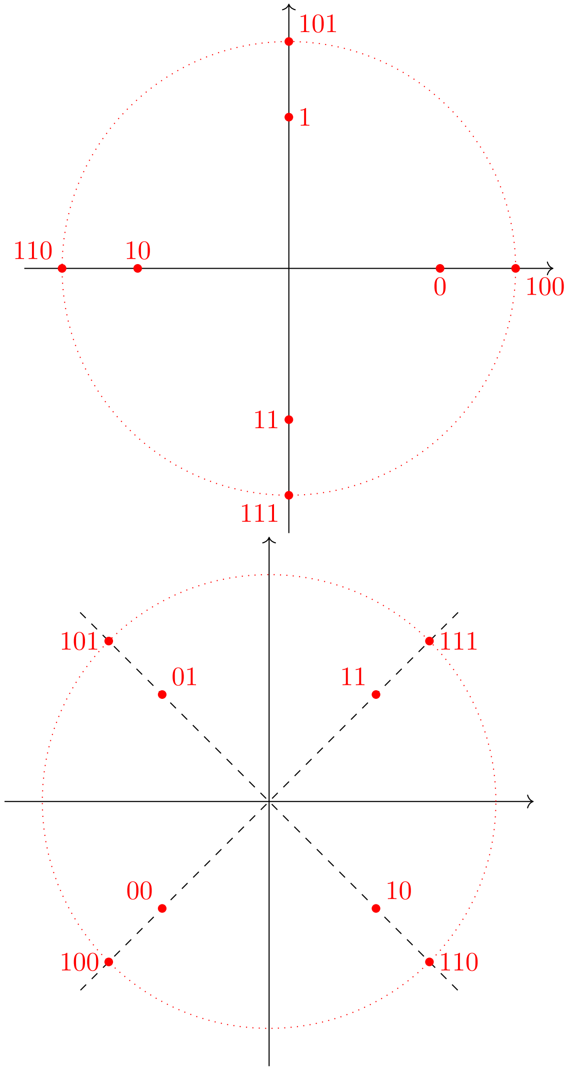

Figure 2.6: Constellation diagrams of two 8QAM systems

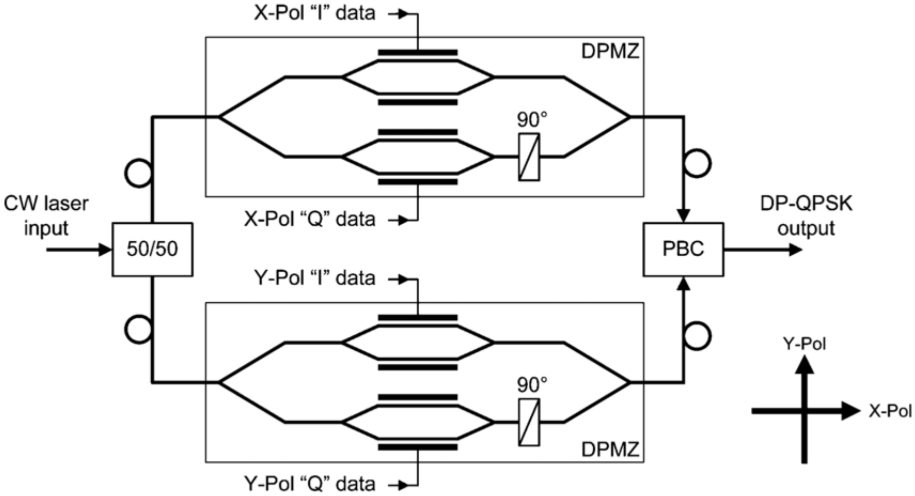

Figure 2.7: DP-QPSK modulator

Chapter 3

Quantum information

3.1 Quantum concepts

For engineers, only two concepts of quantum physics are needed: 1. all matters are waves even the seemingly size-less electrons and protons are; 2. all waves have their smallest drops, which cannot be divided. Physicists refer the two concepts the partical and wave duality of matters. The first concept tells us that, not limited to radio and optical waves, electrons and protons can also be used to make qubits. However, the implication of the second concept is far more profound and is not explored by traditional communication theory:

- Analog AM is not possible because amplitude depends on the number of drops in the wave and can only be use for digital modulation.
- Each qubit can only be measured once. In disregard how many bits of information are modulated into a qubit, only one bit at most can be demodulated from a qubit.

3.1.1 Measurement and limit on channel capacity

When measuring a wave's mass or energy, we find it in a discrete number – 1, 2, ..., or n – of a unit mass or energy. The one with 1 unit is the smallest drop of course. The amplitude is usually proportional to the square root of the mass or energy and takes only discrete values although not exactly 1, 2, ... or n.

When we have a wave of n drops, we can divide it up to n drops for separate measurements. But with measurement of each drop, the drop of the wave is changed or even disappears. A drop of an electromagnetic wave is called a photon. When measuring a photon, its energy is transferred to an electron, and the movement or change in the electron of charge induce an electrical current observable to humans. The photon cannot be divided and disappears after its whole energy is transferred to an electron. The unique feature of quantum information is that we can modulate a qubit device as much information as the cardinal of real numbers but that we can only extract at most one bit of information when measuring it.

3.1.2 Quantum terminology

By tradition, physicists keep on using the term particle, which may cause the biggest confusion. To most people, particles have the image of point like or of negligible sizes. Physicists believed electrons were point-like in size when JJ Thomson discovered them in 1897. But when Ernest Rutherford discovered atomic nucleus 14 years later, people raised the question: why is the size of an atom much bigger than that of its nucleus? Why wouldn't the tiny negatively charged electrons fall into the positively charged nucleus and be combined into an atom close to the size of the nucleus – if it were to happen, we would have not seen the world as we have.

Physicists refer the drop-like behavior of electrons and all other matters as the particle behavior. "Quantum" should have been the perfect word in place of particle, but we think "drop" is a better word for non-physicists to understand.

Beside particle, physicists use the term "state" to refer the wave of one drop. It is the same concept as "mode" in the context of optical communication and photonics. It is used to describe a wave when the absolute amplitude value is known or unimportant. But the term carries many different meanings to engineers. We will believe it's wise to use the term "wave" in place of state. By tradition, physicists use the so-called Dirac "bra-ket" notation to label quantum states. In the ket notation, the base carrier waves are noted as $|0\rangle$ and $|1\rangle$.

When talking about electrons being waves, people are often puzzled and ask what is vibrating in an electron wave. Physicists are puzzled too and have been debating the possibilities without conclusion. Engineers don't have to interject into the debate and need only know that an electron wave qubit has frequency, phase and polarization for modulating.

3.2 Qubit modulation

3.2.1 Requirements on modulation

We have two conflicting requirements when considering how to modulate a qubit:

- For parallel computing/exploration, the modulation code space should be as large as possible.

- For output, demodulated codes are limited to binary "0" and "1".

The first requirement is easy to understand, and analog PM, with symbol set $\phi in[0, 2\pi)$, meets the requirement. The second requirement is due to that fact that one qubit has only one drop wave, which resonates with only one of the local oscillators in the demodulator as shown in Fig. 2.5 and never both.

As described in the Appendix on qubit devices, all devices add polarization modulation or the like to meet the second requirement. (That's because polarization demodulation is easier than phase demodulation.) Polarization modulation is widely used in optical fiber communication. But some qubit modulation schemes such as using waveguide location have never been used in communication. And communication theory has no established terms for them. In this book, we refer them with a generic term θ modulation because all of them can be characterized by an angle value $\theta in (-\pi/2, \pi/2]$ as discussed in the appendix on qubit devices.

3.2.2 Digital modulation

For output

To read out from a qubit, it must be in a binary modulation. Similar to QPSK shown in Fig. 3.1, we use the angles $\theta = 0$ and $\pi/2$ to represent "0" and "1" respectively as shown in the constellation diagram Fig. 2.2

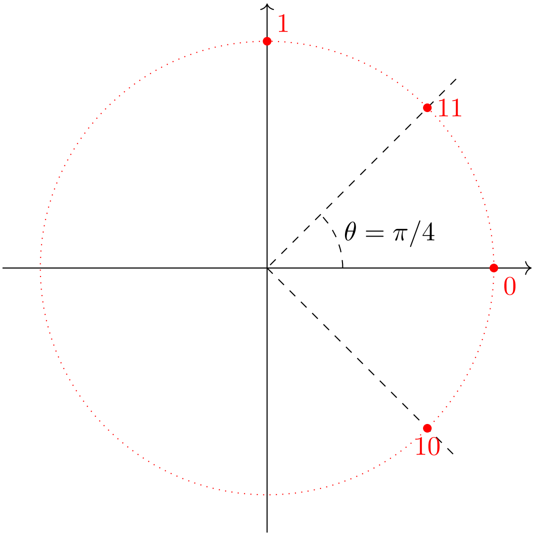

Figure 3.1: Constenlation diagram of quantum θ shift keying

For input

At the input stage of a circuit, we can also use the $\theta = \pi/4 and - \pi/4$ code points. They are called the Bell states by physicists. As we will learn in latter chapters, these waves can be used for parallel computing because each of them is a mixture or superposition of both he "0"ed "1" waves. For quantum communication, they encode the binary numbers "11" and "10", and are used as encrypted code points of one-time pad encryption.

Quadrature amplitude modulation

Since a wave is in drops, 1, 2, 3, ..., or n drops, its amplitude is discrete too although not in increment of 1, 2, 3, ..., or n. Adding amplitude modulation is by adding more qubits and can be used only for digital modulation. Amplitude modulation is always used to add code points for digital modulation and cannot be used for parallel computing.

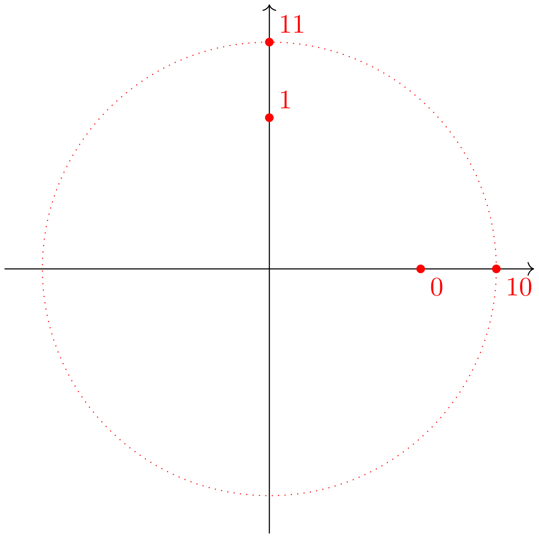

Figure 3.2: Constellation diagrams of two qubits

(Ignore - If we consider the relative amplitude A and phase ϕ of the two waves in a qubit, they can represent all the real number pairs in the rectangle $A \in [0,1], phi \in [0,2\pi)$. Physicists like to represent the relative amplitude as $cos\theta$, and therefore, the (θ,ϕ) pair can represent all the real number pairs in the rectangle $[0,\pi],[0,2\pi)$. This rectangle can also be represented as a Bloch sphere.

3.2.3 Analog modulation

Analog modulation can only be used at input or in processing. For communication, each qubit actually has two channels – θ and φ. And their channel capacities per qubit duty cycle are $\theta in(-\pi/2,\pi/2] and \varphi in[0,\pi)$. For computing, that is the capacities are the amount of information a qubit can store.

3.2.4 Demodulation and quantum measurement

When a cellphone receives a radio wave, the demodulator can divide the wave into many portions to measure the amplitudes and phases. But with a qubit,

Table 3.1: Wave characteristics for qubit modulation

Wave parameters	Represented numbers	Qubit design
Amplitude	Number of qubits 1, 2, ...	all qubits
Phase	$\varphi \in (-\pi/2, \pi/2]$	all qubits
Frequency	$\theta \in (-\pi/2, \pi/2]$	SC-IBM, Google; trapped ion - IonQ
Mode	$\theta \in (-\pi/2, \pi/2]$	Xanadu, PsiQuantum
Polarization	$\theta \in (-\pi/2, \pi/2]$	USTC
Spin	$\theta \in (-\pi/2, \pi/2]$	

although we can adopt any of the modulation technique and put information in any of the data points (θ, φ), we cannot divide one drop of wave for multiple measurement.

Similar to a demodulator of QPSK. a demodulator of a qubit expose the drop of wave to two electronic resonators orthogonal to each other. If we know the qubit is modulated by BQSK, detecting the qubit in the $|0\rangle$ wave means the qubit's phase $\theta = 0$. Further, the absence of detecting signal in the $|1\rangle$ wave also suggests $\theta = 0$ too. But if the qubit is originally modulated in any other way, we have no way of measuring the knowing the information that the qubit represents. the probability of one resonator responds to the wave depends on how much the resontor overlaps with the wave in space and time.

In contrast to conventional communication and computing systems, information entered into a quibit may be lost at demodulation or measurement. That is the unique feature of quantum information.

3.2.5 Wave characteristics for qubit modulation

3.3 Mathematical notation of qubit modulation

From communication theory perspective, a qubit is best described by the parameter pair (θ, φ). But other notations developed by physicists may be easier to use when working on problems involving more than one qubit.

3.3.1 Ket notation

Summing up the base carriers, the superposition wave can be noted as $|s\rangle = cos\theta|0\rangle + e^{i\varphi}sin\theta|1\rangle$ or simply $|s\rangle = a|0\rangle + b|1\rangle$. Here, the + sign means wave addition but has no mathematical meaning. And a and b are complex numbers and reflect the amplitude and phase contributions to the superposition. Even with the constraint $|a|^2 + |b|^2$, this notation includes waves $e^{i\lambda}(cos\theta|0\rangle + e^{i\varphi}sin\theta)$ which are the same except their global phase λ.

3.3.2 Vector notation

For mathematicians and computer scientists, the physical meaning of wave addition can be ignored, and the vector notation $\begin{pmatrix} a \\ b \end{pmatrix}$ is best for derivation and calculation.

But not all of the 4 real numbers the two complex numbers can be used independently for modulation. First, the amplitude of the wave is one to be sure that the qubit contains only one drop $|a|^2 + |b|^2 = 1$.

$$\begin{pmatrix} cos\theta & -e^{i\lambda} sin\theta \\ e^{i\varphi} sin\theta & e^{i(\varphi+\lambda)} cos\theta \end{pmatrix} \tag{3.1}$$

Any operation rotates the data point of a qubit on the Bloch sphere and can be described by the triplet of Euler angles, $\delta\theta, \delta\varphi, \delta\lambda$. The matrix notation is

$$\begin{pmatrix} cos\delta\theta & -e^{i\delta\lambda} sin\delta\theta \\ e^{i\delta\varphi} sin\delta\theta & e^{i\delta\varphi+\delta\lambda} cos\theta \end{pmatrix} \tag{3.2}$$

3.3.3 Binary numbers

If we measure waves in any other way than space or time, we find their smallest "drops" – the particle nature of matter. Quantum physics started a hundred years ago when Einstein first proposed that electromagnetic waves, when measured in their energy, have the smallest drops called photons.

When measuring in electric charge, physicists discovered the smallest drops first and call them electrons before they realized their wave nature.

Measurement is the very thing that the quantum world is different from the classical world. In the quantum world, with an article, you only have one chance to measure it.)

Digital technologies gain precision over analog technologies but lose in the amount of information they can carry. The amount of information that a modulation technique can carry relates to the size or cardinality of the set of numbers that it can represent. With analog PM, the cardinality of the set $[0,\ 2\pi)$ is infinity and is the same as the entire set of real numbers. But the set of integers that a digital modulation represent is finite. And the amount of information that a digital communication channel carries per time slot is finite. To increase the communication speed, the cellphone industry has been trying to squeeze more and more information per time slot by adopting increased data points of QAM modulations – 4QAM, 8QAM, 16QAM .... From the above description of the various types of qubits, we see that they all have the pseudo phase θ_p to characterize the orthogonality or overlap among the waves in the polarization, spatial or frequency domains, and can be used represent real numbers in the $\{\theta_p \in [0, \pi/2)\}$ domain. In addition, the relative phase in the time domain of the two base carrier waves in a qubit is another independent variable that can be. Physicists usually use $\theta_q = \theta_p/2|0\rangle$ and the Bloch sphere as in Fig. 3.3 to

Table 3.2: Parameters and ranges for modulation

Parameter	Represented numbers	Note
Amplitude	Number of qubits $\in \{1, 2, 3, ...\}$	None
Phase	$\varphi \in (-\pi/2, \pi/2]$	Z gate
Polarization angle (spatial overlap)	$\theta \in (-\pi/2, \pi/2]$	X gate

draw an intuitive picture of the entire modulation domain of a qubit $\{\theta_q \in [0, \pi]$ and $\phi \in [0, 2\pi)\}$.

3.4 Graphical depictions

3.4.1 Quarter sphere diagram

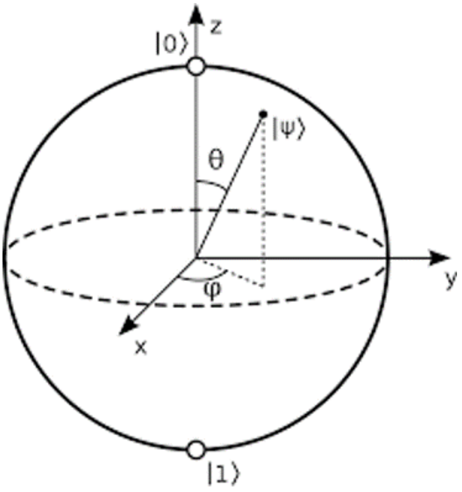

Figure 3.3: Bloch sphere

3.4.2 Bloch sphere

3.4.3 Constellation diagrams

Constellation diagrams are familiar to engineers and are great graphical illustration of modulations involving only phase and amplitude. But quantum devices add θ modulation.

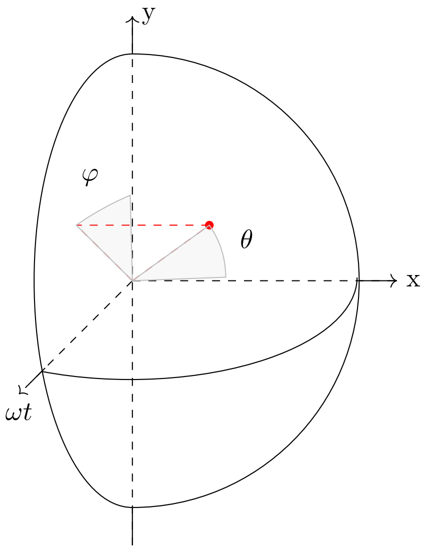

Figure 3.4: Qubit modulation space

3.5 Quantum gates for information processing

Qubits are memory devices or communication channels. Quantum gates are processing devices that can change the modulation of θ and phase φ. As desired by the algorithms, the gates are concatenated or connected into circuits. Amplitude or the number of qubits is never changed until demodulation when qubits are measured. Measurements absorb the energy of qubits to extract digital data from them.

In the ket notation developed by physicists, a qubit gate operation is a quantum operator and can be noted by a letter G. In vector notation, a gate process can always be represented by a matrix. For example,

$$\begin{pmatrix} cos\theta & e^{i\varphi}sin\theta \\ e^{-i\varphi}sin\theta & cos\theta \end{pmatrix} \tag{3.3}$$

which is unitary. A algorithm or protocol is always depicted by a circuit diagram or series of matrix calculations. In circuit diagram, a qubit is shown as a line, and a gate as a rectangle.

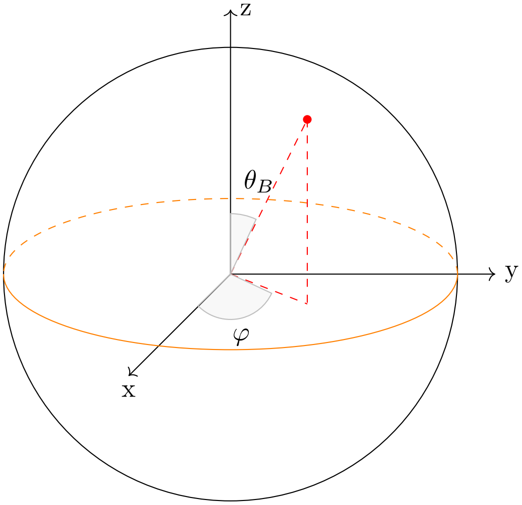

Figure 3.5: Bloch sphere

Chapter 4

Single-qubit operations

4.1 Hadamard gate

Hadamard gate rotates the polarization θ of a qubit by 45 degrees. Its circuit symbol is letter "H" enclosed in a square. Rotating a $|0\rangle$ qubit 45 degrees obvious becomes a qubit of 45 degree polarization.

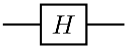

Figure 4.1: Hadamard gate

4.2 Pauli X, Y and Z gates

A Z rotates a qubit's phase φ by 180° or π. A X gate exchanges $|0\rangle$ and $|1\rangle$. A Y gate exchanges $|0\rangle$ and $|1\rangle$ with additional phase change. They are best expressed in the vector notation as the Pauli matrices:

$$\begin{aligned} \sigma_1 &= \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_2 &= \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_3 &= \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{4.1}$$

4.3 Mostly used modulation points

4.3.1 $|1\rangle$

$|1\rangle$ is one of the base waves of a qubit. However, quantum computing circuit diagrams usually assume all input waves are $|0\rangle$, and assume a $|1\rangle$ wave being transformed by an X gate from a $|0\rangle$ wave – $|1\rangle = X|0\rangle$ – in ket notation. In vector notation, the X gate has a matrix representation

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4.2}$$

In circuit notation, The X gate can also be represented as $\bigoplus$. But in this book,

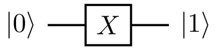

Figure 4.2: Use X gate to produce $|1\rangle$ wave.

we do not use this notation.

We see that an X gate flips the bases $|0\rangle$ and $|1\rangle$ from one to another.

4.3.2 $|+\rangle$ wave

The $|+\rangle$ wave is a superposition wave of the $|0\rangle$ and $|1\rangle$ waves and is best used as the input wave for parallel processing.

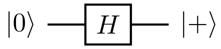

Figure 4.3: Use H gate to produce $|+\rangle$ wave.

4.3.3 $|-\rangle$ wave

The $|-\rangle$ wave is also a superposition wave of the $|0\rangle$ and $|1\rangle$ waves, but is mostly used as the input wave phase kickback algorithm, which will be described in the following chapter.

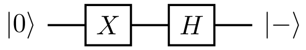

Figure 4.4: Use H gate to produce $|-\rangle$ wave.

4.4 Introducing Deutsch's algorithm

A one-bit function f mapping {0,1} - {0,1} can have 4 possible outputs, which are 2 bits of information. But the outputs belong to 2 categories, constant or balanced, which are an 1-bit information as of $f(1) + f(0)$. We can't obtain the 2-bit information using one operation but can obtain the 1-bit information if we feed the function with the $|+\rangle$ qubit:

$$F(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{1}{\sqrt{2}}(|f(0)\rangle + |f(1)\rangle) \tag{4.3}$$

From above derivation, we see that it takes one operation of the F gate to evaluate both $f(0)$ and $f(1)$. But the result still requires two measurements, one to determine $f(0)$ and the other to determine $f(1) - f(0)$. For two measurements, we need the help of another qubits.

4.5 BB84 protocol

Encryption is used in everyday Internet communication. Encryption conceals the credit card numbers and passwords, which we send to the websites, from hackers or adversaries, who can eavesdrop the communication channels. One of the communication encryption protocols is called one-time-pad (OTP) encryption, which is ideal in theory but is impractical. Charles Bennett and Gilles Brassard proposed in 1984 a quantum version of the protocol and improved its practicality. The improved version is called the BB84 protocol[2].

Named after the inventors Charles Bennett and Gilles Brassard, BB84 protocol secures communication from eavesdropping. If the quantum channel carries one quntum bit at a time made up by one drop of wave. The drop cannot be divided for wire-tapping. Although an eavesdropper can intercept the quantum bits and try to reproduce or clone them for re-transmitting to the receiver, the reproduction or cloning fail 50 percent of the time. So, the BB84 protocol secures communication completely against eavesdropping although it is not secure against some other attacks.

4.5.1 The OTP protocol

By tradition, all communication encryption protocol is narrated as the scenario that Alice wants to transmit a series of data bits to Bob but fears Eve may eavesdrop the communication channel[3]. The OTP protocol goes like - Alice has a second series of random bits of equal length, which is the encryption key. - Alice pairs one bit from each series, calculates the XOR of each of the bit pairs, and sends each of the XOR results to Bob at a time lot. - Bob also has the same series of key bits. Upon receiving the bit of each of the XOR results from Alice, Bob XOR it with the corresponding bit from the key bit series in his possession to decrypt the corresponding data bit.

4.5.2 Key distribution

The OTP protocol is one of the symmetric encryption algorithms. It is the only hundred percent secure algorithm, and there is no way to break it even using brute force. But it is not practical because the encryption key needs to be equally long as the data message. It is a chicken and egg dilemma: how does Alice shares or distribute the series of secret key bits to Bob at the first place? Conventional public key exchange protocols are the current solutions to the chicken and egg problem. But they have many other problems. Among them is that the conventional protocols are computationally expansive and can only be used for key exchanges of short key length. BB84 protocol and the quantum protocols following it do not depend on expansive computation. They recognize the fact that keys are random numbers. And key sharing can afford to lose some candidate key bits and does not require all candidate key bits being exchanged or shared between Alice and Bob. Alice can distribute all the candidate key bits to Bob. And Bob and Alice only need to agree on which of the candidate bits are "good" to use.

BB84 modifies the OTP protocol for key distribution in the following way: - Instead of calculating the XOR of bit pair, Alice concatenates the pair into two-bits binary number 00, 01, 10, or 11, and send it to Bob in the quantum channel (the qubit) encoded according to the constellation diagram 3.1. Anyone who measures the qubit and gets a result of "0" cannot distinguish the actual code point is "00" or "10". So the original data is encrypted. - Bob does not have the key bits that Alice uses but has a series of key bits out of his random generation. And Bob demodulates each received qubit using his key bit and obtain a data candidate bit, i.e. if the key bit is "0", he measures the received qubit using base "0"; if the key bit is "1", he measures the received qubit using base "11". - Alice and Bob then use the conventional communication channel to compare their corresponding key bits. If they agree, Alice and Bob keeps the candidate data bit. Otherwise, the candidate bit is discarded.

With many of the original data bits from Alice being discarded, what is good of BB84? The good part is that the kept data bits can be used as the key for future encryption. Therefore, BB84 is considered a quantum key distribution protocol. The quantum channel guarantees that it cannot be tapped. But it cannot prevent an eavesdropper Eve from intercepting the qubits in the channel. Eve may intercept the qubits without sending anything to Bob and may also attempt to reproduce the qubit to send to Bob. Because of the non-cloning theory, Eve cannot reproduce the qubit to disguise the interception. So, key distribution with BB84 guarantees keys' confidentiality and integrity although the rate of key transmission may suffer from interception.

4.5.3 Circuit diagram

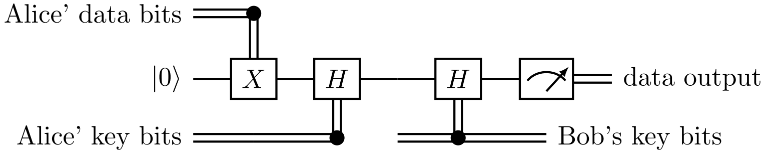

Figure 4.5: BB84 circuit

4.5.4 Performance

Channels: one. Input Processing: Output processing: Transmission rate: one bit per qubit duty cycle.

Chapter 5

2-qubit operations

In conventional computers, 8, 16 or 32 bits are joined together to a unit of one byte, word or UINT32. Quantum circuits have their ways to join qubits into new units. If we look into 2 waveguide qubits, we see 4 waveguides, which we can label as V_0, V_1, W_0 and W_1. If we join the first two, we can make a superposition wave $a|0\rangle_V + b|1\rangle_V$ and allow only one drop of wave in it. If we join the first and the third, physicists may call the new unit a joint wave while we keep the tradition of this book to call it a joint wave. Physicists note the new unit as $|0\rangle_V|0\rangle_W$ or simply $|0\rangle|0\rangle$. For quantum computing and communication, we allow two drops in the joint wave.

5.1 Control gates

Assume $f(x)$ is a binary function mapping $x \in 0, 1$ to $0, 1$. The control-f gate takes input waves $|x\rangle|y\rangle$, where x and y are either 0 or 1, and produce the output waves as shown below. A particularly important type of control gates is the control-NOT or C-NOT gates, in which the f is the Pauli X. A C-NOT gate is best described in vector notation as matrix

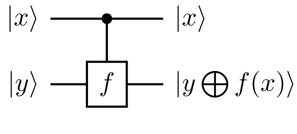

Figure 5.1: Control-f gate

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{5.1}$$

5.2 Mostly used modulation points

5.2.1 The bases

From 4 orthogonal waves, we have 4 joint waves $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ and $|1\rangle|1\rangle$, which are also orthogonal waves. We can use them as the base waves to represent 2-bit binary numbers 00, 01, 10 and 11. It's impossible to draw any 4-dimensional object using the 4 orthogonal base waves. But the constellation of QAM modulation diagram in Fig. 3.2 shows to some extend the phase relation among the base waves except that two pairs of the waves in QPSK are 180-degree different in phase instead of orthogonal.

5.2.2 Evenly mixed waves

In ket notation, the wave of two qubits can be written as $a|0\rangle|0\rangle + b|0\rangle|1\rangle + c|1\rangle|0\rangle + d|1\rangle|1\rangle$. In vector notation, they are $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$.

One useful digital input is the superposition of all the base waves:

$$|s >= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) \tag{5.2}$$

which can be used to compute in parallel.

5.2.3 Bell states

Like in the cases of one qubit and QPSK, we can also use superpositions of the above base waves to come up with a new set of base waves:

$$\begin{array}{rl} |BES1 >= & \frac{1}{\sqrt{2}}|(|0\rangle|0\rangle + |1\rangle|1\rangle), \\ |BES2 >= & \frac{1}{\sqrt{2}}|(|0\rangle|0\rangle - |1\rangle|1\rangle), \\ |BES3 >= & \frac{1}{\sqrt{2}}|(|0\rangle|1\rangle + |1\rangle|0\rangle), \\ |BES4 >= & \frac{1}{\sqrt{2}}|(|0\rangle|1\rangle - |1\rangle|0\rangle). \end{array} \tag{5.3}$$

The second set of base waves can be considered 45 degree rotated from the first set. Physicists call them Bell state waves. They are in the form $cos\theta|B_i >$ $+sin\theta|B_j >$. They are no longer separable waves.

We can use 8 waves from the 2 sets of bases to represent numbers of 3 bits as shown in Fig. 2.6.

5.3 Design patterns

5.3.1 Producing Bell states

Changing the input waves from $|+\rangle$ to $|-\rangle$ or from $|0\rangle$ to $|1\rangle$, we can obtain the other Bell states.

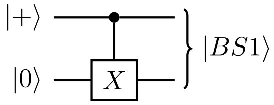

Figure 5.2: Producing Bell states

5.3.2 Phase kick back

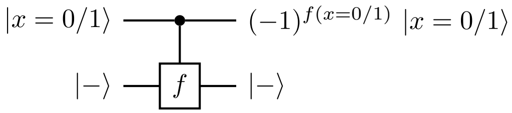

Figure 5.3: Producing Bell states

With the help of a C-NOT gate, the 2 bits of information modulated in one qubit can be transfered to two qubits and therefore can be all extracted.

5.4 The output of Deutsch's algorithm

With the help of a C-NOT gate, the 2 bits of information modulated in one qubit can be transfered to two qubits and therefore can be all extracted.

5.4.1 Circuit diagram

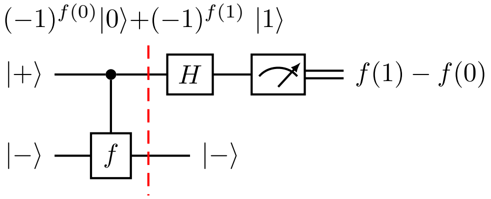

Figure 5.4: Deutsch's algorithm circuit

5.4.2 Performance

Processing: two quantum gates - one operation per gate; one measurement. Memory: one qubit for the processing. But for output, two qubits are required.

Table 5.1: Modulate one qubit to encode 2 bits

Digital input	Modulating operation	gate
00	None	None
01	90*degree*	Z gate
10	Mirror switch $\|0\rangle$ and $\|1\rangle$	X gate
11	Mirror switch $\|0\rangle$ and $\|1\rangle$ and 90*degree*	X gate

5.5 Superdense coding

Superdense coding is also called dense coding. With the consideration of two qubits as one wave, modulation of one qubit is modulating the shared θ of the entanged wave. The modulation appears to be upon one qubit. But the information is actually coded into two qubits.

The operation first creates entanglement $|BES1>$.

5.5.1 Circuit diagram

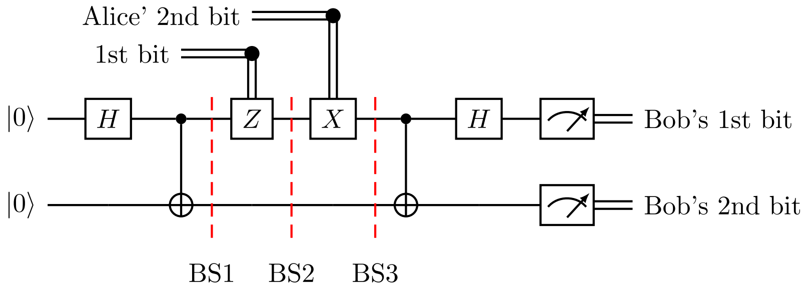

Figure 5.5: Superdense coding circuit

5.5.2 Entanglement and measurement

5.6 Teleportation

Similar to dense coding, quantum teleportation is to modulate an analog signal to one qubit of a $|BS1>$ two-qubit wave. The analog signal comes in the form of a qubit, which we call it the signal qubit. And the wave may be written as $a|0\rangle + b|1\rangle$.

$$\begin{aligned} & (a|0\rangle + b|1\rangle)\tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \\ = \quad & \tfrac{1}{\sqrt{2}}|(|0\rangle|0\rangle + |1\rangle|1\rangle)(a|0\rangle + b|1\rangle) \\ + \quad & \tfrac{1}{\sqrt{2}}|(|0\rangle|0\rangle - |1\rangle|1\rangle)(a|0\rangle - b|1\rangle) \\ + \quad & \tfrac{1}{\sqrt{2}}|(|0\rangle|1\rangle + |1\rangle|0\rangle)(a|0\rangle + b|1\rangle) \\ + \quad & \tfrac{1}{\sqrt{2}}|(|0\rangle|1\rangle - |1\rangle|0\rangle)(a|0\rangle - b|1\rangle) \end{aligned} \tag{5.4}$$

Table 5.2: Modulate one qubit to encode 2 bits

Alice's output $d_1 d_0$	Bob's qubit
00	$a\|0\rangle + b\|1\rangle$
01	$a\|1\rangle + b\|0\rangle$
10	$a\|0\rangle - b\|1\rangle$
11	$a\|1\rangle - b\|0\rangle$

Alice has a qbit with information S and shares a pair of qbits with Bob. The pair is one of the 4 known eigenwaves and has information 2. The total input information is therefore S+2. At the output, Alice measures the first 2 qbits against the same 4 eigenwaves and tells Bob the result, which has information 2. If no information is lost, the information in the 3 qbit should be S.

5.6.1 Circuit diagram

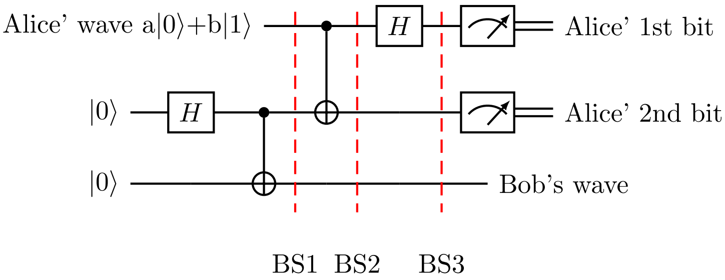

Figure 5.6: Teleportation circuit

5.7 Quantum secure direct communication (QSDC)

QSDC is an adaptation of quantum teleportation to key distribution. The key transmission rate is 1 bit per qubit duty cycle and is a much improvement over the BB84 protocol.

Chapter 6

n-qubit operations

6.1 Mostly used modulation points

6.1.1 Measurement bases

The measurement base waves are $|x_0\rangle|x_1\rangle|x_2\rangle...|x_{n-1}\rangle = \prod_{i=0}^{n-1}$, where $x_i in\{0,1\}$.

6.1.2 Evenly mixed wave and Fourier bases

Expanding on the idea of the $|+\rangle$ wave in 4.3, we can have a wave

$$\begin{aligned} |s_0\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle_0 + |1\rangle_0)\tfrac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1)...\tfrac{1}{\sqrt{2}}(|0\rangle_{n-1} + |1\rangle_{n-1}) \\ &= \tfrac{1}{2^{n/2}}(|b_0\rangle + |b_1\rangle + ... + |b_{N-1}\rangle) \end{aligned} \tag{6.1}$$

which is an evenly mixture of the n-qubit bases. But what are the orthogonal waves similar to the $|-\rangle$ of one qubit?

$$\begin{aligned} |s_k\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle_0 + |1\rangle_0)\tfrac{1}{\sqrt{2}}(|0\rangle_1 + e^{\frac{k*2\pi i}{2}}|1\rangle_1)...\tfrac{1}{\sqrt{2}}(|0\rangle_{n-1} + e^{\frac{(n-1)*2\pi i}{2}^(n-1)}|1\rangle_{n-1}) \\ ... & \\ &= \tfrac{1}{\sqrt{N}}\prod_{l=0}^{n-1}(|0\rangle_l + e^{\frac{k\times l\times 2\pi i}{2}^l}|1\rangle_l) wherek = 0,1,...N-1. \end{aligned} \tag{6.2}$$

Like the $|+\rangle$ and $|-\rangle$ waves, each of the $\{|s_k\rangle, k = 0,1,...N-1\}$ waves is a mixture of all the base waves, but they have different orientations in the N dimension Hilbert space.

6.2 Design patterns

6.2.1 Producing equal superposition

6.2.2 Quantum Fourier transform

Classical discrete Fourier transform maps a set of N complex numbers $x_0, x_1, ..., x_{N-1}$ to another N complex numbers

$$y_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_n \omega_N^{-nk}, k = 0, 1, 2, ..., N-1, \tag{6.3}$$

where $w_N = e^{\frac{2\pi i}{N}}$. For physicists and engineers, the numbers y_n help to reflect prominently the periodic patterns such as their frequency in x_n. For the same purpose, quantum Fourier transform is defined mathematically as follow but is easier to be realized by quantum gates:

$$y_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_n \omega_N^{xk}, k = 0, 1, 2, ..., N-1, \tag{6.4}$$

where $x = x_0 + x_1 2^1 + x_2 2^2 + ... + x_{N-1} 2^{N-1}$. In vector notation, F_N is a unitary matrix, and its i, j element is

$$f_{i,j} = \omega^{i \cdot j}. \tag{6.5}$$

This matrix is the same matrix as for the discrete Fourier transform. Therefore, quantum Fourier transform is equivalent to discrete Fourier transform.

Complexity

6.2.3 Phase estimation

Complexity

6.3 Grover's algorithm

Like the Deutsch's algorithm, the Grover's algorithm also assumes a blackbox function $f(x)$ whose variable x is a n-bit binary variable. Its result is a single-bit value and is always 1 except for an unknown $x = x_w$ at which $f(x_w) = -1$. The goal of the algorithm is to find x_w. This is the simplified version of many search problems. Lov Grover proposed in 1996 that quantum computer can solve it faster than conventional computers.

Let's note x_w as $w_{n-1}...w_i...w_1w_0$ in binary where $w_i = 0 or 1$, and $\vec{w} = (0, 0, ..., 1 at i = w, ..., 0)^T$ as a $2^n - 1$ dimensional vector. Using classical computers, we'd feed each of the $2^n - 1$ possible numbers of x_w at a time to f to test whether the result equals -1. The worst case is that we have to do $2^n - 1$ evaluations of $f(x)$ to find out x_w. We of course wish to explore all the possible

x_w at the same time. We naturally choose $\vec{S} = \frac{1}{\sqrt{2^n}}(1,1,...1)^T$, which is the sum of all the bases of the qubits, to feed the oracle function f.

We know, $\vec{S} = \vec{S} - \frac{1}{\sqrt{2^n}}\vec{w}) + \frac{1}{\sqrt{2^n}}\vec{w}$. Apparently, $\vec{S_1} = \vec{S} - \frac{1}{\sqrt{2^n}}\vec{w}$ is a vector orthogonal to $\vec{w}$, and applying the F gate to it does not change its phase. Therefore, $F(\vec{S}) = F(\vec{S_1}) + F(\frac{1}{\sqrt{2^n}}\vec{w}) = \vec{S_1} - \frac{1}{\sqrt{2^n}}\vec{w}$. We see that

- applying the F gate turns vector $\vec{S}$ toward $-\vec{w}$
- applying the F gate to $\vec{S_1}$ makes no change.

Therefore, can we apply F gate 2^n times and turn $\vec{S}$ completely to $-\vec{w}$? But applying F gate once more will change the phase of the $\vec{w}$ vector back. We need to change the sign of vector $\vec{w}$ first while preserving its angle with $\vec{S}$ before applying F gate again. This can be accomplished by apply gate $U_S = 2\vec{S}X\vec{S} - I$.

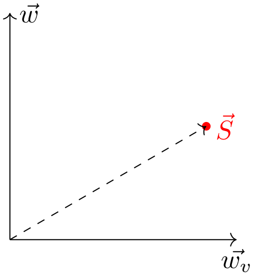

Figure 6.1: Applying F gate

6.3.1 Complexity

6.4 Simon's algorithm

The Simon's algorithm assumes a blackbox oracle function $f(x)$ whose variable x is a n-bit binary variable. Its results are m-bit values that are periodic, but the period t is unknown – $f(x+t) = (fx)$ for all x. How do we find the period t? Of course, we are tempted to play the trick again of feeding $\vec{S} = \frac{1}{\sqrt{2^n}}(1,1,...1)^T$ to the oracle function f. We have $f(\vec{S}) = \frac{1}{\sqrt{2^n}}\sum_x f(x)$.

6.4.1 Circuit diagram

6.4.2 Complexity

Using conventional computer, finding the period takes $2^{n/2}$ operations.

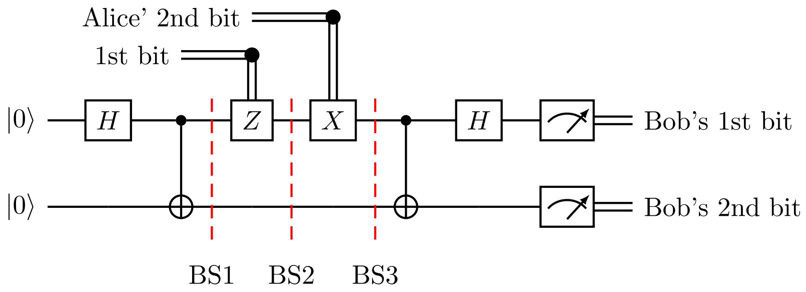

Figure 6.2: Simon's algorithm

6.5 Shor's algorithm

Much of modern day cryptography is based on the difficulty of factoring large integer numbers. Almost all Internet connections from our mobile phones and computers are based on AES, which is a private key encryption algorithm, and RSA or DH algorithms for key exchange.

For a positive integer M, how can we find out whether it has factors? A naive approach is to iterate over $a = 2, 3, ..., [M/2]$ one by one to see whether M modulo a is zero. Mathematicians have found a shortcut basing on the fact that if a pair of positive integers $a < N$ and r exist, such that $a^r = 1(modM)$, and that if they exist and r is an even number, $(a^{r/2}+1)(a^{r/2}-1) = 0(modM)$. r is called the order of a. But, beside some trivial solutions, iterating over all the possible a and r is still a daunting task. Peter Shor, in his 1997 monumental paper[4], described a quantum algorithm, which finds the existence of r and its value without iteration for every given a.

With all the design patterns, which we have learned so far, how would we design such an algorithm? We may simply extend the ideas behind the Deutsch's algorithm to the n dimension, where n is the closest integer for $M < 2^n$. 1. feed the function $f(x) = a^x(ModM)$ with the evenly mix quantum waves $|s_0\rangle$ 2. use phase kickback to transfer the values of $f(j), j \in \{0, N-1\}$, which should have periodicity of r, to the phases of the waves in the Fourier base 3. use phase estimate to reveal the information containing r.

For phase kickback to work, we need to find an eigen-waves of U_f,

$$|u\rangle = \sum_{j=0}^{r-1} c_j |a^j(modM)\rangle. \tag{6.6}$$

If we assume the eigen-values are $e^{2\pi i\frac{k}{r}}$ where $k = 0, 1, 2, ..., r-1$. We derive the corresponding eigen-waves to be

$$|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-\frac{2\pi}{r}kj} |a^j(modM)\rangle \tag{6.7}$$

However, we don't know the value of r at the first place except the trivial u_0. How can we produce any of the non-trivial eigen waves to feed the operator U_f? Fortunately, the even mixture of the eigen waves

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle = \frac{1}{r}\sum_{k=0}^{r-1}\sum_{j=0}^{r-1}e^{-\frac{2\pi}{r}kj}|a^j(modM)\rangle = \sum_{j=0}^{r-1}\delta_j,0|a^j(modM)\rangle = |1\rangle \tag{6.8}$$

is a wave that we know how to produce.

6.5.1 Circuit diagram

6.5.2 Complexity

6.6 Boson sampling algorithms

6.6.1 Complexity

Chapter 7

Noise, and error correction

7.1 Channel capacity

According to Shannon theorem, under noise, the channel capacity is $C = 2B(1+ SNR)$.

Chapter 8

Appendix: Qubit devices

8.1 Free space optical qubits and gates

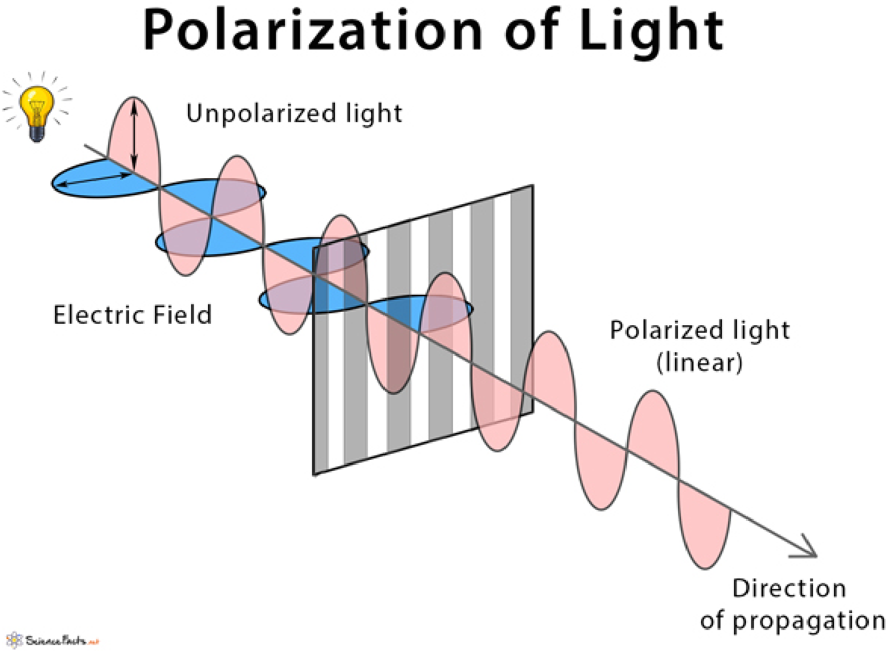

Figure 8.1: Polarization

Free space communication is mostly used for satellites to communicate with each other. There is no substance in space to degrade the power of the light wave. The receiver may as receive less power if the light beam diverge in a large angle. Laser lights are typically used. Free space communication can also be used for ship-ship communication if the distance is not too far resulting in high power loss.

Lights are propagating electromagnetic waves and obviously are best suited for communications. The vibration direction of the electric field of an electromagnet wave is its polarization. A free space optical qubit uses one optical wave of horizontal polarization to represent the binary number 0 and is thus label $|0\rangle$. It uses the one of vertical polarization to represent 1 and is labeled $|1\rangle$. The two waves have the same frequency and amplitude. They are orthogonal to each other of course. A wave of polarization angle θ_p can be considered the superposition of the two base waves: the $|0\rangle$ wave contributes $cos\theta_p$ amount in amplitude while the $|1\rangle$ wave contributes $sin\theta$.

Polarization modulation is also used in optical fiber communication. For example, dual polarization quadrature phase shift keying (DP-QPSK) modulation is a widely used.

8.2 Optical waveguide qubits and gates

Another type of qubits uses lights confined in optical waveguides or fibers. We use the optical wave in waveguide A to represent the binary number 0 and label it $|0\rangle$. We use the one in waveguide B to represent 1 and label it $|1\rangle$. The two waves have the same frequency and amplitude. They don't overlap and are of course orthogonal to each other. If we bring the two waveguides together to overlap (using an optical coupler), we get a superposition wave that is a sum of both waves. If the sum has $cos\theta$ amount in amplitude from $|0\rangle$ wave contributes and $sin\theta_p$ amount in amplitude from the $|1\rangle$ wave, we can use the value θ_p to characterize the superposition wave.

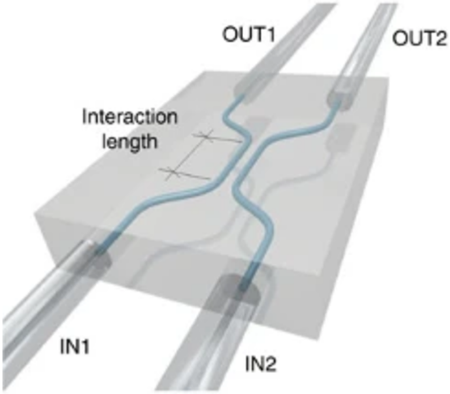

Figure 8.2: Waveguide qubit

8.3 Superconductor qubits

A superconductor transmon qubit is similar to the string of a guitar and uses the first two standing waves, which resonate at the first and second harmonic frequencies respectively, to represent the integers of ”0” and ”1”. Such a qubit is constructed by two superconductors separated by a layer of insulator. The insulator is thin enough for electrons to move (”tunnel”) back and forth from one superconductor to another without loss of energy. But traveling through the insulator leads to delays (phase delays) of the electrons. The back-and-forth movement (vibration) of the electrons between the two superconductors resonate as standing waves at periods fractions of the delay. typically, the first fundamental frequency and the first harmonic are used to represent ”0” and ”1”.

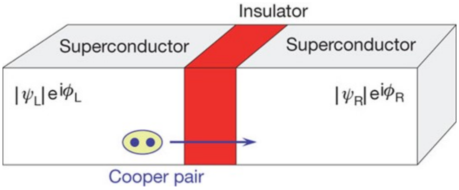

Figure 8.3: Josephson junction

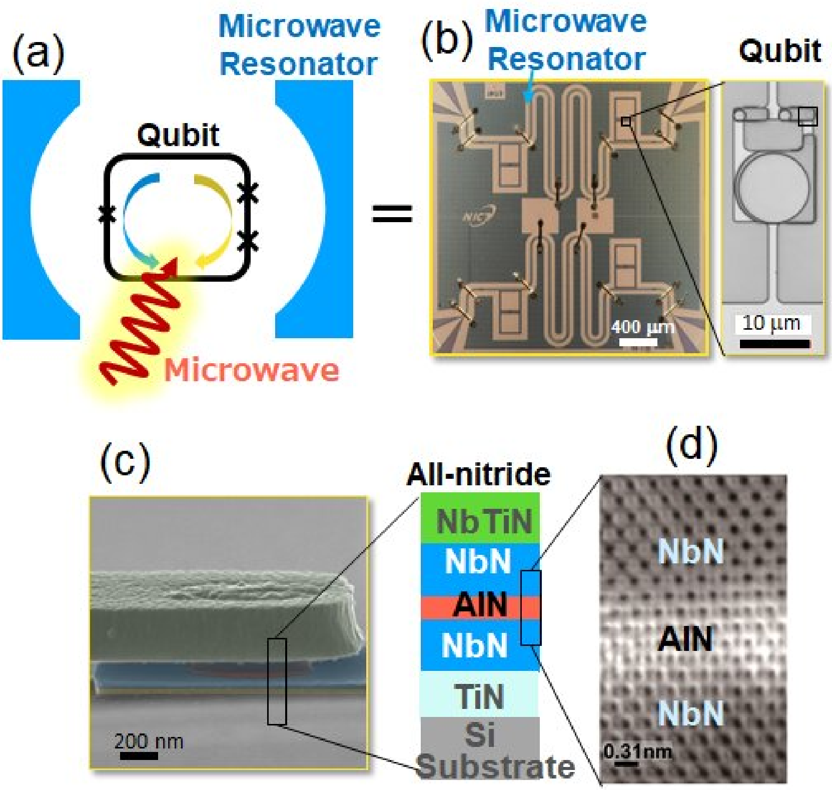

Figure 8.4: Superconductor qubits are LC resonators.

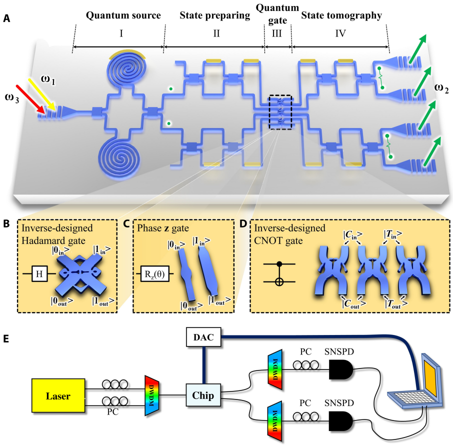

Figure 8.5: Superconductor gates.

Chapter 9

Appendix: Quantum gates

9.0.1 C-NOT gate

9.0.2 Phase kick back

9.0.3 Generator

How a qubit is put in the wave of ”0” or ”1” depends on the specific implementation. A quantum circuit diagram is usually drawn with a qubit starts in the ”0” or occasionally in the ”1” wave.

9.0.4 Hadamard gate

To modulate a qubit in the 10 or 11 wave, a $\theta_p m = 45$ degree phase shifter in the constellation diagram is needed. In the Bloch sphere, a $\theta_q = 90, \phi = 0$ phase shift is needed. Such a phase shifter is called a Hadamard gate. In the ket notation, $|11>= 1 over[\sqrt{2}](|0\rangle + |1\rangle)$ and $|10>= 1 over[\sqrt{2}](|0\rangle - |1\rangle)$. So, as a vector transformation, the Hadamard gate is a transformation matrix:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{9.1}$$

Chapter 10

Bibliography

Bibliography

[1] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London Series A*, 400(1818):97–117, July 1985.

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, dec 2014.

[3] Bruce Schneier. *Applied Cryptography.*

[4] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, oct 1997.