A **CRCPress** FREEBOOK

Quantum Computing, Communication & Information

CRC Press
Taylor & Francis Group

TABLE OF CONTENTS

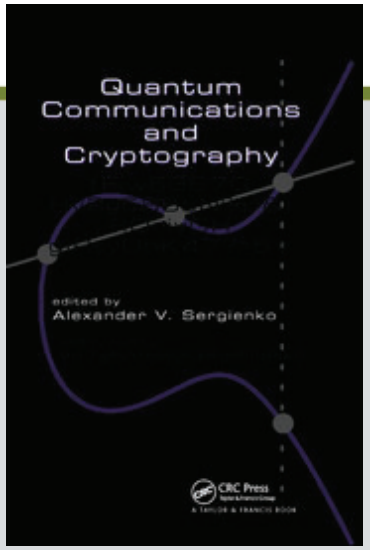
Introduction

This freebook explores cutting-edge applications in quantum communication and information. Featuring chapters from some of CRC Press' key titles, this book covers important concepts in quantum cryptography, quantum algorithms, quantum gates and circuits, and other advanced applications, including quantum teleportation, quantum games, and quantum chaos.

CHAPTER

1

QUANTUM CRYPTOGRAPHY



This chapter is excerpted from

Quantum Communications and Cryptography

by Alexander V. Sergienko

Learn more

chapter 1

Quantum Cryptography

A. Ekert
University of Cambridge

Contents

> Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve . . .
>
> — Edgar Alan Poe, "A Few Words on Secret Writing," 1841

Abstract

Quantum cryptography offers new methods of secure communication. Unlike traditional classical cryptography, which employs various mathematical techniques to restrict eavesdroppers from learning the contents of encrypted messages, quantum cryptography is focused on the physics of information. The process of sending and storing information is always carried out by physical means, for example photons in optical fibers or electrons in electric current. Eavesdropping can be viewed as measurements on a physical object — in

this case the carrier of the information. What the eavesdropper can measure, and how, depends exclusively on the laws of physics. Using quantum phenomena, we can design and implement a communication system that can always detect eavesdropping. This is because measurements on the quantum carrier of information disturb it and so leave traces. What follows is a brief overview of the quest for constructing unbreakable ciphers, from classical to quantum.

1.1 Classical Origins

Human desire to communicate secretly is at least as old as writing itself and goes back to the beginnings of civilization. Methods of secret communication were developed by many ancient societies, including those of Mesopotamia, Egypt, India, China, and Japan, but details regarding the origins of cryptology, i.e., the science and art of secure communication, remain unknown.

We know that it was the Spartans, the most warlike of the Greeks, who pioneered cryptography in Europe. Around 400 B.C. they employed a device known as the scytale (Figure 1.1). The device, used for communication between military commanders, consisted of a tapered baton around which was wrapped a spiral strip of parchment or leather containing the message. Words were then written lengthwise along the baton, one letter on each revolution of the strip. When unwrapped, the letters of the message appeared scrambled

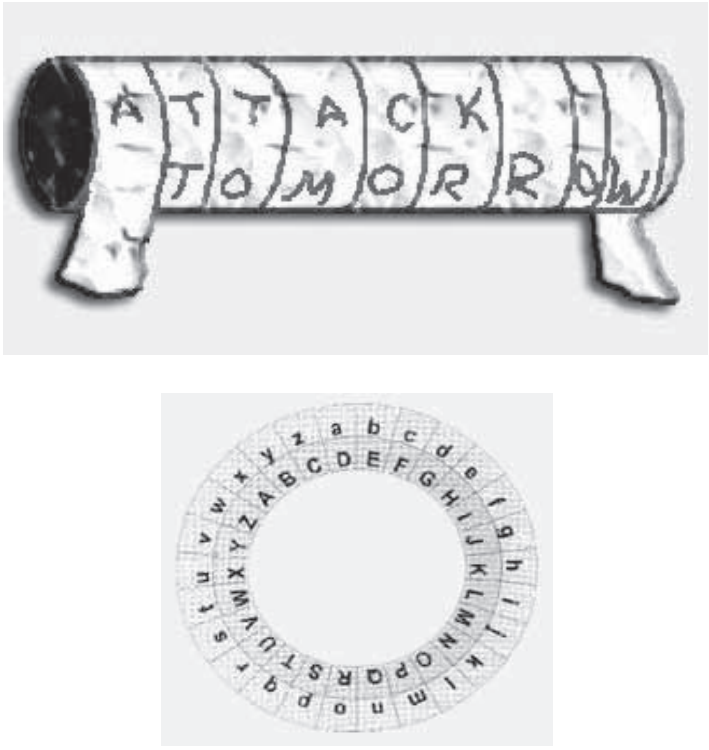


Figure 1.1 Scytale (top) and Alberti's disk (bottom) were the first cryptographic devices implementing permutations and substitutions, respectively.

and the parchment was sent on its way. The receiver wrapped the parchment around another baton of the same shape and the original message reappeared.

In his correspondence, Julius Caesar allegedly used a simple letter substitution method. Each letter of Caesar's message was replaced by the letter that followed it alphabetically by three places. The letter A was replaced by D, the letter B by E, and so on. For example, the English word COLD after the Caesar substitution appears as FROG. This method is still called the Caesar cipher, regardless of the size of the shift used for the substitution.

These two simple examples already contain the two basic methods of encryption which are still employed by cryptographers today, namely, *transposition* and *substitution*. In transposition (scytale) the letters of the *plaintext*, the technical term for the message to be transmitted, are rearranged by a special permutation. In substitution (Caesar's cipher) the letters of the plaintext are replaced by other letters, numbers or arbitrary symbols. The two techniques can be combined to produce more complex ciphers.

Simple substitution ciphers are easy to break. For example, the Caesar cipher with 25 letters admits any shift between 1 and 25, so it has 25 possible substitutions (or 26 if you allow the zero shift). One can easily try them all, one by one. The most general form of one-to-one substitution, not restricted to the shifts, can generate

$$26! \quad \text{or} \quad 403,291,461,126,605,635,584,000,000 \tag{1.1}$$

possible substitutions. And yet, ciphers based on one-to-one substitutions, also known as monoalphabetic ciphers, can be easily broken by frequency analysis. The method was proposed by the ninth-century polymath from Baghdad, Al-Kindi (800–873 A.D.), often called the philosopher of the Arabs.

Al-Kindi noticed that if a letter in a message is replaced with a different letter or symbol then the new letter will take on all the characteristics of the original one. A simple substitution cipher cannot disguise certain features of the message, such as the relative frequencies of the different characters. Take the English language: the letter E is the most common letter, accounting for 12.7% of all letters, followed by T (9.0%), then A (8.2%) and so on. This means that if E is replaced by a symbol X, then X will account for roughly 13% of symbols in the concealed message, thus one can work out that X actually represents E. Then we look for the second most frequent character in the concealed message and identify it with the letter T, and so on. If the concealed message is sufficiently long then it is possible to reveal its content simply by analyzing the frequency of the characters.

1.2 *Le Chiffre Indéchiffrable*

In the fifteenth and sixteenth centuries, monoalphabetic ciphers were gradually replaced by more sophisticated methods. At the time, Europe, Italy in particular, was a place of turmoil, intrigue, and struggle for political and financial power, and the cloak-and-dagger atmosphere was ideal for cryptography to flourish.

In the 1460s Leone Battista Alberti (1404–1472), better known as an architect, invented a device based on two concentric discs that simplified the use of Caesar ciphers. The substitution, i.e., the relative shift of the two alphabets, is determined by the relative rotation of the two disks (Figure 1.1).

Rumor has it that Alberti also considered changing the substitution within one message by turning the inner disc in his device. It is believed that this is how he discovered the so-called polyalphabetic ciphers, which are based on superpositions of Caesar ciphers with different shifts. For example, the first letter in the message can be shifted by 7, the second letter by 14, the third by 19, the fourth again by 7, the fifth by 14, the sixth by 19, and so on repeating the shifts 7, 14, 19 throughout the whole message. The sequence of numbers — in this example 7, 14, 19 — is usually referred to as a cryptographic key. Using this particular key we transform the message SELL into its concealed version, which reads ZSES.

As said, the message to be concealed is called the plaintext; the operation of disguising it is known as encryption. The encrypted plaintext is called the ciphertext or cryptogram. Our example illustrates the departure from a simple substitution; the repeated L in the plaintext SELL is enciphered differently in each case. Similarly, the two S's, in the ciphertext represent different letters in the plaintext: the first S corresponds to the letter E and the second to the letter L. This makes the straightforward frequency analysis of characters in ciphertexts obsolete. Indeed, polyalphabetic ciphers invented by the main contributors to the field at the time, such as Johannes Trithemius (1462–1516), Blaise de Vigenre (1523–1596), and Giovanni Battista Della Porta (1535–1615), were considered unbreakable for at least another 200 years. Indeed, Vigenre himself confidently dubbed his invention "le chiffre indéchiffrable" — the unbreakable cipher.

1.3 Not So Unbreakable

The first description of a systematic method of breaking polyalphabetic ciphers was published in 1863 by the Prussian colonel Friedrich Wilhelm Kasiski (1805–1881), but, according to some sources (for example, Simon Singh, *The Code Book*), Charles Babbage (1791–1871) had worked out the same method in private sometime in the 1850s.

The basic idea of breaking polyalphabetic ciphers is based on the observation that if we use N different substitutions in a periodic fashion then every Nth character in the cryptogram is enciphered with the same monoalphabetic cipher. In this case we have to find N, the length of the key and apply frequency analysis to subcryptograms composed of every Nth character of the cryptogram.

But how do we find N? We look for repeated sequences in the ciphertext. If a sequence of letters in the plaintext is repeated at a distance which is a multiple of N, then the corresponding ciphertext sequence is also repeated. For example, for N = 3, with the 7, 14, 19 shifts, we encipher TOBEORNOTTOBE

as ACULCVUCMACUL:

T	O	B	E	O	R	N	O	T	T	O	B	E
A	C	U	L	C	V	U	C	M	A	C	U	L

The repeated sequence ACUL is a giveaway. The repetition appears at a distance 9; thus we can infer that possible values of N are 9 or 3 or 1. We can then apply frequency analysis to the whole cryptogram, to every third character and to every ninth character; one of them will reveal the plaintext. This trial and error approach becomes more difficult for large values of N, i.e., for very long keys.

In the 1920s, electromechanical technology transformed the original Alberti's disks into rotor machines in which an encrypting sequence with an extremely long period of substitutions could be generated, by rotating a sequence of rotors. Probably the most famous of them is the Enigma machine, patented by Arthur Scherbius in 1918.

A notable achievement of cryptanalysis was the breaking of the Enigma in 1933. In the winter of 1932, Marian Rejewski, a 27-year-old cryptanalyst working in the Cipher Bureau of the Polish Intelligence Service in Warsaw, mathematically determined the wiring of the Enigma's first rotor. From then on, Poland was able to read thousands of German messages encrypted by the Enigma machine. In July 1939 Poles passed the Enigma secret to French and British cryptanalysts. After Hitler invaded Poland and France, the effort of breaking Enigma ciphers continued at Bletchley Park in England. A large Victorian mansion in the center of the park (now a museum) housed the Government Code and Cypher School and was the scene of many spectacular advances in modern cryptanalysis.

1.4 Truly Unbreakable?

Despite its long history, cryptography only became part of mathematics and information theory in the late 1940s, mainly as a result of the work of Claude Shannon (1916–2001) of Bell Laboratories in New Jersey. Shannon showed that truly unbreakable ciphers do exist and, in fact, they had been known for over 30 years. They were devised in 1918 by an American Telephone and Telegraph engineer Gilbert Vernam and Major Joseph Mauborgne of the U.S. Army Signal Corps. They are called one-time pads or Vernam ciphers (Figure 1.2).

Both the original design of the one-time pad and the modern version of it are based on the binary alphabet. The plaintext is converted to a sequence of 0's and 1's, using some publicly known rule. The key is another sequence of 0's and 1's of the same length. Each bit of the plaintext is then combined with the respective bit of the key, according to the rules of addition in base 2:

$$0+0=0, \qquad 0+1=1+0=1, \qquad 1+1=0. \tag{1.2}$$

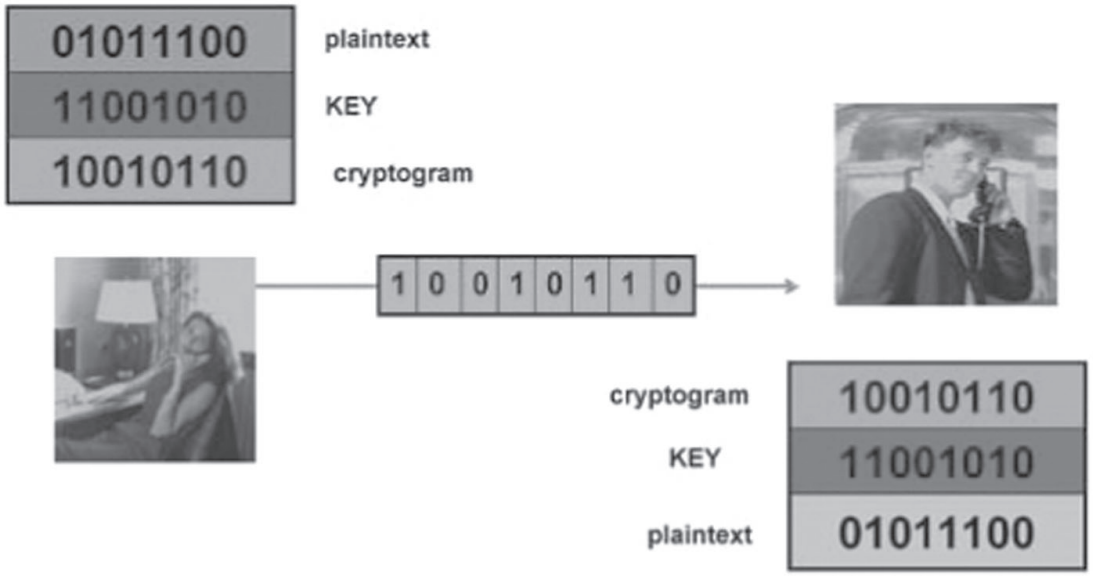


Figure 1.2 One-time pad.

The key is a random sequence of 0's and 1's, and therefore the resulting cryptogram, the plaintext plus the key, is also random and completely scrambled unless one knows the key. The plaintext can be recovered by adding (in base 2 again) the cryptogram and the key.

In the example above (shown in Figure 1.2), the sender, traditionally called Alice, adds each bit of the plaintext (01011100) to the corresponding bit of the key (11001010) obtaining the cryptogram (10010110), which is then transmitted to the receiver, traditionally called Bob. Both Alice and Bob must have exact copies of the key beforehand; Alice needs the key to encrypt the plaintext, Bob needs the key to recover the plaintext from the cryptogram. An eavesdropper, called Eve, who has intercepted the cryptogram and knows the general method of encryption but not the key, will not be able to infer anything useful about the original message. Indeed, Shannon proved that if the key is secret, the same length as the message, truly random, and never reused, then the one-time pad is unbreakable. Thus we do have unbreakable ciphers.

1.5 Key Distribution Problem

There is, however, a snag. All one-time pads suffer from a serious practical drawback, known as the key distribution problem. Potential users have to agree secretly and in advance on the key, a long, random sequence of 0's and 1's. Once they have done this, they can use the key for enciphering and deciphering, and the resulting cryptograms can be transmitted publicly, for example, broadcasted by radio, posted on the Internet, or printed in a newspaper, without compromising the security of the messages. But the key itself must be established between the sender and the receiver by means of a secure

channel — for example, a secure telephone line, or via a private meeting or hand delivery by a trusted courier.

Such a secure channel is usually available only at certain times and under certain circumstances. So users far apart, in order to guarantee perfect security of subsequent cryptocommunication, have to carry around with them an enormous amount of secret and meaningless information (cryptographic keys), equal in volume to all the messages they might later wish to send. This is, to say the least, not very convenient.

Furthermore, even if a secure channel is available, this security can never be truly guaranteed. A fundamental problem remains because, in principle, any classical private channel can be monitored passively, without the sender or receiver knowing that the eavesdropping has taken place. This is because classical physics — the theory of ordinary-scale bodies and phenomena such as paper documents, magnetic tapes, and radio signals — allows all physical properties of an object to be measured without disturbing those properties. Since all information, including cryptographic keys, is encoded in measurable physical properties of some object or signal, classical theory leaves open the possibility of passive eavesdropping, because in principle it allows the eavesdropper to measure physical properties without disturbing them. This is not the case in quantum theory, which forms the basis for quantum cryptography. However, before we venture into quantum physics, let us mention in passing a beautiful mathematical approach to solving the key distribution problem.

The 1970s brought a clever mathematical discovery in the shape of "public-key" systems. The two main public-key cryptography techniques in use today are the Diffie–Hellman key exchange protocol [13] and the RSA encryption system (named after the three inventors, Ron Rivest, Adi Shamir, and Leonard Adleman) [24]. They were discovered in the academic community in 1976 and 1978, respectively. However, it was widely rumored that these techniques were known to British government agencies prior to these dates, although this was not officially confirmed until recently. In fact, the techniques were first discovered at the British Government Communication Headquarters in the early 1970s by James Ellis, who called them nonsecret encryption. In 1973, building on Ellis' idea, C. Cocks designed what we now call RSA, and in 1974 M. Williamson proposed what is essentially known today as the Diffie–Hellman key exchange protocol.

In the public-key systems, users do not need to agree on a secret key before they send the message. They work on the principle of a safe with two keys, one public key to lock it, and another private one to open it. Everyone has a key to lock the safe but only one person has a key that will open it again, so anyone can put a message in the safe but only one person can take it out. The systems avoid the key distribution problem but unfortunately their security depends on unproven mathematical assumptions. For example, RSA — probably the most popular public-key cryptosystem — derives its security from the difficulty of factoring large numbers. This means that if mathematicians or computer scientists come up with fast and clever procedures

for factoring, the whole privacy and discretion of public-key cryptosystems could vanish overnight.

Indeed, we know that quantum computers can, at least in principle, efficiently factor large integers [19]. Thus in one sense public-key cryptosystems are already insecure: any RSA-encrypted message that is recorded today will become readable moments after the first quantum computer is switched on, and therefore RSA cannot be used for securely transmitting any information that will still need to be secret on that happy day. Admittedly, that day is probably decades away, but can anyone prove, or give any reliable assurance, that it is? Confidence in the slowness of technological progress is all that the security of the RSA system now rests on.

1.6 Local Realism and Eavesdropping

We shall now leave mathematics and enter the world of quantum physics. Physicists view key distribution as a physical process associated with sending information from one place to another. From this perspective, eavesdropping is a set of measurements performed on carriers of information. In order to avoid detection, an eavesdropper wants to learn about the value of a physical property that encodes information without disturbing it. Is such a passive measurement always possible?

In 1935, Albert Einstein together with Boris Podolsky and Nathan Rosen (EPR) published a paper in which they outlined how a "proper" fundamental theory of nature should look [15]. The EPR program required completeness ("In a complete theory there is an element corresponding to each element of reality.") and locality ("The real factual situation of the system A is independent of what is done with the system B, which is spatially separated from the former.") and defined the element of physical reality as "If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity." In other words, if we can know the value of some physical property without "touching" the system in any way, then the property must be physically real, i.e., it must have a determinate value, even before we measure it.

This world view is known as "local realism" and it implies possibilities of perfect eavesdropping. Indeed, this is exactly what the EPR definition of the element of reality means in the cryptographic context.

Einstein and his colleagues considered a thought experiment, on two entangled particles, that showed that quantum states cannot in all situations be complete descriptions of physical reality. The EPR argument, as subsequently modified by David Bohm [9], goes as follows. Imagine the singlet-spin state of two spin $\frac{1}{2}$ particles

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle |\downarrow\rangle - |\downarrow\rangle |\uparrow\rangle \right), \tag{1.3}$$

where the single particle kets $|\uparrow\rangle$ and $|\downarrow\rangle$ denote spin up and spin down with respect to some chosen direction. This state is spherically symmetric, and the

choice of direction does not matter. The two particles, which we label A and B, are emitted from a source and fly apart. After they are sufficiently separated so that they do not interact with each other, we can predict with certainity the x component of spin of particle A by measuring the x component of spin of particle B. Each measurement on B, in $\frac{1}{2}\hbar$ units, can yield two results, $+1$ (spin up) and -1 (spin down) and reveals the value of the x component of A. This is because the total spin of the two particles is zero, and the spin components of the two particles must have opposite values. The measurement performed on particle B does not disturb particle A (by locality) so the x component of spin is an element of reality according to the EPR criterion. By the same argument and by the spherical symmetry of state $|\Psi\rangle$ the y, z, or indeed any other spin components are also elements of reality. Therefore all the spin components must have predetermined values $+1$ or -1.

Local realism has experimental consequences. Consider two pairs of spin components, A_1 and A_2 pertaining to the particle A, and B_1 and B_2 pertaining to the particle B. A_1, A_2, B_1, and B_2 all have simultaneous definite values, either $+1$ or -1. Hence the quantity

$$Q = A_1(B_1 - B_2) + A_2(B_1 + B_2) \tag{1.4}$$

can have two different values, either -2 or $+2$, and consequently,

$$-2 \leq \langle Q \rangle \leq 2, \tag{1.5}$$

where $\langle Q \rangle$ stands for the average value of Q. This inequality is known as the Bell inequality [3] or more precisely as the CHSH inequality [11].

Both quantum-mechanical predictions and experiments show that for two particles in the singlet state, $\langle AB \rangle = -\vec{a} \cdot \vec{b}$, $\vec{a}$ and $\vec{b}$ are the unit vectors specifying the directions of the spin components of particles A and B, respectively. This leads to a violation of the CHSH inequality (Equation (1.5)). For if we choose $\vec{a}_i$ and $\vec{b}_j$ in the x–y plane, perpendicular to the trajectory of the particles emitted from the source, and characterized by the azimuthal angles $\phi_1^a = 0$, $\phi_2^a = \frac{1}{2}\pi$, and $\phi_1^b = \frac{1}{4}\pi$, $\phi_2^b = \frac{3}{4}\pi$ then $\langle Q \rangle = -2\sqrt{2}$. Local realism is refuted, which opens possibilities of constructing key distribution schemes that will always detect eavesdropping.

Please note that any theory that refutes local realism, be it quantum or post-quantum, opens such possibilities. Even if quantum mechanics is refuted sometime in the future and a new physical theory is conjectured, as long as the new theory refutes local realism, possibilities for post-quantum cryptography are wide open.

1.7 Quantum Key Distribution

1.7.1 Entanglement-Based Protocols

Let us take advantage of the CHSH inequality within the quantum theory. The key distribution is performed via a quantum channel that consists of a source that emits pairs of spin $\frac{1}{2}$ particles in the singlet state as in

Equation (1.3). The particles fly apart along the z-axis toward the two legitimate users of the channel, Alice and Bob, who, after the particles have separated, perform measurements and register spin components along one of three directions, given by unit vectors $\vec{a}_i$ and $\vec{b}_j (i,\ j = 1, 2, 3)$, respectively, for Alice and Bob. For simplicity, both $\vec{a}_i$ and $\vec{b}_j$ vectors lie in the x–y plane, perpendicular to the trajectory of the particles, and are characterized by azimuthal angles: $\phi_1^a = 0$, $\phi_2^a = \frac{1}{4}\pi$, $\phi_3^a = \frac{1}{2}\pi$ and $\phi_1^b = \frac{1}{4}\pi$, $\phi_2^b = \frac{1}{2}\pi$, $\phi_3^b = \frac{3}{4}\pi$. Superscripts a and b refer to Alice's and Bob's analyzers, respectively, and the angle is measured from the vertical x-axis. The users choose the orientation of the analyzers randomly and independently for each pair of incoming particles. Each measurement can yield two results, $+1$ (spin up) and -1 (spin down) and can reveal one bit of information.

After the transmission has taken place, Alice and Bob can announce in public the orientations of the analyzers they have chosen for each particular measurement and divide the measurements into two separate groups: a first group for which they used different orientations of the analyzers and a second group for which they used the same orientation of the analyzers. They discard all measurements in which either or both of them failed to register a particle at all. Subsequently Alice and Bob can reveal publicly the results they obtained, but within the first group of measurements only. This allows them to establish the value of $\langle Q \rangle$, which if the particles were not directly or indirectly "disturbed" should be very close to $-2\sqrt{2}$. This assures the legitimate users that the results they obtained within the second group of measurements are anticorrelated and can be converted into a secret string of bits — the key.

An eavesdropper, Eve, cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The information "comes into being" only after the legitimate users perform measurements and communicate in public afterwards. Eve may try to substitute her own prepared data for Alice and Bob to misguide them, but as she does not know which orientation of the analyzers will be chosen for a given pair of particles, there is no good strategy to escape being detected. In this case her intervention will be equivalent to introducing elements of *physical reality* to the spin components and will lower $\langle Q \rangle$ below its "quantum" value.

1.7.2 Prepare and Measure Protocols

Instead of tuning into an external source of entangled particles, Alice and Bob may also rely on the Heisenberg uncertainty principle. Suppose a spin $\frac{1}{2}$ particle is prepared in one of the four states, say spin up and down along the vertical x-axis ($|\uparrow\rangle$, $|\downarrow\rangle$) and spin up and down along the horizontal y-axis ($|\rightarrow\rangle$, $|\leftarrow\rangle$). Then the two x states $|\uparrow\rangle$ and $|\downarrow\rangle$ can be distinguished by one measurement and the two y states $|\rightarrow\rangle$ and $|\leftarrow\rangle$ by another measurement. The measurement that can distinguish between the two x states will give a completely random outcome, when applied to distinguish between the two y

states and vice versa. If, for each incoming particle, the receiver performing the measurement is not told in advance which type of spin (x or y) was prepared by the sender, then the receiver is completely lost and unable to determine the spin value. This can be used for the key distribution.

Alice and Bob agree on the bit encoding, e.g., $|\uparrow\rangle = 0 = |\rightarrow\rangle$, $|\downarrow\rangle = 1 = |\leftarrow\rangle$, and Alice repeatedly prepares one of the four quantum states, choosing randomly out of $|\uparrow\rangle$, $|\downarrow\rangle$, $|\rightarrow\rangle$, and $|\leftarrow\rangle$. She then sends it to Bob, who randomly chooses to measure either the x or the y spin component. After completing all the measurements, Alice and Bob discuss their data in public so that anybody can listen, including their adversary Eve. Bob tells Alice which spin component he measured for each incoming particle and she tells him "what should have been measured." Alice does not disclose which particular state she prepared, and Bob does not reveal the outcome of the measurement, so the actual values of bits are still secret. Alice and Bob then discard those results in which Bob failed to detect a particle and those for which he made measurements of the wrong type. They then compare a large subset of the remaining data. Provided no eavesdropping has taken place, the result should be a shared secret that can be interpreted by both Alice and Bob as a binary key.

But let us suppose there is an eavesdropper, Eve. Eve does not know in advance which state will be chosen by Alice to encode a given bit. If she measures this bit and resends it to Bob, this may create errors in Bob's readings. Therefore in order to complete the key distribution Alice and Bob have to test their data for discrepancies. They compare in public some randomly selected readings and estimate the error rate; if they find many discrepancies, they have reason to suspect eavesdropping and should start the whole key distribution from scratch. If the error rate is negligibly small, they know that the data not disclosed in the public comparison form a secret key. No matter how complex and subtle is the advanced technology and computing power available to the eavesdropper, the "quantum noise" caused inevitably by each act of tapping will expose each attempt to gain even partial information about the key.

1.8 Security Proofs

Admittedly the key distribution procedures described above are somewhat idealized. The problem is that there is in principle no way of distinguishing noise due to an eavesdropper from innocent noise due to spurious interactions with the environment, some of which are presumably always present. All good quantum key distribution protocols must be operable in the presence of noise that may or may not result from eavesdropping. The protocols must specify for which values of measurable parameters Alice and Bob can establish a secret key and provide a physically implementable procedure that generates such a key. The design of the procedure must take into account that an eavesdropper may have access to unlimited quantum computing power.

The best way to analyze eavesdropping in the system is to adopt the entanglement-based protocol and the scenario that is most favorable for

eavesdropping, namely that Eve herself is allowed to prepare and deliver all the pairs that Alice and Bob will subsequently use to establish a key. This way we take the most conservative view, which attributes all disturbance in the channel to eavesdropping, even though most of it (if not all) may be due to innocent environmental noise. This approach also applies to the prepare and measure protocols because they can be viewed as special cases of entanglement-based protocols, e.g., the source of entangled particles can be given either to Alice or to Bob. It is prudent to assume that Eve has disproportional technological advantage over Alice and Bob. She may have access to unlimited computational power, including quantum computers; she may monitor all the public communication between Alice and Bob in which they reveal their measurement choices and exchange further information in order to correct errors in their shared key and to amplify its privacy. In contrast, Alice and Bob can only perform measurements on individual qubits and communicate classically over a public channel. They do not have quantum computers, or any sophisticated quantum technology, apart from the ability to establish a transmission over a quantum channel.

The search for good security criteria under such stringent conditions led to early studies of quantum eavesdropping [17,28] and finally to the first proof of the security of key distribution [12]. The original proof showed that the entanglement-based key distributions are indeed secure and noise-tolerant against an adversary with unlimited computing power as long as Alice and Bob can implement quantum privacy amplification. In principle, quantum privacy amplification allows us to establish a secure key over any distance, using entanglement swapping [29] in a chain of quantum repeaters [2,14]. However, this procedure, which distills pure entangled states from corrupted mixed states of two qubits, requires a small-scale quantum computation. Subsequent proofs by Inamori [21] and Ben-Or [4] showed that Alice and Bob can also distill a secret key from partially entangled particles using only classical error correction and classical privacy amplification [6,7].

Quantum privacy amplification was also used by Lo and Chau to prove the security of the prepare and measure protocols over an arbitrary distance [22]. A concurrent proof by Mayers showed that the protocol can be secure without Alice and Bob having to rely on the use of quantum computers [23]. The same conclusion, but using different techniques, was subsequently reached by Biham et al. [8]. Although the two proofs did not require quantum privacy amplification, they were rather complex. A nice fusion of quantum privacy amplification and error correction was proposed by Shor and Preskill, who formulated a relatively simple proof of the security of the BB84 [5] protocol based on virtual quantum error correction [25]. They showed that a protocol that employs quantum error-correcting code to prevent Eve from becoming entangled with qubits that are used to generate the key reduces to the BB84 augmented by classical error correction and classical privacy amplification. This proof has been further extended by Gottesman and Lo [20] for two-way public communication to allow for a higher bit error rate in BB84 and by Tamaki et al. [26] to proof the security of the B92 protocol.

More recently, another simple proof of the BB84, which employs results from quantum communication complexity, has been provided by Ben-Or [4] and a general proof based on bounds on the performance of quantum memories has been proposed by Christandl et al. [30].

Let us also mention in passing that apart from the scenario that favors Eve, i.e., Eve has access to quantum computers while Alice and Bob do not, there are interesting connections regarding the criteria for the key distillation in commensurate cases, i.e., when Alice, Bob, and Eve have access to the same technology, be it classical or quantum [18,10,1].

1.9 Concluding Remarks

Quantum cryptography was discovered independently in the U.S. and Europe. The first one to propose it was Stephen Wiesner, then at Columbia University in New York, who, in the early 1970s introduced the concept of quantum conjugate coding [27]. He showed how to store or transmit two messages by encoding them in two "conjugate observables" such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. He illustrated his idea with a design of unforgeable bank notes. A decade later, building upon this work, Charles H. Bennett of the IBM T. J. Watson Research Center and Gilles Brassard of the Université de Montreal, proposed a method for secure communication based on Wiesner's conjugate observables [5]. However, these ideas remained by and large unknown to physicists and crytologists. In 1990, independently and initially unaware of the earlier work, the current author, then a Ph.D. student at the University of Oxford, discovered and developed a different approach to quantum cryptography based on peculiar quantum correlations known as quantum entanglement [16]. Since then, quantum cryptography has evolved into a thriving experimental area and is quickly becoming a commercial proposition.

This brief overview has only scratched the surface of the many activities that are presently being pursued under the heading of quantum cryptography. It is focused solely on the development of theoretical concepts that led to creating unbreakable quantum ciphers. The experimental developments, although equally fascinating, are left to the other contributors to this book. I have also omitted many interesting topics in quantum cryptography that go beyond the key distribution problem. Let me stop here hoping that even the simplest outline of quantum key distribution has enough interesting physics to keep you entertained for a while.

References

1. A. Acin, N. Gisin, and V. Scarani, Security bounds in quantum cryptography using d-level systems, *Quant. Inf. Comp.*, 3(6), 563–580, November 2003.
2. H. Aschauer and H.-J. Briegel, A security proof for quantum cryptography based entirely on entanglement purification, *Phys. Rev. A*, 66, 032302, 2002.
3. J.S. Bell, *Physics*, 1, 195, 1964.

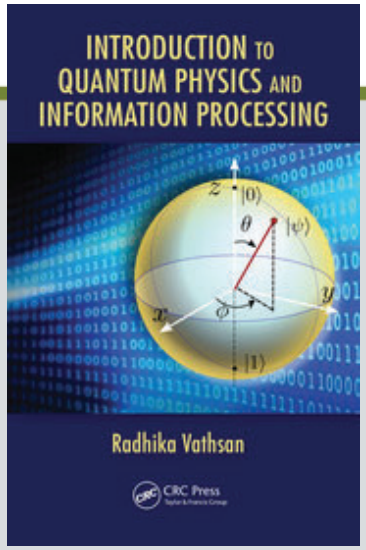
4. M. Ben-Or, Simple security proof for quantum key distribution. On-line presentation available at http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/index.html.
5. C.H. Bennett and G. Brassard, Quantum cryptography, public key distribution and coin tossing, in *Proceedings of International Conference on Computer Systems and Signal Processing*, IEEE, 1984, p. 175.
6. C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, Generalized privacy amplification, *IEEE Trans. Inf. Theory*, 41(6), 1915–1923, 1995.
7. C.H. Bennett, G. Brassard, and J.-M. Robert, Privacy amplification by public discusion. *SIAM Journal on Computing*, 17(2), 210–229, 1988.
8. E. Biham, M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury, A proof of the security of quantum key distribution, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC)*, ACM Press, New York, 2000, p. 715. quant-ph/9912053.
9. D. Bohm, *Quantum Theory*, New York: Prentice Hall, 1951.
10. D. Bruss, M. Christandl, A. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello, Tomographic quantum cryptography: equivalence of quantum and classical key distillation, *Phys. Rev. Lett.*, 91, 097901, 2003. quant-ph/0303184.
11. J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, *Phys. Rev. Lett.*, 23, 880, 1969.
12. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noisy channels, *Phys. Rev. Lett.*, 77, 2818–2821, 1996. Erratum, ibid., 80, 2022–2022, 1998, quant-ph/9604039.
13. W. Diffie and M.E Hellman, *IEEE Trans. Inf. Theory*, IT-22, 644, 1976.
14. W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Quantum repeaters based on entanglement purification, *Phys. Rev. A*, 59, 169–181, 1999.
15. A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47, 777, 1935.
16. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.*, 67(6), 661, 1991.
17. A.K. Ekert and B. Huttner, Eavesdropping techniques in quantum cryptosystems, *Journal of Modern Optics*, 41, 2455–2466, 1994. Special issue on Quantum Communication.
18. N. Gisin and S. Wolf, in *Advances in Cryptology—CRYPTO'00*, Lecture Notes in Computer Science, Springer–Verlag, 2000, pp. 482–500.
19. S. Goldwasser, ed., *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA, 1994.
20. D. Gottesmann and H.-K. Lo., Proof of security of quantum key distribution with two-way classical communication, *IEEE Trans. Inf. Theory*, 49(2), 457–475, 2003, quant-ph/0105121.
21. H. Inamori, Security of EPR-based quantum key distribution, quant-ph/0008064.
22. H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science*, 283(5410), 2050–2056, 1999.
23. D. Mayers, Unconditional security in quantum cryptography, quant-ph/9802025, 1998.
24. R. Rivest, A. Shamir, and L. Adleman, On digital signatures and public-key cryptosystems, Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, January 1979.

25. P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, *Phys. Rev. Lett.*, 85(2), 441–444, 2000; quant-ph/0003004.
26. K. Tamaki, M. Koashi, and N. Imoto, Unconditionally secure key distribution based on two nonorthogonal states, *Phys. Rev. Lett.*, 90, 167904, 2003.
27. S. Wiesner, Conjugate coding, *Sigact News*, 15(1), 78–88, 1983; Originally written c. 1970 but them unpublished.
28. A.C.-C. Yao, Security of quantum protocols against coherent measurements, in *Proceedings of the 27th ACM Symposium on the Theory of Computing*, ACM Press, 1995, pp. 67–75.
29. M. Zukowski, A. Zeilinger, M. Horne, and A.K. Ekert, Event-ready detectors, Bell experiment via entanglement swapping, *Phys. Rev. Lett.*, 71, 4287–4290, 1993.
30. M. Christandl, R. Renner, and A. Ekert, A generic security proof for quantum key distribution, quant-ph/0402131.

CHAPTER

2

QUANTUM ALGORITHMS



This chapter is excerpted from

Introduction to Quantum Physics and Information Processing

by Radhika Vathsan

Learn more

Chapter 8

Quantum Algorithms

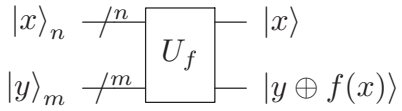
In the last chapter, we introduced the circuit model for quantum computation, where a computation is essentially the evaluation of a function. In the binary system of computation a function is a map $f : \{0,1\}^n \mapsto \{0,1\}^m$. The function takes an n-bit input and produces an m-bit output. However, this can be regarded as m functions $f_i : \{0,1\}^n \mapsto \{0,1\}$, that take an n-bit input and give a one-bit output, each of which is one bit of $f(x)$. We can thus restrict our attention to $n \to 1$ functions alone, in other words, we can reduce our problem to questions with yes/no answers, a so-called binary decision problem.

In order to evaluate a function, we have to feed it all allowed inputs and tabulate the corresponding outputs. We can construct circuits evaluating different functions by suitable combinations of gates. Now a given function evaluation or computational task is to be optimized by exploiting quantum mechanics. How is this done efficiently?

We have seen that the quantum function evaluator for $f : \{0,1\}^n \mapsto \{0,1\}^m$ is defined by the 2^{n+m}-square unitary operator of Definition 7.1:

$$U|x\rangle_n|y\rangle_m = |x\rangle_n|y \oplus f(x)\rangle_m.$$

This is essentially an **f-controlled NOT gate** as in Figure 7.15:



For $y = 0$ the output is simply $|f(x)\rangle$. If the function evaluator is fed a uniform superposition of all n-qubit basis states, then the linearity of the operator U_f ensures that the output is a uniform superposition of functions on each input, (entangled with the corresponding input state,) as in Figure 8.1.

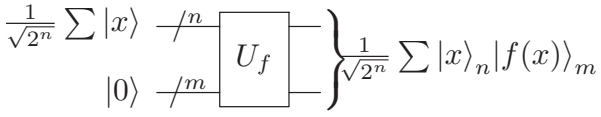


FIGURE 8.1: The quantum function evaluator with a uniform superposition.

Here the top line is sometimes called the *input register*, since the input to the function is fed through it, and the bottom one is the so-called *output register*, since it reflects the state containing the evaluated function.

The advantage of the quantum function evaluator is that it can take all possible inputs simultaneously as a superposition of states, and the corresponding outputs are all simultaneously present in the output state. This has often been called quantum parallelism. However, in this basic form it gives us no advantage, since to actually discover the value of the function, we must measure the output, upon which the output state will collapse to *one* of the possible outputs at random. The trick to making quantum computing work is to cleverly manipulate this basic function evaluator in such a way that the probability amplitude for the answer to the problem is maximum. It is quantum interference that enables this to happen. If this had not been possible, quantum computing would have been a forgotten chapter in the history of science. As it happens, this field received new impetus when Peter Shor shook up the world in 1994 with his famous algorithm for finding the prime factors of large integers.

All known quantum algorithms seem to fall into three broad classes:

1. Based on the Fourier transform: Deutsch–Josza, Shor's algorithm etc.
2. Based on quantum search, involving amplitude amplification: Grover's algorithm etc.
3. Quantum simulations.

In this chapter we will examine the first two kinds, leaving the last to more physics-specific texts. The algorithms are typically framed as yes-no answers to inputs to the function evaluator treated as a black box (Figure 8.2). This is also referred to as querying the oracle, as the unknown function evaluator is regarded, like a mysterious priestess who will only give single-bit answers when questioned!

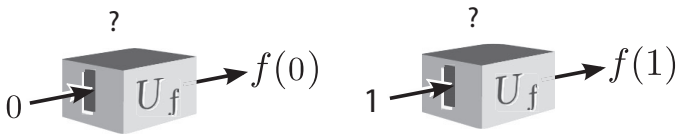


FIGURE 8.2: Classical black box function evaluator as an oracle.

8.1 The Deutsch Algorithm

Let's start with 1-bit functions $f : \{0,1\} \mapsto \{0,1\}$. There are totally four possible functions, and evaluated on inputs 0 and 1 can give answers 0 or 1. To actually determine which of these our black box is we need to query it with both inputs, whether classically or otherwise, and we obtain no

advantage using quantum computing. However, as David Deutsch [24] showed in 1985, it is possible to distinguish the function on the basis of some property, more efficiently in the quantum case. The particular classification Deutsch's algorithm considers is the following: they are either *constant* ($\mathbb{C}$), i.e., $f(0) = f(1)$, or *balanced* ($\mathbb{B}$), i.e., the outputs contain an equal number of 0's and 1's ($f(0) = \overline{f(1)}$).

Example 8.1.1. For $n > 1$, functions need not fall into the classes $\mathbb{C}$ or $\mathbb{B}$ alone. For example, consider f_1 and f_2 defined by:

$$f_1: \begin{array}{ll} f(00) = & 0 \\ f(01) = & 1 \\ f(10) = & 0 \\ f(11) = & 1 \end{array}, \quad f_2: \begin{array}{ll} f(00) = & 0 \\ f(01) = & 1 \\ f(10) = & 0 \\ f(11) = & 0 \end{array}$$

Here, f_1 is balanced while f_2 is neither constant nor balanced.

Deutsch's algorithm[1] is formulated for the following problem. Although it might seem contrived, it is the first algorithm to demonstrate the principles of the new paradigm.

The problem: given a black-box (oracle) that implements a 1-bit function $f(x)$, how will you determine whether the function belongs to class $\mathbb{C}$ or to class $\mathbb{B}$ with a minimum number of runs of the black box (or equivalently, queries to the oracle)?

Classically, it is clear that we have to run the machine twice, with inputs 0 and 1.

The Deutsch algorithm shows how this problem can be solved in just *one* run of the black box. The circuit is shown in Figure 8.3, that we will work through step by step.

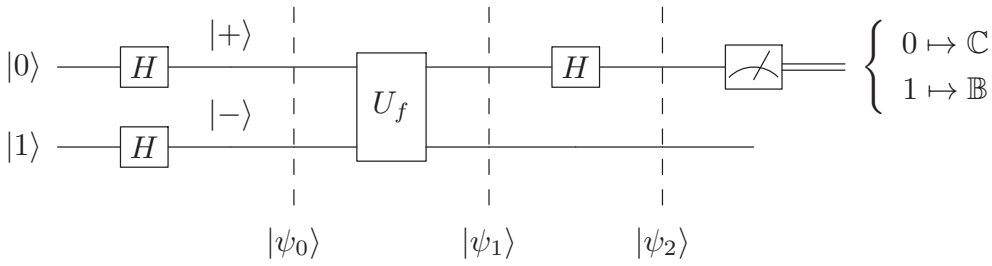


FIGURE 8.3: The Deutsch algorithm.

Step 1: Supply as input the uniform superposition

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{8.1}$$

[1]The presentation given here is not the original one in [24] but an improved version presented first by [19].

Step 2: On the bottom register, supply the state $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. This is the crucial feature that introduces useful interference in the result. The reason for this will be clear when we evaluate the output of the black box. So the input state is

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}[|00\rangle - |01\rangle + |10\rangle - |11\rangle] \end{aligned} \tag{8.2}$$

Step 3: Run the function evaluator. The output is

$$\begin{aligned} |\psi_1\rangle &= U_f|\psi_0\rangle \\ &= \frac{1}{2}\left[|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle + |1\rangle|f(1)\rangle - |1\rangle|\overline{f(1)}\rangle\right] \\ &= \frac{1}{2}|0\rangle\left[|f(0)\rangle - |\overline{f(0)}\rangle\right] + \frac{1}{2}|1\rangle\left[|f(1)\rangle - |\overline{f(1)}\rangle\right]. \end{aligned} \tag{8.3}$$

Step 4: Measure the top register in the X-basis. That is, change basis by applying the H gate on the first qubit and then measure it. Just before the measurement, the output state on both wires is

$$\begin{aligned} |\psi_2\rangle &= H_1|\psi_1\rangle \\ &= \frac{1}{2\sqrt{2}}|0\rangle\left[|f(0)\rangle - |\overline{f(0)}\rangle + |f(1)\rangle - |\overline{f(1)}\rangle\right] \\ &\quad + \frac{1}{2\sqrt{2}}|1\rangle\left[|f(0)\rangle - |\overline{f(0)}\rangle - |f(1)\rangle + |\overline{f(1)}\rangle\right] \end{aligned} \tag{8.4}$$

If the function is $\mathbb{C}$, then $f(0) = f(1)$ and the amplitude for $|0\rangle$ is 1 while that for $|1\rangle$ is 0. On the other hand, when f is $\mathbb{B}$ then $f(0) = \overline{f(1)}$ and the amplitude for $|1\rangle$ is 1 while that for $|0\rangle$is 0. Thus a measurement of the output gives us the answer to the query with certainty. We have run the function evaluator only once. The quantum advantage has given us a double speedup in this case.

The reason why this works is that Step 2 implements the so called "*phase kickback*" trick. If the state $|-\rangle$ on the lower register fed into the black box, then the output acquires a phase that depends on $f(x)$. This phase can effectively be regarded as attached to the state of the upper register.

$$\begin{aligned} U_f\left[|x\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right] &= \frac{1}{\sqrt{2}}|x\rangle\left[|f(x)\rangle - |\overline{f(x)}\rangle\right] \\ &= \begin{cases} \frac{1}{\sqrt{2}}|x\rangle(|0\rangle + |1\rangle) & \text{if } f(x) = 0, \\ \frac{1}{\sqrt{2}}|x\rangle(|1\rangle - |0\rangle) & \text{if } f(x) = 1 \end{cases} \\ &= (-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right]. \end{aligned} \tag{8.5}$$

The output is separable, with the lower register unchanged in state $|-\rangle$, while the upper register is effectively the input with an $f(x)$-dependent phase.

With this effect, we can re-analyze the algorithm with the uniform superposition $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ in the input register:

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &\xrightarrow{U_f} \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right] && (8.6) \\ &\xrightarrow{H} \frac{1}{\sqrt{2}}\left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle\right. \\ &\quad \left. + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right] && (8.7) \end{aligned}$$

where it's obvious that a measurement gives $|0\rangle$ if $f(x)$ is $\mathbb{C}$ and $|1\rangle$ if $f(x)$ is $\mathbb{B}$.

8.1.1 Deutsch–Josza algorithm

The Deutsch algorithm was extended to n-bit functions by Josza and others in 1992 [26].

The problem: Given an $n \to 1$ function $f : \{0,1\}^n \mapsto \{0,1\}$ that is guaranteed to be either constant or balanced, find out which it is in a minimum number of runs.

Classically, we would proceed by querying the oracle with each n-bit number. If we find an answer that is not equal to the previous one then we have a balanced function. In worst-case scenario, we might find the same $f(x)$ until the half the possible inputs, i.e., after querying the function $2^n/2$ times. The answer to the next query would solve the problem. Thus we need to run the oracle at worst $2^{n-1}+1$ times: exponential in the number of bits of input.

The quantum algorithm achieves the distinction in just one run! This is a dramatic speedup indeed. The circuit (Figure 8.4) is an n-qubit extension of that for the Deutsch problem:

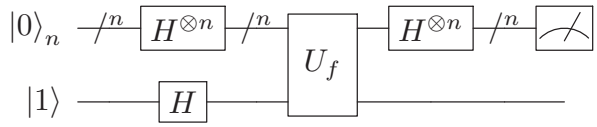


FIGURE 8.4: The circuit for the Deutsch–Josza algorithm.

The input to the circuit is the uniform n-qubit superposition

$$H^{\otimes n}|0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \tag{8.8}$$

Due to the phase-kickback trick, the output of U_f on the input register is the

superposition

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle. \tag{8.9}$$

After the Hadamard, this state becomes

$$H^{\otimes n}|\psi_1\rangle = \frac{1}{2^n} \sum_{x,y=0}^{2^n-1} (-1)^{[f(x)+x\cdot y]} |y\rangle. \tag{8.10}$$

Here, we have used the result of Equation 7.28 and $x \cdot y$ is the bitwise product of x and y summed modulo 2, as in Equation 7.29. Now when $f(x)$ is constant, the amplitude for the state $|0\rangle$ in this superposition is

$$\text{coefficient of } |0\rangle = \frac{1}{2^n} \sum_x (-1)^{f(x)} = 1.$$

In other words the probability of getting $|0\rangle$ is one for a constant function. Whereas if $f(x)$ is balanced, then the amplitude for $|0\rangle$ is a sum of an equal number of $+1$s and -1s, that is, zero. Thus if the function is balanced, the output measures to any number *other* than 0. We thus distinguish the two classes in one run of the black box, which is nearly an n-fold speedup compared to the classical case.

8.2 The Bernstein–Vazirani Algorithm

We'll now look at algorithms that show more substantial speedups compared to classical ones. One such algorithm was invented by Umesh Vazirani and his student Ethan Bernstein in 1993 [11]. This algorithm identifies a linear Boolean function in one query of the oracle.

The problem: given a function evaluator for

$$f : \{0,1\}^n \mapsto \{0,1\} \text{ where } f(x) = a \cdot x, \quad a \in [0, 2^n], \tag{8.11}$$

and the dot is a bitwise product with modulo 2 addition:

$$a \cdot x \equiv a_0 x_0 \oplus a_1 x_1 \oplus \cdots \oplus a_{n-1} x_{n-1}, \tag{8.12}$$

determine the function, or in other words find a.

Example 8.2.1. An example of such a function for $n = 2$ and $a = 11$, which evaluates to

$$f(00) \quad = \quad 0$$

$$\begin{aligned} f(01) &= 0.1 \oplus 1.1 = 1 \\ f(10) &= 1.1 \oplus 0.1 = 1 \\ f(11) &= 1.1 \oplus 1.1 = 0 \end{aligned}$$

Classically, we can determine the k^{th} bit of a if we feed the oracle the input $x = 2^k$, that has only the k^{th} bit as 1 and all the rest as 0. This becomes obvious when you look at the binary expansion of a:

$$a = a_0 + a_1 2^1 + \cdots + a_k 2^k + \ldots \implies a_k = a \cdot 2^k. \tag{8.13}$$

This calls the function n times.

The quantum algorithm, which uses the same circuit as for the Deutsch–Josza algorithm, succeeds with *one* call!

Let's analyze the output of the circuit of Figure 8.4 for this form of the function:

$$\sum_x \sum_y \frac{1}{2^n}(-1)^{f(x)+x\cdot y}|y\rangle \otimes |-\rangle \quad = \quad \frac{1}{2^n}\sum_y \left[\sum_x (-1)^{a\cdot x + y\cdot x}\right] |y\rangle \otimes |-\rangle$$
$$. \tag{8.14}$$

The amplitude for $|y\rangle$ is $\frac{1}{2^n}\sum_x (-1)^{a\cdot x+y\cdot x} = \frac{1}{2^n}\sum_x (-1)^{(a+y)\cdot x} = 1$ if $y = a$! It's easy to see why it is zero for all other values of y. Thus with certainty, the output of the circuit gives us a.

A more explicit way of seeing why this works is by analyzing the circuit for U_f. This analysis is lucidly given in Mermin [48]. The black box for $a\cdot x$ flips the bit in the lower register whenever a bit of the input x and the corresponding bit of a are both 1. For instance, suppose we had $a = 11010$ with $n = 5$. Then it can easily be seen that $a \cdot x$ is implemented by the circuit of Figure 8.5.

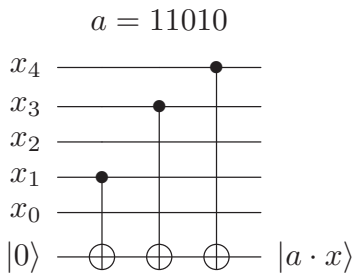


FIGURE 8.5: A circuit that executes U_f for $f = 11010 \cdot x$.

Coming to the circuit for solving the Bernstein–Vazirani problem, it has an H gate before each qubit enters the function evaluator and after. This is true even of the lower register, which can be thought of as initialized to $|1\rangle$. Note that an H gate before and after a CNOT interchanges the roles of the control and target qubits (see Figure 7.8).

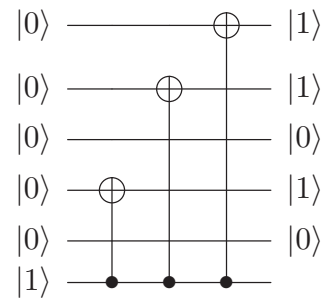


FIGURE 8.6: Analysis of circuit for the Bernstein–Vazirani algorithm for $a = 11010$.

The solution is therefore the circuit of Figure 8.6, whose output directly reads out the bits of a.

The algorithm thus gives an n-fold speedup over the classical case.

8.3 Simon's Algorithm

Even though the Bernstein–Vazirani algorithm offers such a great speedup, the classical solution is still not exponential. Daniel Simon came up with an algorithm [65] in 1994 that is the first to demonstrate a dramatic exponential speedup over a hard classical problem, but the solution is probabilistic. This feature is characteristic of many quantum algorithms. Simon's problem also illustrates a class of problems that basically use Fourier transforms, in the form of the amplitudes of the output states that "interfere" to give a large probability for the expected solution.

The problem: Given a black box implementing a function

$$f : \{0,1\}^n \mapsto \{0,1\}^{n-1} \text{ such that} f(x \oplus a) = f(x), \quad a \in [0, 2^n - 1], \quad (8.15)$$

determine a with the minimum number of queries to the box.

Example 8.3.1. The functions considered in Simon's algorithm can be thought of as "periodic" under bitwise addition. For example, let's look at the 3-bit function

x	000	001	010	011	100	101	110	111
$f(x)$	3	2	2	3	1	4	4	1

The first repetition is of the value $f(1) = f(2)$. The "period" is therefore $a = 001 \oplus 010 = 011 = 3$. You can verify that all the other repetitions also satisfy the same condition.

The classical solution to this problem is *hard*, i.e., the number of runs of the function grows exponentially as the size of the input. We would query the oracle with successive values of n-bit numbers x until we found a repeated value for the output: $f(x_i) = f(x_j)$. Then we could calculate $a = x_i \oplus x_j$. However, a could be any one of 2^n possible numbers. By the m^{th} run, $\frac{1}{2}m(m-1)$ pairs have been compared and eliminated as possible a's. For reasonable chance of success, we need $\frac{1}{2}m(m-1) \geq 2^n \implies$ a lower bound on the number of trials $m = \Omega(2^{n/2})$, which is exponential in the number of bits.

The quantum circuit (Figure 8.7) that solves this problem is essentially the same as the Deutsch–Josza circuit except that the lower register is also expanded to n qubit, and initialized to $|0\rangle_n$ (we dispense with the phase kickback).

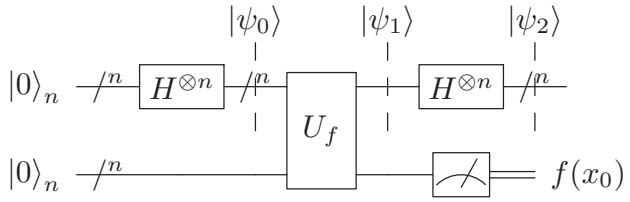


FIGURE 8.7: The circuit for the Simon algorithm.

The input to the oracle gives us

$$U_f|\psi_0\rangle \otimes |0\rangle = U_f \left[\sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle\right] = \sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle. \tag{8.16}$$

In order to analyze the solution, let us use the reverse of the principle of delayed measurement, and assume we measure the lower register after the action of U_f. Let's denote the outcome by $f(x_0)$, which is generated from two possible inputs x_0 or $x_0 \oplus a$. The top register therefore collapses to a superposition of these two states alone:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \left(|x_0\rangle + |x_0 \oplus a\rangle\right). \tag{8.17}$$

If we now apply H to each qubit in the upper register, we get

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \left[(-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y}\right] |y\rangle. \tag{8.18}$$

Now $a \cdot y$ is either 0 or 1. If $a \cdot y = 1$, then the amplitude for $|y\rangle$ is zero and all those states do not occur in the output. Thus the only states that can be measured in the output are those for which the condition $a \cdot y = 0$ is satisfied. This is a binary algebraic equation with n unknowns (the bits of a). We can find a if we can obtain n independent equations, corresponding to n different values of y. If we repeat the experiment until we have collected n distinct,

non-zero y's then we can solve for the bits of a. It is not guaranteed that we will get a distinct y on each run, so we may most probably have to run the oracle more than n times.

To determine the complexity of this problem, we will need to estimate how the number of runs of the oracle scales with n. It can be shown (see Box 8.3) that the number of times the oracle has to be queried is $n+m$ where m doesn't depend on n. This algorithm is thus a sub-exponential solution to a classically hard problem.

Box 8.1: Complexity Analysis for Simon's Algorithm

As in many quantum algorithms, the analysis of why the algorithm is computationally more efficient than the classical case involves a detailed mathematical examination of the solution. In the case of Simon's algorithm, the output after measurement is an n-bit string y such that

$$a \cdot y = a_{n-1}y_{n-1} \oplus a_{n-2}y_{n-2} \oplus \cdots \oplus a_1 y_1 \oplus a_0 y_0 = 0.$$

We need to collect at least $n-1$ such *distinct* bit-strings in order to determine the coefficients a. So we need to query the oracle at least $n-1$ times and need to find a lower bound on the probability of success.

Suppose we ran the algorithm k times and got linearly independent y's. What's the probability that the next run gives a different y? The minimum probability for this occurring is

$$\frac{2^n - 2^k}{2^n} = 1 - 2^{k-n}.$$

So the probability of getting $n-1$ independent y's is just

$$\mathcal{P} = \left(1 - \frac{1}{2^n}\right)\left(1 - \frac{1}{2^{n-1}}\right)\cdots\left(1 - \frac{1}{2}\right).$$

Now notice that $(1-s)(1-t) = 1-(s+t)+st \geq 1-(s+t)$. So we have

$$\begin{aligned} \mathcal{P} &\geq \left(1 - \sum_{i=1}^{n} \frac{1}{2^i}\right)\frac{1}{2} \\ &\geq \left(1 - \frac{1}{2}\right)\frac{1}{2} = \frac{1}{4}. \end{aligned}$$

This means that there is a *finite* minimum probability with which we will succeed in n runs. To ensure success, we'll have to run the algorithm a few more times, *independent* of n, so that the number of runs is still $\mathcal{O}(n)$.

The trick that makes the kind of algorithms considered so far work is that the output before measuring in the X basis has $f(x)$-dependent phases. Until

now these phases were restricted to ± 1. More general phases come about if the Fourier transform is implemented. In this section, we introduced the idea of using the H gate on the output to produce interfering amplitudes. This is just a special case of the quantum Fourier transform, as we will see in the next section.

8.4 Quantum Fourier Transform and Applications

The Fourier transform, a mathematical tool named after the 18th century French mathematician Joseph Fourier, is an invaluable tool in engineering and the sciences. No technical education is complete without a firm grasp of this technique and its uses. The simplest way to understand the Fourier transform $\mathcal{F}$ of a function $f(x)$ is to imagine the function as made up of various components that are periodic (like a sine function) with a frequency y, and $\mathcal{F}(f(x))$ as a function $\tilde{f}(y)$ measuring the amplitude of each frequency component in the function. In other words, we construct a decomposition of the function in terms of the oscillatory exponential $e^{-2\pi iyx}$, where the coefficients in that decomposition are the Fourier transform:

$$f(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dy \; e^{2\pi iyx} \tilde{f}(y). \tag{8.19}$$

This formula is said to define the *inverse Fourier transform* of $\tilde{f}(y)$, while the Fourier transform is defined as

$$\mathcal{F}(f(x)) = \tilde{f}(y) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dx \; e^{-2\pi iyx} f(x). \tag{8.20}$$

The factor in front of the integral captures the normalization. A function can in general have an infinite number of frequency components, and the frequencies can be distributed continuously. That's how the Fourier transform is a continuous function of the frequency y.

The two Equations 8.20 and 8.19 define a *Fourier transform pair*. The Fourier transform naturally produces complex numbers, so that $f(x)$ and $\tilde{f}(y)$ are in general complex. When we compute the Fourier transform on a digital machine, we need to discretize the integral to get the Discrete Fourier Transform (DFT).

8.4.1 The discrete Fourier transform and classical algorithm

When $f(x)$ is a discrete function over the finite range $N = 2^n$ of discrete n-bit inputs x, we can think of it as a vector with N components $\{f_0 \; f_1 \; ... \; f_{N-1}\}$. The integral over x in Equation 8.20 is then a sum over an index k with

$x \to k/N$ and the limits are restricted from 0 to $N-1$. We then get the discrete Fourier transform of order N defined as

$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i y k/N} f_k.$$

This is another vector with N components $\{g_0\ g_1\ ...\ g_{N-1}\}$, given by

$$g_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i j k/N} f_k. \tag{8.21}$$

These are just the coefficients of orthogonal harmonic components $e^{2\pi i j k/N}$ of the function, which can be expressed as the inverse discrete Fourier transform (IDFT):

$$f_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} g_j. \tag{8.22}$$

We can regard the DFT as a complex matrix transformation of the vector $\{f_k\}$:

$$g_j = \sum_{k=0}^{N-1} M_{jk} f_k; \qquad f_k = \sum_{j=0}^{N-1} M_{jk}^{-1} g_k, \tag{8.23}$$

where M_{jk} are the elements of an $N \times N$ matrix M given by

$$M_{jk} = \frac{1}{\sqrt{N}} e^{2\pi i j k/N} = \frac{1}{\sqrt{N}} \omega_N^{jk}. \tag{8.24}$$

Here $\omega_N = e^{2\pi i/N}$ is the N^{th} root of unity. More explicitly,

$$\begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \cdots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)^2} \end{bmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{pmatrix} \tag{8.25}$$

Example 8.4.1. The simple case of $N = 2$, $\omega_2 = e^{i\pi} = -1$ and

$$\text{DFT}_2 \quad = \quad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & \omega_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{8.26}$$

which is just the Walsh–Hadamard transform.

Exercise 8.1. Write out the DFT matrix for $N = 4$.

Exercise 8.2. Calculate the DFT on the N-dimensional zero-vector.

Example 8.4.2. Unitarity of the DFT:

The crucial point that allows us to extend the DFT to an operator on quantum states is that it is unitary. To prove this, we need to show that

$$M^\dagger M = \mathbb{1} \implies \sum_{l=0}^{N-1} M_{jl} M^*_{lk} \quad = \quad \delta_{jk} \tag{8.27}$$

where M_{jk} is defined by Equation 8.24.

$$\text{When } j = k: \quad \frac{1}{N} \sum_l \omega_N^{jl} \omega_N^{-lj} = \frac{1}{N} \sum_l 1 = 1; \tag{8.28}$$

When $j \neq l$, then $\sum_l \omega_N^{l(j-k)}$ is the sum of N terms of a geometric series whose first term is 1 and ratio is $\omega_N^{(j-k)}$. So we have

$$\sum_l \omega_N^{l(j-k)} = \frac{1 - \omega_N^{N(j-k)}}{1 - \omega_N^{(j-k)}} = 0 \tag{8.29}$$

Thus Equation 8.27 is proved.

Box 8.2: Classical FFT Algorithm

Computing the DFT_N of a vector involves evaluating N^2 elements of the DFT matrix, and looks like a job that scales as 2^{2n} with the number of bits $n = \log_2 N$. In implementing the DFT transform on a digital machine, one can easily optimize by exploiting the properties of the integer powers of ω_N. There are cycles among elements of DFT_N, since $\omega_N^N = 1$. So while a direct matrix multiplication of the form of Equation 8.24 would typically require $\mathcal{O}(N^2)$ basic operations, the optimized fast Fourier transform (FFT) algorithm requires $\mathcal{O}(N \log_2 N)$ operations only.

For example, consider $N = 4$; $\omega_4 = e^{2\pi i/4} = i$, $\omega_4^2 = -1$, $\omega_4^4 = 1$.

$$\mathrm{DFT}_4 = \frac{1}{2} \left(\begin{array}{cc:cc} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ \hdashline 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{array} \right) \tag{8.30}$$

Now there is a relationship between the upper and lower halves of this matrix. Look at the highlighted columns, repeated for the upper and lower halves: they form a 2×2 matrix that acts on the even index components (note the index starts at 0).

$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\mathrm{DFT}_2. \tag{8.31}$$

The part that acts on the odd index components is for the upper half

$$\begin{aligned} \frac{1}{2}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \times \mathrm{DFT}_2 \\ &= \frac{1}{\sqrt{2}}\mathrm{Diag}(1\ \omega_4) \times \mathrm{DFT}_2. \end{aligned} \tag{8.32}$$

The negative of this acts on the lower half. Thus the DFT of a 4-d vector is reduced to two DFT's of a 2-d vector. This is at the heart of the classical FFT algorithm.

The above example shows that DFT_N can be reduced to $\mathrm{DFT}_{N/2}$. The FFT algorithm works by recursively dividing the original vector into even numbered and odd numbered elements, until at the final stage there are just two terms and DFT_2 can be applied. The process is then reversed by successively doubling the vectors and eventually covering the entire input. Let's see how this is possible in general: let $N = 2M$.

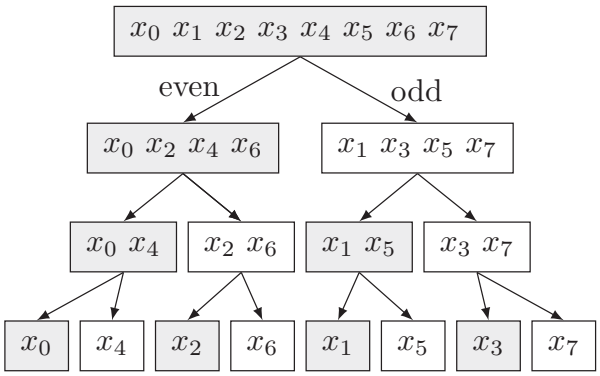
$$\mathrm{DFT}_N(f(x)) = \tilde{f}(y) = \frac{1}{\sqrt{2M}}\sum_{x=0}^{2M-1} \omega_{2M}^{xy} f(x). \tag{8.33}$$

Breaking this up into even and odd terms,

$$\begin{aligned} \mathrm{DFT}_{2M}(f(x)) =& \frac{1}{\sqrt{2M}}\left(\sum_{x=0}^{M-1} \omega_{2M}^{2xy} f(2x) + \sum_{x=0}^{M-1} \omega_{2M}^{(2x+1)y} f(2x+1)\right) \\ =& \frac{1}{\sqrt{2}}\Bigg(\underbrace{\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1} \omega_M^{xy} f(2x)}_{\mathrm{DFT}_M \text{ of even terms}} + \underbrace{\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1} \omega_M^{(x)y} f(2x+1)}_{\mathrm{DFT}_M \text{ of odd terms}} \times \omega_{2M}^{y}\Bigg) \end{aligned} \tag{8.34}$$

At any stage l of evaluating the DFT, one can divide the input into two to write it in terms of $\mathrm{DFT}_{l/2}$, and continue successively until one is left with DFT_2's.

Successive division of the terms in the input into two until we reach the two-term pairs is called *decimation*. The process of decimating higher-order DFT's looks like the following for $N = 8$:



We then start evaluating upward from the 2-point DFTs, successively doubling at each stage. The generic 2-point DFT looks like Figure 8.8, called a butterfly diagram for its symmetric structure. The labels on the sides represent the multiplicative factors and two lines joined at a node represent addition of the corresponding terms.

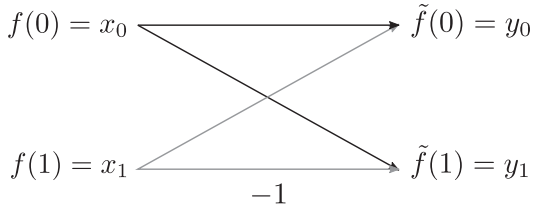


FIGURE 8.8: The 2-point DFT: butterfly diagram.

For $N = 8$, we have worked out the decimation process in Example 8.4.4. The butterfly diagram looks like Figure 8.9.

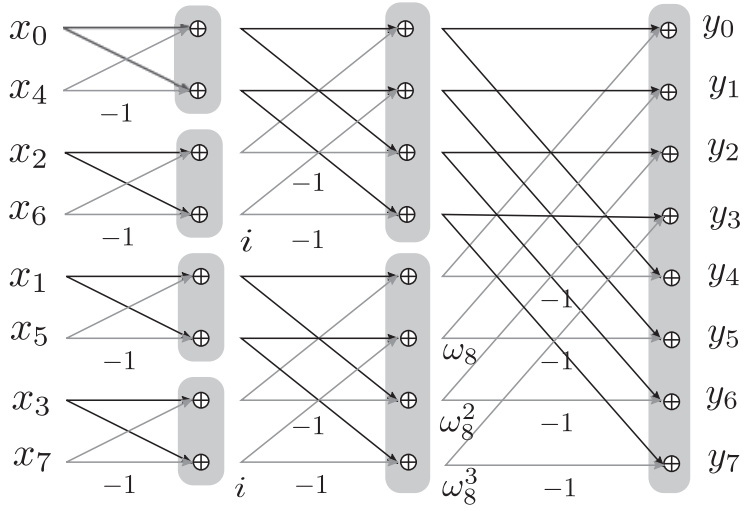


FIGURE 8.9: Butterfly diagram for computing an 8-point DFT. The output vector $\{y_0\ y_1 \ldots\ y_8\}$ is the DFT of the input vector.

Exercise 8.3. Show how the DFT of a 6-d vector reduces to the DFT's of the even and odd indexed 3-d components.

8.4.2 Complexity of the classical FFT algorithm

Suppose the computation of DFT_N requires $T(N)$ basic operations. From Equation 8.34, we see that this is related to $T(N/2)$ since we need to evaluate two DFT's of order $N/2$ and also do N multiplications of the exponential factors. Thus,

$$T(N) = 2T(N/2) + \mathcal{O}(N). \tag{8.35}$$

Using this recursively to solve for $T(N)$ one gets

$$T(N) = \mathcal{O}(N \log_2 N). \tag{8.36}$$

8.5 Definition of the QFT from Discrete Fourier Transform

The quantum Fourier transform (QFT) is simply the DFT operation on the amplitudes of a quantum state. The DFT matrix is unitary, and can therefore represent a quantum transformation. We can define the QFT (order $N = 2^n$) of an n-qubit basis state $|x\rangle$ by

$$\hat{\mathcal{F}}_N|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{xy}|y\rangle. \tag{8.37}$$

Interestingly, as we have seen in Equation 8.26, the QFT transform for $n = 2$ is just the Hadamard gate.

When applied to a superposition state $|\psi\rangle = \sum_i C_i|i\rangle$, the QFT performs a DFT on the coefficients C_i:

$$\begin{aligned} \hat{\mathcal{F}}_N|\psi\rangle &= \sum_i C_i U_N|i\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_i C_i \sum_j \omega_N^{ij}|j\rangle \qquad (8.38) \\ &= \sum_j \left(\mathrm{DFT}_N C\right)_j |j\rangle. \qquad (8.39) \end{aligned}$$

where C denotes the vector of coefficients in the state representation.

An efficient algorithm for evaluating the QFT is inspired by the FFT algorithm, where we compute the bit-wise breakup of the action of $\hat{\mathcal{F}}$ on its

input. Remember, $|y\rangle_n = \bigotimes_{j=0}^{n-1} |y_j\rangle$. Each y_j takes a value 0 or 1. The QFT has superpositions of $|y\rangle$ with a phase $\omega_N^{xy/N}$, containing the integer product of x and y. We want to break this up into the constituent bits, the y_js. So we write

$$xy = \left(x_0 + 2x_1 + \cdots + 2^{n-1}x_{n-1}\right)\left(y_0 + 2y_1 + \cdots 2^{n-1}y_{n-1}\right). \tag{8.40}$$

Now any product in this expansion that has a coefficient of 2^n or higher can be dropped since it would contribute unity to the phase: $\omega_N^{2n} = 1$. So we find

$$\begin{aligned}
\frac{xy}{N} &= \left(\frac{x_0}{2^n} + \frac{x_1}{2^{n-1}} + \cdots + \frac{x_{n-1}}{2}\right) y_0 \\
&+ \left(\frac{x_0}{2^{n-1}} + \frac{x_1}{2^{n-2}} + \cdots + \frac{x_{n-2}}{2}\right) y_1 \\
&\vdots \\
&+ \left(\frac{x_0}{2^2} + \frac{x_1}{2}\right) y_{n-2} \\
&+ \left(\frac{x_0}{2}\right) y_{n-1}.
\end{aligned} \tag{8.41}$$

Using the binary "point" notation

$$0.x_1x_2x_3...x_n = \frac{x_1}{2} + \frac{x_2}{2^2} + \frac{x_3}{2^3} + ...\frac{x_n}{2^n}, \tag{8.42}$$

$$\frac{xy}{N} = y_0(0.x_{n-1}x_{n-2}\cdots x_0) + y_1(0.x_{n-2}\cdots x_0) + \cdots + y_{n-1}(0.x_0). \tag{8.43}$$

Using this to write the QFT in bit-wise expansion, we can associate an exponential factor with each bit of y, the output becomes the following product state:

$$\begin{aligned}
\hat{\mathcal{F}}_N|x\rangle &= \frac{1}{\sqrt{2^n}} \sum_y e^{2\pi i xy/N} |y_0\rangle \otimes |y_1\rangle \cdots |y_{n-1}\rangle \\
&= \frac{1}{\sqrt{2^n}} \left(\sum_{y_0=0,1} e^{2\pi i y_0 (0.x_{n-1}x_{n-2}\cdots x_0)} |y_0\rangle \right) \\
&\quad \otimes \left(\sum_{y_1=0,1} e^{2\pi i y_1 (0.x_{n-2}\cdots x_0)} |y_1\rangle \right) \otimes \\
&\quad \cdots \otimes \left(\sum_{y_{n-1}=0,1} e^{2\pi i y_{n-1} (0.x_0)} |y_{n-1}\rangle \right) \\
&= \left(\frac{|0\rangle + e^{2\pi i (0.x_{n-1}x_{n-2}\cdots x_0)}|1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{|0\rangle + e^{2\pi i (0.x_{n-2}\cdots x_0)}|1\rangle}{\sqrt{2}} \right) \otimes \\
&\quad \cdots \otimes \left(\frac{|0\rangle + e^{2\pi i (0.x_0)}|1\rangle}{\sqrt{2}} \right)
\end{aligned} \tag{8.44}$$

Each term in the product of Equation 8.44 is the state of an output qubit for the corresponding qubit of the input. This translates into a circuit for evaluating $\hat{\mathcal{F}}_{2^n}$. The order of occurrence of the terms must be noted: the first term is the least significant bit, and the last is the most significant bit of the output.

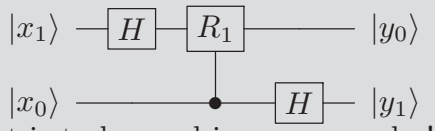
Example 8.5.1. QFT circuit for $n = 2$:

$$|x_1 x_0\rangle \xrightarrow{\hat{\mathcal{F}}} \frac{|0\rangle + e^{2\pi i(0.x_0)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(0.x_1 x_0)}|1\rangle}{\sqrt{2}}$$

This means

$$\begin{aligned} |x_1\rangle &\longrightarrow \frac{|0\rangle + e^{2\pi i(\frac{x_0}{2})}|1\rangle}{\sqrt{2}} = |y_1\rangle \\ |x_0\rangle &\longrightarrow \frac{|0\rangle + e^{2\pi i(\frac{x_1}{2}+\frac{x_0}{4})}|1\rangle}{\sqrt{2}} = |y_0\rangle \end{aligned}$$

Here $|y_1\rangle$ has an x_0-dependent phase of $e^{i\pi}$ for $|1\rangle$, which can be obtained by an H acting on $|x_0\rangle$. Similarly $|y_0\rangle$ has a x_1-dependent phase of $e^{i\pi}$ and an x_0-dependent phase of $e^{i\pi/2}$ for $|1\rangle$. The first is obtained by an H on $|x_1\rangle$ while the second is the x_0-controlled action of the gate $R_1 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$:



Note that the output is to be read in reverse order!

Exercise 8.4. Work out the circuit for the QFT for $n = 3$.

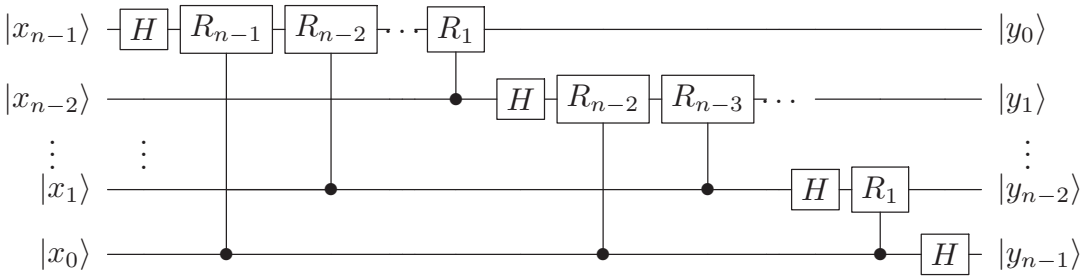


FIGURE 8.10: Circuit for the quantum Fourier transform $\hat{\mathcal{F}}_{2^n}$, on n qubits.

You should now be able to work out that Figure 8.10 is an efficient quantum circuit for the QFT on n qubits.. We require controlled phase gates, with phase

matrices like

$$R_d = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^d} \end{pmatrix}, \tag{8.45}$$

where d can be interpreted as the distance from the control bit. Notice that the output bits are in reverse order. One can either agree to read the output in reverse order or to perform a swap at the end.

The efficiency of this circuit is related to the number of basic gate operations required per input bit. We can easily see that this is n H-gates and $n(n-1)/2$ C-R-gates for n bits, which is $\mathcal{O}(n^2)$. This is *exponentially* faster than the classical FFT which takes $\mathcal{O}(n2^n)$. Hurray for quantum algorithms!

But before we exult too much, observe that the output of the quantum Fourier transform is a superposition of basis states whose phases represent the Fourier transform of the corresponding input bit. A measurement at the end of the above circuit gives us **no** information whatsoever about the Fourier transform of the input! So we cannot use this circuit as a super-efficient Fourier transform computer! Instead, we have to incorporate it in procedures that require FT-dependent phases. And Peter Shor did just that in his path-breaking algorithm for prime factorization.

8.5.1 Period-finding using QFT

Preliminary to the Shor algorithm, let's focus on one that lends itself naturally to the QFT: computing the period r of a periodic n-bit function

$$f : \{0,1\}^n \mapsto \{0,1\}^n \text{ such that } f(x+r) = f(x), \quad r \in [0, 2^n - 1]. \tag{8.46}$$

We will take $2^n = N$ in what follows. The function could repeat more than once in the interval $[0, N-1]$, so we have

$$f(x + kr) = f(x), \qquad kr < N.$$

We assume we are presented with a black box (oracle) that evaluates such a function. The algorithm uses a circuit that is a direct extension of Simon's algorithm (Section 8.3), in which we'll use the full QFT instead of the 1-bit version (the Hadamard transform) used there. The circuit (Figure 8.11) is straightforward.

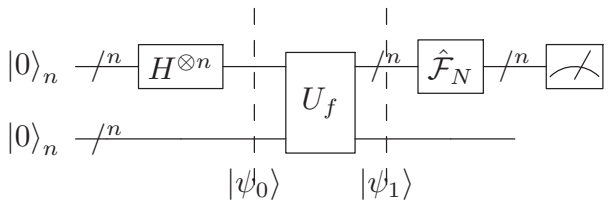


FIGURE 8.11: Circuit for quantum period finding.

The input to the U_f black box is once again

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle_n \otimes |0\rangle_n, \tag{8.47}$$

So the output ought to be

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |f(x)\rangle. \tag{8.48}$$

We will again assume that we measure the lower register at this point, obtaining some number f_0. Then the top register collapses to a superposition of only those states $|x\rangle$ for which $f(x) = f_0$. All such x's are of the form $x_0 + kr$ for some $x_0 < r$, and some integer $k : kr < N$. Suppose the number of periods within the interval $[0, N-1]$ is p:

$$p = [N/r]\,, \tag{8.49}$$

where the square bracket notation stands for the ceiling function (greatest integer less than the argument). The state of the computer is then a superposition of p terms of the form

$$|\psi_1\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} |x_0 + kr\rangle \otimes |f_0\rangle. \tag{8.50}$$

Now subjecting the top register to a QFT, we get

$$\hat{\mathcal{F}}_N \left(\frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} |x_0 + kr\rangle \right) = \sum_{y=0}^{N-1} \left(\frac{1}{\sqrt{Np}} \sum_{k=0}^{p-1} e^{2\pi i (x_0 + kr) y/N} \right) |y\rangle. \tag{8.51}$$

This is a superposition of basis states with a probability of occurrence of a particular y given by the mod-squared of the term in the brackets:

$$\begin{aligned} \mathcal{P}(y) &= \frac{1}{Np} \left| \sum_{k=0}^{p-1} e^{2\pi i (x_0 + kr)/N} \right|^2 \\ &= \frac{1}{Np} \left| \sum_{k=0}^{p-1} e^{2\pi i k r y/N} \right|^2 \end{aligned} \tag{8.52}$$

So y has an r-dependent probability of occurrence. The crux of this algorithm is that the most probable value of y gives us enough information about r for us to compute it. In fact, the claim is that the values of y that are measured are close to an integer multiple of N/r.

Let's first see this in the special case when there are exactly integer number of periods in the interval $[0, N-1]$, i.e., when

$$p = \frac{N}{r}.$$

We will compare the probability of y for mp when m is some integer, and when not:

$$\mathcal{P}(y) = \frac{1}{r}\left|\frac{1}{p}\sum_{k=0}^{p-1} e^{2\pi iky/p}\right|^2. \tag{8.53}$$

$$\mathcal{P}(y = mp) = \frac{1}{r}, \tag{8.54}$$

$$\mathcal{P}(y \neq mp) = \frac{1}{rp^2}\left|\sum_{k=0}^{p-1} e^{ik\theta}\right|^2, \text{ where } \theta = 2\pi\frac{y}{p}, \tag{8.55}$$

$$= \frac{1}{rp^2}\frac{\sin^2(p\theta/2)}{\sin^2(\theta/2)}$$

$$= 0 \text{ (since } p\theta \text{ is an integer multiple of } 2\pi\text{)}. \tag{8.56}$$

So the *only* values of y obtained in this case are integer multiples of N/r.

For a general function, it is highly unlikely that there are exactly integer numbers of periods in the interval $[0, N-1]$. Yet, the most probable values of y turn out to be close to integer multiples of N/r! To see this, let us start by writing

$$y = m\frac{N}{r} + \delta_m, \tag{8.57}$$

where m is an integer and $|\delta_m| \leq \frac{1}{2}$. Let's substitute this in Equation 8.52:

$$\mathcal{P}(y) = \frac{1}{Np}\left|\sum_{k=0}^{p-1} e^{2\pi ikr(mN/r+\delta_m)/N}\right|^2$$

$$= \frac{1}{Np}\left|\sum_{k=0}^{p-1} e^{2\pi ikr\delta_m/N}\right|^2$$

$$= \frac{1}{Np}\frac{\sin^2(p\theta_m)}{\sin^2\theta_m}, \text{ where } \theta_m = \frac{\pi r}{N}\delta_m. \tag{8.58}$$

Now since p is nearly N/r, the numerator is nearly $\sin^2(\pi\delta_m)$. Also, $r\delta_m/N$ is very small, so the denominator is nearly $\theta_m \sim \pi\delta_m r/N$.

Therefore,

$$\mathcal{P}(y) \sim \frac{1}{Np}\frac{\sin^2(\pi\delta_m)}{(\pi\delta_m r/N)^2} = \frac{1}{r}\frac{\sin^2(\pi\delta_m)}{(\pi\delta_m)^2}. \tag{8.59}$$

Since $\delta_m < 1/2$, and $\dfrac{\sin\theta}{\theta} \geq \dfrac{2}{\pi}$ for $0 \leq \theta \leq \pi/2$, (see Figure 8.12), we have

$$\mathcal{P}(y \sim m/r) \geq \frac{4}{\pi^2 r}. \tag{8.60}$$

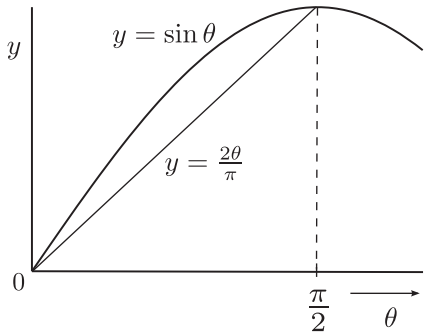


FIGURE 8.12: Graph comparing $\sin\theta$ and $2\theta/\pi$.

There are r possible such y's, so the probability of any such y is greater than $4/\pi^2 \sim 40\%$. This result is to be interpreted as saying that when we rerun the algorithm many times, with high probability we measure y's that are integer multiples of N/r. Now from such numbers we can use classical algorithms to deduce r, most famously the Euclid algorithm for continued fractions. The period-finding algorithm thus succeeds to a high probability.

Such analyses of the probability of obtaining good results are a common feature of most known quantum algorithms.

Box 8.3: Finding r Given N/r: Continued Fractions

The output y of a run of the period-finding algorithm is close to an integer multiple of N/r. Consider the number $x = y/N \sim m/r$. We now look at the continued fraction expansion of x:

$$x = c_0 + \frac{1}{x_1} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{x_2}} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{x_3}}} = \cdots \tag{8.61}$$

$$= c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}} \tag{8.62}$$

At each stage of the expansion (Equations 8.61), c_i is the integer part of the denominator x_i from the previous stage, and each x_i, known as the i^{th} *partial sum*, is a fraction $\in [0, 1]$. To find the fractional expression for $\frac{1}{x_i}$, Euclid's GCD algorithm can be used. Equation 8.62 is the continued fraction expansion of x. If x is a rational number then the continued fraction expansion terminates after a finite number of steps. For n-bit m and r, it turns out that the continued fraction can be computed in $\mathcal{O}(n^3)$ steps.

Now there is a theorem (proved in [50], Appendix 4) stating that m/r is

one of the partial sums x_i of the continued fraction of x. $r < N$, and the best guess for r is the partial sum having the largest denominator less than N. This is tested out and if it is not the period then the we try again with a different x.

8.5.1.1 Shor's factorization algorithm

The above algorithm for period finding, due in some form to Peter Shor, is really the heart of the factorization algorithm. For the more curious, the relationship between factoring and period-finding is through a series of mathematical results that we will outline here. (This section is purely for the purpose of completeness, and the results of pure mathematics used will not be derived or explained.)

For a good understanding of what follows, one must be familiar with *modular algebra*, that is algebra restricted to the range $[0, N-1]$ by considering all results of algebraic operations as periodic with period N. Then "mod N" essentially means "the remainder after dividing the result by N". For example, addition mod 4 will mean $2+2=0$ and $2+3=1$.

- If a is a random integer $< N$ such that a and N are coprime, then it is possible to find an integer $r \in [1, N]$ such that

  $$a^r \bmod N = 1.$$

  r is called the *order* of a in $\bmod N$.

- For a with order $r \bmod N$, the function

  $$f(x) = a^x \bmod N,$$

  is periodic with period r. To see how:

  $$\begin{aligned} f(x+r) &= a^{x+r} \bmod N = (a^x \bmod N)(a^r \bmod N) \\ &= a^x \bmod N \times 1 = f(x). \end{aligned}$$

  Therefore, finding the period of a function $f(x)$ is the same as finding the order of some integer coprime with N.

- Now if N is a large integer, choose a random integer a coprime with N and find its order r using the period-finding algorithm. Now if r is even then construct $b = a^{r/2}$.

  $$\begin{aligned} b^2 &= 1 \bmod N \\ \implies b^2 - 1 &= 0 \bmod N \end{aligned}$$

  So $b \pm 1$ must have factors common with N. If we find the GCDs of $b \pm 1$ and N we have the prime factors of N!

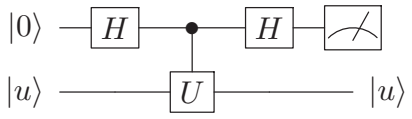
8.5.2 Phase estimation

One version of Shor's algorithm is based on phase estimation. This application of the quantum Fourier transform is used to estimate the eigenvalue of a unitary operator, which is a phase:

$$\hat{U}|u\rangle = e^{i\theta}|u\rangle; \quad \theta = 2\pi\phi \tag{8.63}$$

where ϕ is a fraction.

As a preliminary to this algorithm, let's look at a toy version. Suppose you are given U and an eigenstate $|u\rangle$. We have seen that the circuit of Figure 7.14 simulates a measurement of U.



Here,

$$\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |u\rangle \rightarrow \frac{1}{\sqrt{2}}\big(|0\rangle + e^{2\pi i\phi}|1\rangle\big) \otimes |u\rangle. \tag{8.64}$$

If ϕ were a single bit, then you can see that the output is 0 if $\phi = 0.0$ and 1 if $\phi = 0.1$. This circuit thus gives us the value in one run. But in general ϕ will be several bits long. A measurement of the upper register in the H basis will yield a 0 or 1 with probabilities $\cos^2 \pi\phi$ and $\sin^2 \pi\phi$. A statistically large number of measurements will allow us to recover ϕ from the counts. But this is an inefficient method.

Note that the H transform on the upper register is the one-bit Fourier transform. In order to estimate ϕ to more bits of accuracy, we must have a qubit for each significant figure of ϕ and then perform an inverse Fourier transform, as shown in the circuit of Figure 8.13.

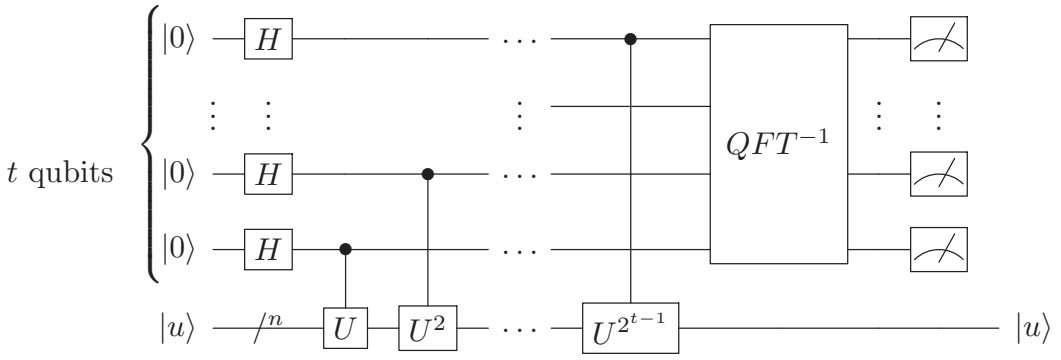


FIGURE 8.13: Circuit for phase estimation.

Imagine ϕ upto t bits as

$$\phi = 0.\phi_1\phi_2\cdots\phi_t = \frac{\phi'}{2^t}, \quad \phi' = \phi_t\phi_{t-1}\cdots\phi_1. \tag{8.65}$$

Then we start with t working qubits in the input register, and use them to control gates of the form U^{2^k}. After the control gates, the output on the k^{th} line is

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 2^k \phi}|1\rangle\right) \tag{8.66}$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.\phi_1\phi_2\cdots\phi_k)}|1\rangle\right). \tag{8.67}$$

You can see that just before the QFT gate, the state of the upper register is

$$\frac{1}{\sqrt{2^t}}\left(|0\rangle + e^{2\pi i\phi}|1\rangle\right) \otimes \left(|0\rangle + e^{4\pi i\phi}|1\rangle\right) \otimes \ldots \otimes \left(|0\rangle + e^{2\pi i.2^t\phi}|1\rangle\right) \tag{8.68}$$

$$= \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i\phi k}|k\rangle \tag{8.69}$$

This is just the QFT mod 2^t of ϕ' and an inverse Fourier transform will give you ϕ' exact to t significant figures.

8.6 Grover's Search Algorithm

Another famous algorithm that made a splash in the world of quantum computing was invented by L. K. Grover in 1997 [40]. This algorithm is in a different class from the ones we have studied so far, which may all be said to be QFT-based. Grover's algorithm introduced a new technique: amplitude amplification. Even though it did not demonstrate an exponential speed-up over the classical case, it was still dramatic enough to get noticed.

The problem Grover attacked was that of search for an element in an unstructured database. The problem is like doing a reverse search in a phone directory: you have a number and need to know the person it belongs to. Thus there is no regular short-cut to the search, you have to go through each entry in the book and check if it matches the number you have.

The problem can be phrased in the language of oracles, if we assume that the criterion for the search is built into a function evaluator: a function that tells you whether the input number matches the search criterion or not. So we imagine that the numbers x are indices to the entries in the database, and one index, let's say k, belongs to the entry being searched for. Then

$$f_k(x) = \begin{cases} 1 & \text{if } x = k \\ 0 & \text{otherwise.} \end{cases} \tag{8.70}$$

Here, if x is an n-bit number, then the size of the database is $2^n = N$. As

this becomes really large, the problem becomes harder. In fact, classically this problem has a complexity $\mathcal{O}(N)$. Grover's algorithm turns out to be $\mathcal{O}(\sqrt{N})$.

As in most quantum algorithms, the first step exploits quantum parallelism, and inputs the uniform superposition of all x's to the oracle U_{f_k}, the unitary implementation of $f_k(x)$:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{N-1} |x\rangle. \tag{8.71}$$

It also uses the phase kickback trick to give f-dependent phases to the states in this superposition:

$$|\psi\rangle \otimes |-\rangle \xrightarrow{U_{f_k}} \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{N-1} (-1)^{f_k(x)} \; |x\rangle \otimes |-\rangle. \tag{8.72}$$

We need to look more closely at the form of the output state. Remember that $f_k(x)$ is zero unless $x = k$. Thus each $|x\rangle$ in the above superposition has the same phase $(+1)$ as before except the state $|k\rangle$ which has a phase -1. Thus though we do not know what k is, this step is equivalent to *tagging* that particular state:

$$\sum_{x=0}^{N-1} (-1)^{f_k(x)} \; |x\rangle = |0\rangle + |1\rangle + \cdots - |k\rangle + \cdots + |N-1\rangle. \tag{8.73}$$

Algebraically, this step is equivalent to the action of the following *oracle operator* on the input register alone:

$$\hat{O} = \mathbb{1} - 2|k\rangle\langle k|, \tag{8.74}$$

since $|k\rangle\langle k|$ projects the state $|k\rangle$ out of the superposition. It helps to visualize this step, as well as the rest of the algorithm, by looking at what happens to the input state $|\psi\rangle$ in the Hilbert space $\mathcal{H}^{\otimes n}$. This space is spanned by the n unit vectors $\{|x\rangle\}$. Concentrate on the 2-d hyperplane spanned by the solution ket $|k\rangle$ and the vector $|\alpha\rangle$, a linear combination of all the other basis states, representing the hyperplane perpendicular to $|k\rangle$. You can visualize the input state $|\psi\rangle$ in this plane, as having a (small) component $\frac{1}{\sqrt{N}}$ along $|k\rangle$. The oracle operator $\hat{O}$ of Equation 8.74) reverses the sign of this component, performing a reflection in the hyperplane $|\alpha\rangle$ as shown in Figure 8.14.

Check out what this figure shows us. The initial uniform superposition is equally "far" from all the basis kets, including the target $|k\rangle$. In fact, it makes an angle

$$\theta = \sin^{-1} \frac{1}{\sqrt{N}} \tag{8.75}$$

with $|\alpha\rangle$ in this plane. The idea behind Grover's algorithm is to increase this

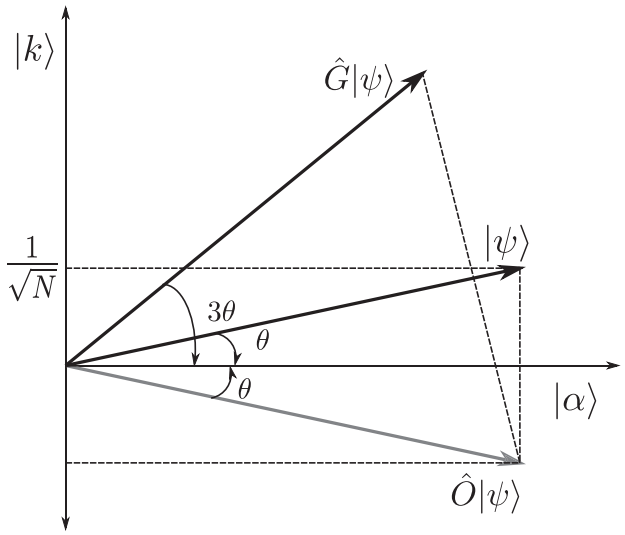


FIGURE 8.14: Geometric Visualization of the action of the Grover Iterate

angle to $\frac{\pi}{2}$ or as close to it as possible, by manipulating the phases of the state of the quantum computer.

Grover took a clue from the action of the operator $\hat{\mathcal{O}}$, and came up with another one $\hat{S}$, which implements a reflection in the plane of $|\psi\rangle$, which brings the input state closer to $|k\rangle$. By iterating this process a sufficient number of times, the input state $|\psi\rangle$ is rotated to $|k\rangle$. To see how this happens, let's construct $\hat{S}$:

$$\begin{aligned} \hat{S} &= \mathbb{1} - 2\big(\mathbb{1} - 2|\psi\rangle\langle\psi|\big) \\ &= 2|\psi\rangle\langle\psi| - \mathbb{1}. \end{aligned} \tag{8.76}$$

The action of the Grover iterate $\hat{G} = \hat{S}\hat{O}$ is to rotate the input state by an angle 3θ towards $|k\rangle$. This can be seen in the basis of vectors $|k\rangle$ and $|\alpha\rangle$:

$$\hat{G}|\psi\rangle = \cos 3\theta|\alpha\rangle + \sin 3\theta|k\rangle. \tag{8.77}$$

If this is repeated p times,

$$\hat{G}^p|\psi\rangle = \cos[(2p+1)\theta]|\alpha\rangle + \sin[(2p+1)\theta]|k\rangle. \tag{8.78}$$

Thus the iteration can stop when

$$\begin{aligned} (2p+1)\theta &\sim \frac{\pi}{2} \\ p &\sim \frac{1}{2\theta}\left(\frac{\pi}{2} - \theta\right). \end{aligned} \tag{8.79}$$

For large N, we have $\sin\theta = \frac{1}{\sqrt{N}} \simeq \theta$, so that the number of iterations required is given by

$$p = \frac{\pi}{4}\sqrt{N} - \frac{1}{2} = \mathcal{O}(\sqrt{N}). \tag{8.80}$$

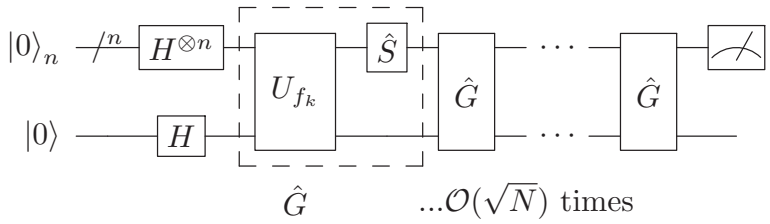


FIGURE 8.15: Circuit implementing Grover's algorithm

The circuit representation for this algorithm is given in Figure 8.15.

The process of rotating the superposition $|\psi\rangle$ towards the solution essentially works because of increasing the amplitude for $|k\rangle$, so this method goes under the name of "amplitude amplification".

Example 8.6.1. Let's look at the case $N = 4$, for 2-bit indices. The initial angle is given by $\sin\theta = \frac{1}{2} \implies \theta = \frac{\pi}{6}$. After a single iteration, the angle becomes $\frac{\pi}{2}$: thus a single run of the algorithm gives the answer.

Example 8.6.2. The deity who constructs the oracle in Grover's algorithm must give us a circuit implementing U_f for the checking the criterion. Let's say we have a 5-bit database and the 19^{th} entry is the search item. In binary, the index for the solution is $k = 18 = 10010$. The oracle output must be 1 for this input and 0 otherwise. It's easy to see that the circuit of Figure 8.16 will do the trick:

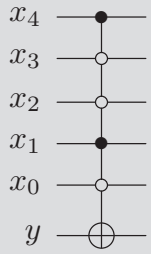


FIGURE 8.16: Construction of oracle for $k = 18$.

Example 8.6.3. We'll see how to construct the circuit for $\hat{S}$ (Equation 8.76).

$$\begin{aligned}\hat{S} &= -(\mathbb{1} - 2|\psi\rangle\langle\psi|) \\ &= -H^{\otimes n}\left(\mathbb{1} - 2|0\rangle\langle 0|\right)H^{\otimes n} \\ &= H^{\otimes n}\hat{P}H^{\otimes n}\end{aligned}$$

where the operator $\hat{P}$ leaves all basis states unchanged except $|0\rangle$, whose

sign is flipped. (We can also ignore the overall negative sign.) This can be implemented by an $(n-1)$-fold 0-controlled Z gate. Since $Z = HXH$, we have the circuit of Figure 8.17 for $\hat{S}$.

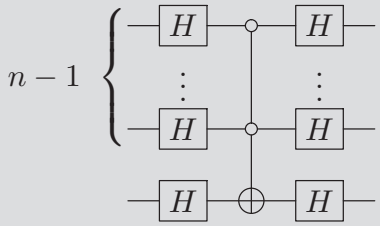


FIGURE 8.17: Construction of operator $\hat{S}$.

8.6.1 Extension to multiple solutions

A simple extension to this algorithm works when the search criterion has multiple solutions. The oracle then gives an answer "yes" whenever any one of the M possible solutions is input. The Hilbert space then has a "solution subspace" $\mathcal{M}$, spanned by M solution states. Let us denote by $|\beta\rangle$ the uniform superposition of all these vectors, and by $|\alpha\rangle$, its orthogonal complement.

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \in \mathcal{M}} |x\rangle, \tag{8.81}$$

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \notin \mathcal{M}} |x\rangle. \tag{8.82}$$

In this situation, the input state is

$$|\psi\rangle = \sqrt{\frac{M}{N}}|\beta\rangle + \sqrt{\frac{N-M}{N}}|\alpha\rangle. \tag{8.83}$$

The angle θ is now given by

$$\sin\theta = \langle\psi|\beta\rangle = \sqrt{\frac{M}{N}}. \tag{8.84}$$

The operator $\hat{O}$ tags all of the M solutions with a '$-$' sign, and the Grover iterate is defined the same way as before. After p iterations we get the state

$$\hat{G}^p|\psi\rangle = \cos[(2p+1)\theta]|\alpha\rangle + \sin[(2p+1)\theta]|\beta\rangle, \tag{8.85}$$

and the number of iterations required is nearly

$$p \approx \frac{\pi}{4}\sqrt{\frac{N}{M}}. \tag{8.86}$$

You should check for yourself that this works out.

8.6.2 Quantum counting

A fallout of the multiple search algorithm is the counting algorithm. Before we know how many times to iterate, we need to know how many solutions M there are to the search criterion. Can we deduce a quantum algorithm for finding M given U_{f_k}? The solution found by Brassard et al. [15], is a combination of Grover's search and Shor's phase estimation algorithms. The key point here is to note that the number of solutions is related to the eigenvalues of the operator $\hat{G}$, which can also be expressed in the $|\alpha\rangle$-$|\beta\rangle$ basis as the 2-d matrix

$$\hat{G} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \text{ where } \sin\varphi = 2\frac{\sqrt{M(N-M)}}{N}. \tag{8.87}$$

The eigenvalues of this matrix are $e^{\pm i\varphi}$. We can therefore use the phase estimation algorithm to deduce φ. We need to feed the algorithm with an eigenstate of $\hat{G}$. Now you can see for yourself that $|\psi\rangle$ is a linear superposition of the two eigenstates of $\hat{G}$, so the circuit of Figure 8.18 will work to t bits of accuracy.

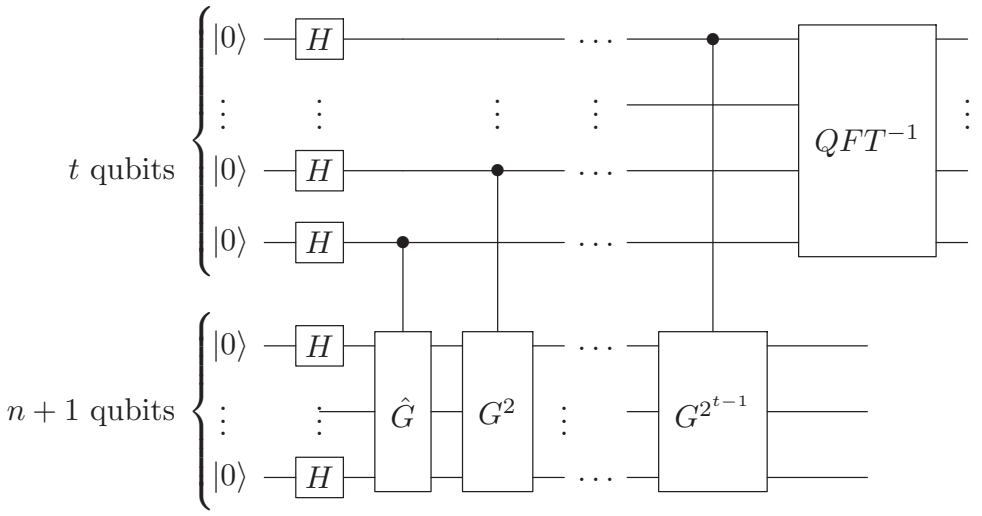


FIGURE 8.18: Circuit for quantum counting.

For Further Reading

The subject of quantum algorithms has rapidly evolved from its beginnings. Good references, apart from the original papers that may be found in the bibliography, are the excellent text book by Kaye, Laflamme, and Mosca [43] and the introductory text by Rieffel and Polak [58].

Problems

8.1. Some texts implement the quantum function evaluator as a "controlled-$\tilde{U}_f$" gate (Figure 8.19), where $\tilde{U}_f$ acts only on the lower register, and is defined by $\tilde{U}_f|y\rangle = |y \oplus f(x)\rangle$:

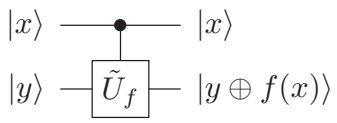


FIGURE 8.19: The quantum function evaluator as a controlled $\tilde{U}_f$ gate.

How is the action of this implementation different from the f-controlled NOT gate of Figure 7.15? Check by using standard basis states as well as superpositions as inputs.

8.2. Show that the phase kickback trick works because the input state in the bottom register is an eigenstate of the $\tilde{U}_f$ operator for the Deutsch algorithm.

8.3. Deutsch's original version of his algorithm used $|0\rangle$ as the input to the bottom register instead of $|0\rangle - |1\rangle$. Show that in this case you obtain the correct answer with probability $3/4$. Also show that the algorithm has probability $1/2$ of succeeding.

8.4. Prove the shift-invariance property of the Fourier transform, i.e., show that

$$\hat{\mathcal{F}}|x + k\rangle = e^{i\theta}\hat{\mathcal{F}}|x\rangle \tag{8.88}$$

for some θ. Find θ in terms of k.

8.5. For the operator R_d of Equation 8.45, give a construction for the controlled R_d gate using CNOT and single-qubit gates.

8.6. Find the eigenvalues and eigenvectors of the matrix R_d. What can you say about the commutators (i) $[R_d, X]$ (ii) $[R_d, Y]$ (iii) $[R_d, Z]$ (iv) $[R_d, R'_d]$?

8.7. Work out a circuit that calculates the inverse quantum Fourier transform.

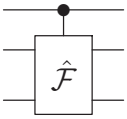
8.8. Consider a periodic function $f(x + r) = f(x)$ for $0 \leq x < N$ where N is

an integer multiple of r. Suppose you are given a unitary operator U_y that performs the transformation $U_y|f(x)\rangle = |f(x+y)\rangle$. Show that the state

$$|\tilde{f}(k)\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i k x/N} |f(x)\rangle \tag{8.89}$$

is an eigenvector of U_y. Calculate the corresponding eigenvalue.

8.9. Compute the output of the controlled-QFT gate shown in the figure if the input is $H^{\otimes 3}|x\rangle$.



8.10. On examining the period finding algorithm, we can find a relationship with the phase-estimation algorithm. On applying the oracle, we get

$$\frac{1}{\sqrt{N}} \sum |x\rangle|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{N}} \sum |f(x)\rangle.$$

Express $|f(x)\rangle$ in terms of its Fourier transform, $|\tilde{f}(k)\rangle$. Invert this expression and show that $|\tilde{f}(k)\rangle$ are of the same form as Equation 8.89 of Problem 8.8. Now show that the period finding algorithm is the phase estimation for the operator U_y defined there.

8.11. Apply the quantum phase estimation algorithm to the following cases and obtain the results:

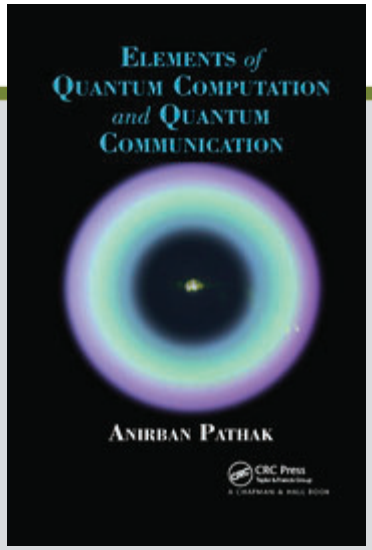
(a) $U = X, \quad |u\rangle = |-\rangle, \quad t = 2,$

(b) $U = R_d, \quad |u\rangle = |1\rangle, \quad t = d + 1.$

CHAPTER

3

QUANTUM GATES AND CIRCUITS



This chapter is excerpted from

Elements of Quantum Computation and Quantum Communication

by Anirban Pathake

Learn more

Chapter 4

Quantum gates and quantum circuits

Except for the NOT gate, all the other familiar classical gates are irreversible in the sense that we cannot uniquely reconstruct the input states from the output states. For example, OR, AND, NAND, NOR, etc. are irreversible. They all map a two-bit input state into a single bit output state. Thus one bit is erased during operation of each of these gates, and according to Landauer's principle that requires dissipation of a minimum amount of energy. Now a simple question arises in our curious mind: Is it possible to avoid this loss of energy? The answer is yes. If we don't erase any bit then we can circumvent this energy loss. Thus we need to map n bit input states to n bit output states. In addition, if a one-to-one correspondence exists between the input states and the output states then only we will be able to uniquely reconstruct the input states from the output states. In such a case the gate is called reversible. For example, if we have $f(00) = 00, f(01) = 10, f(10) = 01, f(11) = 11$ then f represents a reversible gate. Quantum evolution operators are unitary so for every operator U we have an inverse operator $U^{-1} = U^{\dagger}$. Therefore, quantum evolution operators are the natural choice for the construction of energy efficient reversible gates. However, it is not the only choice. We can have classical reversible gates, too. Usually by reversible gates we refer to classical reversible gates, and quantum gates are specifically referred to as quantum gates. Reversible gates and quantum gates are similar but there exists a fundamental difference that reversible gates cannot accept superposition states (e.g. $\alpha|0\rangle + \beta|1\rangle$) as input states, whereas quantum gates can. Thus all quantum gates are essentially reversible but the converse is not true.

In brief, simple unitary operations on qubits are called quantum logic gates. If a gate acts on a single qubit then it is called a single qubit gate.

Similarly, we can define a two qubit gate, three qubit gate and so on. We know that gates are combined together to form circuits, so in this chapter we will first describe single qubit gates, two qubit gates and three qubit gates. Then we will provide a few examples of quantum circuits and briefly describe the quantitative measures of the quality of the quantum circuits. We will also describe a few simple tricks that are usually used to improve the quality of quantum circuits. This chapter is focused on quantum gates and quantum circuits, but the techniques described here are also valid for reversible gates and reversible circuits.

4.1 Single qubit gates

A general structure of single qubit gates is shown in Fig. 4.1. Here the single qubit gate is a unitary operator which transforms a single qubit state $|\psi\rangle_{\text{in}}$ to another single qubit state $|\psi\rangle_{\text{out}} = U|\psi\rangle_{\text{in}}$. In this figure and in all the subsequent figures that depict quantum gates and quantum circuits, time moves from left to right, and each horizontal line represents a qubit. The horizontal lines are often referred to as qubit lines. Single qubit gates are represented by 2×2 unitary matrices. Every unitary operator (U), which is represented by a 2×2 matrix, is a valid single qubit gate. In principle, we can construct an infinite number of 2×2 unitary matrices. Consequently, there are an infinite number of possible single qubit quantum gates. However, in the conventional classical circuit theory, only two single bit logic gates are possible, namely the Identity gate and the logical NOT gate. Among this infinite number of possible single qubit quantum gates, some have special importance as they are used most frequently, and as they can be used as elements of a set of gates, which form a universal gate library. In this section we will briefly introduce these important and useful single qubit quantum gates, which are nothing but single qubit quantum state transformations. Since these transformations are linear, they are completely specified by their effect on the basis vectors. For instance, if we know that a single qubit quantum gate A maps $|0\rangle$ to $|\psi_0\rangle$ and $|1\rangle$ to $|\psi_1\rangle$ then linearity implies that the gate maps an arbitrary single qubit state $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|\psi_0\rangle + \beta|\psi_1\rangle$. Keeping this in mind, we will now describe the effect of important single qubit gates on the basis vectors $|0\rangle$ and $|1\rangle$ and will also provide the corresponding 2×2 unitary matrices that represent the gates.

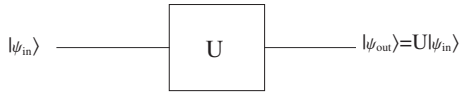


Figure 4.1: An arbitrary single qubit gate U.

1. **Pauli gates:** The quantum NOT gate transforms $|0\rangle$ to $|1\rangle$ and vice versa, so it is analogous to a classical NOT gate. But there is a fundamental difference with a classical NOT gate. A quantum NOT gate can accept a superposition state $\alpha|0\rangle + \beta|1\rangle$ as an input state, but a classical NOT gate cannot accept it as an input. The NOT gate is also called X gate since the unitary matrix that represents this gate is given by
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{4.1}$$
which is the same as the Pauli matrix σ_x. Consequently, this gate is also called the Pauli gate. It is easy to obtain the matrix (4.1). Suppose we don't know the matrix of the NOT gate, but we know that it transforms $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. A single qubit operation must be a 2×2 matrix since the states $|0\rangle$ and $|1\rangle$ are represented by column matrices of dimension 2×1. Now if we assume that the matrix for the NOT gate is NOT $= \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then using NOT$|0\rangle = |1\rangle$ we obtain
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$\Rightarrow a = 0,\ c = 1$$
and similarly, NOT$|1\rangle = |0\rangle$ implies $b = 1$ and $d = 0$. Thus we have obtained the matrix of the NOT gate. We can also express it in bra-ket notation as follows:
$$X = |0\rangle\langle 1| + |1\rangle\langle 0|. \tag{4.2}$$
One can quickly check that $X|0\rangle = |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle\langle 1|1\rangle + |1\rangle\langle 0|1\rangle = |0\rangle$. We can also obtain the matrix of NOT gate from (4.2) by replacing $|0\rangle$, $|1\rangle$, $\langle 0|$ and $\langle 1|$ by their equivalent matrices. The other two Pauli matrices (σ_y, σ_z) represent two more single qubit gates
$$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ and } Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.3}$$
In general X, Y, Z are known as Pauli gates. The quantum NOT or X gate just flips the bits. In analogy to X we can understand the effect of Y and Z on the single qubit state. For example Z will map an arbitrary quantum state $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|0\rangle - \beta|1\rangle$. Thus the sole effect of Z is to flip the relative phase. Y is actually a combination of bit flip and phase flip. To visualize this feature we may note that $Y = iXZ \equiv XZ$ (as the global phase does not have any meaning).
Now we provide a simple rule which will be found useful in the rest

of the book. If an arbitrary single qubit gate A maps $|0\rangle$ to a single qubit state $|\psi_0\rangle$ and $|1\rangle$ to another single qubit state $|\psi_1\rangle$ then we can write

$$A = |\psi_0\rangle\langle 0| + |\psi_1\rangle\langle 1|. \tag{4.4}$$

Similarly, if an arbitrary two qubit gate B maps $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ to two qubit states $|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{10}\rangle$ and $|\psi_{11}\rangle$ respectively then

$$B = |\psi_{00}\rangle\langle 00| + |\psi_{01}\rangle\langle 01| + |\psi_{10}\rangle\langle 10| + |\psi_{11}\rangle\langle 11|. \tag{4.5}$$

One can easily extend this simple rule to $n-$qubit gates and to other basis sets.

2. **Hadamard gate:** The Hadamard transformation is defined by the operation

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

and

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Thus the unitary matrix corresponding to this gate can be given as

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4.6}$$

and following (4.4) we can express it in bra-ket notation as

$$\begin{aligned} H &= \tfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\langle 0| + \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\langle 1| \\ &= \tfrac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|\right) \\ &= \textstyle\sum_{x,y=0}^{1}(-1)^{xy}|x\rangle\langle y|. \end{aligned}$$

Here we can easily observe that H is self-inverse as

$$HH = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

A self-inverse operator always maps the input states into mutually orthogonal output states and we can check that H maps $|0\rangle$ and $|1\rangle$ to mutually orthogonal states $|+\rangle$ and $|-\rangle$. A Hadamard operation can be described in a compact notation as

$$H\,|a\rangle = \frac{(-1)^a\,|a\rangle + |\bar{a}\rangle}{\sqrt{2}}, \tag{4.7}$$

where $a \in \{0, 1\}$.

3. **Phase gate or phase shift gate:** Consider a unitary operation that acts as $|0\rangle \to |0\rangle$, $|1\rangle \to \exp(i\phi)|1\rangle$. Thus it keeps $|0\rangle$ unchanged and changes the phase of $|1\rangle$ by $\exp(i\phi)$. We can represent this gate as
$$P(\phi) = |0\rangle\langle 0| + \exp(i\phi)|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\phi) \end{pmatrix}. \tag{4.8}$$
Since ϕ can have infinitely many values, we can have infinitely many different single qubit gates. This fact is in sharp contrast to the classical case where only one non-trivial single bit operation (NOT) is possible. Again among these infinitely many possible values of ϕ, particular values have drawn special attention. For example,
$$S = P\left(\frac{\pi}{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{4.9}$$
is often called a phase gate. $P(\frac{\pi}{4})$ is also a very popular gate and is often referred to as T gate or $\frac{\pi}{8}$ gate. Here a question is expected to arise in the reader's mind: Why is $P(\frac{\pi}{4})$ called $\frac{\pi}{8}$ gate? This unfortunate nomenclature arises from the fact that historically this gate was referred to as $\frac{\pi}{8}$ gate as up to a global phase this gate is equivalent to a gate which has $\exp\left(\pm\frac{i\pi}{8}\right)$ in its diagonals. To clarify this, we may note
$$T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\frac{\pi}{4}) \end{pmatrix} = \exp(i\frac{\pi}{8}) \begin{pmatrix} \exp(-i\frac{\pi}{8}) & 0 \\ 0 & \exp(i\frac{\pi}{8}) \end{pmatrix}. \tag{4.10}$$
Now we may show that $T^2 = S$ as follows:
$$T^2 = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\frac{\pi}{4}) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\frac{\pi}{4}) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\frac{\pi}{2}) \end{pmatrix} = S. \tag{4.11}$$
Another important point is that the $P(\phi)$ gates are not self-inverse gates in general. For example, $T^2 = S \neq I$ is the manifestation of the fact that $P(\phi)$ gates are not self-inverse. There is a special case $P(\pi) = Z$, which is self-inverse.
A very special case of $P(\phi)$ gate is
$$R_k = P\left(\frac{2\pi}{2^k}\right) = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{pmatrix}. \tag{4.12}$$
In Chapter 5 we show that R_k gates are very useful for the implementation of quantum Fourier transform operation which is required for implementation of Shor's algorithm.

4. **Rotation gates:** Rotation gates are defined as follows:
$$\begin{aligned} R_x(\theta) &= \mathrm{e}^{-\frac{i\theta X}{2}}, \\ R_y(\theta) &= \mathrm{e}^{-\frac{i\theta Y}{2}}, \\ R_z(\theta) &= \mathrm{e}^{-\frac{i\theta Z}{2}}. \end{aligned} \tag{4.13}$$

Now to obtain the matrix forms of these useful single qubit gates we have to prove a simple identity which is stated as:
Identity: If x is a real number and A is a matrix such that $A^2 = I$ then $e^{iAx} = I\cos(x) + iA\sin(x)$.
Proof:

$$\begin{aligned} e^{iAx} &= I + iAx - \tfrac{AAx^2}{2!} - \tfrac{iAAAx^3}{3!} + \tfrac{AAAAx^4}{4!} + \tfrac{iAAAAAx^5}{5!} \\ &= I\left(1 - \tfrac{x^2}{2!} + \tfrac{x^4}{4!} + \cdots\right) + iA\left(x - \tfrac{x^3}{3!} + \tfrac{x^5}{5!} + \cdots\right) \\ &= I\cos(x) + iA\sin(x). \end{aligned} \tag{4.14}$$

We have already seen in Subsection 3.1.3 that the squares of Pauli matrices are Identity (i.e., $\sigma_i^2 = I$). Now we can use this property of Pauli matrices and the above identity (4.14) to provide matrices for rotation gates as follows:

$$\begin{aligned} R_x(\theta) &= I\cos(\tfrac{\theta}{2}) - iX\sin(\tfrac{\theta}{2}) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\cos(\tfrac{\theta}{2}) - i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\sin(\tfrac{\theta}{2}) \\ &= \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}, \\ R_y(\theta) &= I\cos(\tfrac{\theta}{2}) - iY\sin(\tfrac{\theta}{2}) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\cos(\tfrac{\theta}{2}) - i\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\sin(\tfrac{\theta}{2}) \\ &= \begin{pmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}, \\ R_z(\theta) &= I\cos(\tfrac{\theta}{2}) - iZ\sin(\tfrac{\theta}{2}) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\cos(\tfrac{\theta}{2}) - i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\sin(\tfrac{\theta}{2}) \\ &= \begin{pmatrix} \mathrm{e}^{-i\frac{\theta}{2}} & 0 \\ 0 & \mathrm{e}^{i\frac{\theta}{2}} \end{pmatrix}. \end{aligned} \tag{4.15}$$

Now we may recall Equation (3.108) of the previous chapter, where we had described an arbitrary qubit in a Bloch sphere as $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)e^{i\phi} \end{pmatrix}$. If we apply the rotational gate $R_z(\theta_1)$ on this Bloch state then the state will be transformed to

$$\begin{aligned} R_z(\theta_1)|\psi\rangle &= \begin{pmatrix} \mathrm{e}^{-i\frac{\theta_1}{2}} & 0 \\ 0 & \mathrm{e}^{i\frac{\theta_1}{2}} \end{pmatrix}\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)\mathrm{e}^{i\phi} \end{pmatrix} \\ &= \mathrm{e}^{-i\frac{\theta_1}{2}}\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)\mathrm{e}^{i(\phi+\theta_1)} \end{pmatrix} \\ &= \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)\mathrm{e}^{i(\phi+\theta_1)} \end{pmatrix}. \end{aligned} \tag{4.16}$$

In the last step of the previous equation we ignored the global phase. Now one can easily see that $R_z(\theta_1)$ has rotated the Bloch vector by an angle θ_1 about the z axis of the Bloch sphere. Similarly, $R_x(\theta_1)$ and $R_y(\theta_1)$ gates rotate the Bloch vector by an angle θ_1 with respect to x and y axes respectively.

5. **Square-root-of-NOT gates:** This interesting single qubit gate is usually denoted as V gate or $\sqrt{\text{NOT}}$ gate. In matrix representation

$$V = \sqrt{\text{NOT}} = \frac{(1+i)}{2}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}.$$

Now it is easy to see that

$$VV = \frac{1}{4}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \text{NOT}.$$

This is why V gate is called $\sqrt{\text{NOT}}$ gate. Now we can quickly check that $V^\dagger = \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$ satisfies the following relations: $VV^\dagger = V^\dagger V = I$ and $V^\dagger V^\dagger = \text{NOT}$. Therefore, $V^\dagger = V^{-1} = \sqrt{\text{NOT}}$. In other words, $\sqrt{\text{NOT}}$ operation can be described by both V and $V^\dagger$ but usually we use V to represent $\sqrt{\text{NOT}}$ gate.

4.2 Two qubit gates

1. **Controlled-NOT gate:** The most popular and the most important example of a two qubit gate is the controlled − NOT or CNOT gate, which complements the second qubit if the first qubit is in the state $|1\rangle$ and leaves the second qubit unchanged otherwise. Thus the matrix representation for this gate is

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{4.17}$$

Alternatively, it can also be represented in bra-ket notation (Dirac notation) as

$$\text{CNOT} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|.$$

As the state of the first qubit controls whether the second qubit will be flipped or not, the first qubit is referred to as control qubit and the second qubit is called target qubit. The same convention is used in other controlled gates. In multiqubit gates there may exist more

than one control qubit. The basic reason of the popularity of the CNOT gate is twofold, firstly it is used in many quantum circuits of practical importance and secondly if we can construct all single qubit gates and CNOT gate then we can construct any other unitary quantum operation with suitable combination of these gates. Specifically, if we can physically realize all single qubit gates and any two qubit entangled quantum gate[1] then in principle we can construct all possible quantum circuits. In most of the physical realization of two qubit gates, CNOT is reported and gradually it has become almost synonymous to universal gate (a quantum correspondent of classical NAND). A symbolic representation of CNOT is shown in Fig. 4.2.

2. **Swap gate:** Another popular two qubit gate is the SWAP gate. It swaps the states of the two qubits; thus it maps $|ab\rangle \rightarrow |ba\rangle$ (i.e., $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |10\rangle$, $|10\rangle \rightarrow |01\rangle$ and $|11\rangle \rightarrow |11\rangle$) and it can be represented as
$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.18}$$
Following (4.5) we can write it in bra-ket notation as
$$\text{SWAP} = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|.$$
Symbolic representation of the SWAP gate is shown in Fig. 4.2, and in Fig. 4.3 we have shown that the SWAP gate can be constructed by using three CNOT gates.

3. **Controlled-U gates:** If U is an arbitrary single qubit gate (unitary operation) then we may construct a two qubit Controlled$-U$ gate, such that the single qubit operation U operates on the second (target) qubit if the first (control) qubit is in state $|1\rangle$, otherwise the input state remains unchanged. Thus the Controlled$-U$ gate maps $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |01\rangle$, $|10\rangle \rightarrow |1\rangle \otimes U|0\rangle$, $|11\rangle \rightarrow |1\rangle \otimes U|1\rangle$. In Dirac notation such a gate is described in general as
$$\text{Controlled}{-}U = |00\rangle\langle 00| + |01\rangle\langle 01| + |1\rangle \otimes U|0\rangle\langle 10| + |1\rangle \otimes U|1\rangle\langle 11|$$
and the corresponding matrix is
$$\text{Controlled}{-}U = \begin{pmatrix} I & O \\ O & U \end{pmatrix}, \tag{4.19}$$
where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ are respectively the Identity and Null operations (gate) in C^2. Now we can see that CNOT is just

[1] By an entangled two qubit gate we mean a two qubit gate which cannot be achieved as tensor product of two single qubit gates.

a special case of Controlled$-U$ where $U = X$. In a similar fashion we may construct Controlled$-T$, Controlled$-P(\phi)$, Controlled$-R_x(\theta)$, etc. and it is a straightforward job to write the corresponding matrices. As examples, we may explicitly write the matrices for Controlled$-V$ and Controlled$-V^\dagger$gates as follows:

$$\text{Controlled}-V = \begin{pmatrix} I & O \\ O & V \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1+i}{2} & \frac{1-i}{2} \\ 0 & 0 & \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \tag{4.20}$$

$$\text{Controlled}-V^\dagger = \begin{pmatrix} I & O \\ O & V^\dagger \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1-i}{2} & \frac{1+i}{2} \\ 0 & 0 & \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix}. \tag{4.21}$$

Controlled$-V$ and Controlled$-V^\dagger$ are very often used in construction of more complex quantum gates and quantum circuits. Actually {NOT, CNOT, Controlled$-V$, Controlled$-V^\dagger$} forms a universal gate library for reversible circuits. Such a gate library is referred to as NCV gate library. As $\sqrt{\text{NOT}}$ or Controlled $-\sqrt{\text{NOT}}$ operations cannot be achieved classically so NCV is actually a quantum gate library which is universal for classical reversible operations.

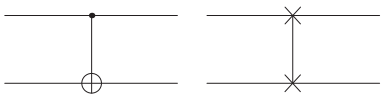


Figure 4.2: CNOT (left) and SWAP (right) gates.

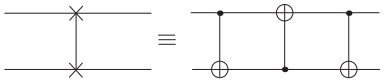


Figure 4.3: SWAP gate as composition of CNOTs.

4.3 Three qubit gates

1. **Toffoli gate and Fredkin gate:** The three qubit gates used in the quantum circuits are generally either controlled-controlled single qubit gate or controlled two qubit gate. The most popular three

qubit gates are the Toffoli gate and Fredkin gate, which are CCNOT and CSWAP gates respectively. Thus in the three qubit Toffoli gate the first two qubits are control qubits and the third one is the target qubit. So the third qubit will be flipped only if both the first and second qubits are in state $|1\rangle$. Similarly, in the case of the Fredkin gate the swap operation between the second and third qubit is done only if the first qubit (i.e., the control qubit) is at state $|1\rangle$. Now we can write the unitary matrices representing these two quantum gates as

$$\text{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{4.22}$$

and

$$\text{Fredkin} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.23}$$

respectively. Here we would like to note that a quantum Toffoli gate can be built up from CNOT and single qubit gates but a classical (reversible) Toffoli gate cannot be built using two bit and one bit classical reversible gates. Symbolic representations of Toffoli and Fredkin gates are provided in Fig. 4.4.

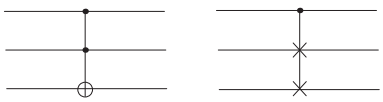


Figure 4.4: Toffoli (left) and Fredkin (right) gates.

2. **Deutsch gate:** TheDeutsch gate was introduced by David Deutsch

in 1989 as a universal quantum gate. This gate is defined as

$$\text{Deutsch}(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & i\cos(\theta) & \sin(\theta) \\ 0 & 0 & 0 & 0 & 0 & 0 & \sin(\theta) & i\cos(\theta) \end{pmatrix},$$

where θ is a constant angle such that $\frac{2\theta}{\pi}$ is an irrational number. This choice isolates Toffoli gate as $D\left(\frac{\pi}{2}\right) \equiv$ Toffoli. $\{\text{Deutsch}(\theta)\}$ forms a universal quantum gate library. However, circuits built using this gate library are usually inefficient and this is why this particular gate library is not used very frequently [63].

4.4 A little more on quantum gates

Here we would like to note an interesting feature of quantum gates. If a quantum gate is self-inverse then it will always map input states to mutually orthogonal output states. For example, consider a single qubit gate A, which maps $|0\rangle$ to $|\psi_0\rangle$ and $|1\rangle$ to $|\psi_1\rangle$ (i.e., $A = |\psi_0\rangle\langle 0| + |\psi_1\rangle\langle 1|$). If it is self-inverse (i.e., $A = A^{-1} = A^\dagger$) then $\langle 0|A = \langle\psi_0| \Rightarrow \langle 0| = \langle\psi_0|A^{-1} = \langle\psi_0|A = \langle\psi_0|\psi_0\rangle\langle 0| + \langle\psi_0|\psi_1\rangle\langle 1| \Rightarrow \langle\psi_0|\psi_1\rangle = 0$, $\langle\psi_0|\psi_0\rangle = 1$. The idea can be easily extended to n-qubit systems. In general outputs of self-inverse gates are mutually orthogonal. But the converse is not true. That means there exist quantum gates that are not self-inverse but that map input states to mutually orthogonal output states.

Now we can note another interesting point. A unitary operator A must satisfy $A^{-1} = A^\dagger$ and a Hermitian operator A must satisfy $A = A^\dagger$. Consequently, all unitary operators are not Hermitian and all Hermitian operators are not unitary. If a unitary operator is Hermitian then $A^{-1} = A^\dagger = A$, i.e., $A = A^{-1}$, so the operator is self-inverse. We can easily show the converse (i.e., self-inverse unitary operators are Hermitian). This implies that quantum gates represented by Hermitian unitary operators always map input states to mutually orthogonal states. Now we can observe that the CNOT gate $|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$ is self-inverse, so it is Hermitian. We can easily drop the symmetry required for the gate to be self-inverse and modify it to another quantum gate $B = |01\rangle\langle 00| + |11\rangle\langle 01| + |10\rangle\langle 10| + |10\rangle\langle 11|$. You can easily check that this gate is not self-inverse as $BB|00\rangle = B|01\rangle = |11\rangle \neq |00\rangle$. Thus this gate is not Hermitian but interestingly it is unitary and it maps the input states into a set of mutually orthogonal output states.

Now we may ask some simple questions: (1) How many such quantum gates are possible that can map input states to mutually orthogonal states? This question is relevant from several perspectives. Especially in the secure quantum communication we need the output states to be mutually orthogonal. (2) How many of these gates are non-Hermitian (non-self-inverse)? (3) Can we physically construct a unitary non-Hermitian gate with the help of a Hermitian Hamiltonian?

Assume that we are working in M dimension and the input states are $\{|a_1\rangle, |a_2\rangle, |a_3\rangle, \cdots, |a_M\rangle\}$. Thus $\{|a_j\rangle\}$ forms our input basis set. Similarly, assume that $\{|b_j\rangle\}$ represent a new basis set in the same dimension and $\{|b_j\rangle\}$ is our output basis set. For quantum gates $\{|b_j\rangle\}$ may or may not be a permutation of $\{|a_j\rangle\}$. Now we may introduce the operators $U_J = \sum_j |b_j\rangle\langle a_j|$, which are unitary, as is easily verified to satisfy $U_J U_J^\dagger = U_J^\dagger U_J = \left(\sum_p |a_p\rangle\langle b_p|\right)\left(\sum_q |b_q\rangle\langle a_q|\right) = \left(\sum_j |a_j\rangle\langle a_j|\right) = I_M$, where I_M is the identity operation in M dimension. We can elaborate the idea with a few examples.

Example 4.1: Consider SWAP gate. Here $\{|a_j\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and $\{|b_j\rangle\} = \{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$ and so

$$U_J = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| = \text{SWAP}.$$

Example 4.2: Consider a gate where $\{|a_j\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and $\{|b_j\rangle\} = \{|00\rangle, |01\rangle, |11\rangle, |10\rangle\}$. In this case

$$U_J = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| = \text{CNOT}.$$

Example 4.3: In the last two examples output basis $\{|b_j\rangle\}$ is just a permutation of input basis $\{|a_j\rangle\}$. How many such gates are possible where output basis is a permutation of input basis?

Solution: Arbitrary permutation on M basis vectors can be achieved in $M!$ ways; each of these permutations will provide us with a unitary operator. Thus each of these $M!$ unitary operators U_J is a quantum gate that always maps input states into mutually orthogonal output states. We may call these quantum gates as permutation gates. In brief, we have $M!$ permutation gates of the given type.

Example 4.4: How many reversible n-bit gates are possible?

Solution: As for reversible gates superposition states are not allowed in input and output, so $\{|a_j\rangle\}$ is always in computational basis and $\{|b_j\rangle\}$ is just a permutation of input basis $\{|a_j\rangle\}$. Consequently, only $M!$ gates are possible, where $M = 2^n$. Thus the number of possible 2-bit reversible gates is $4! = 24$.

Example 4.5: How many quantum permutation gates are possible?

Solution: Infinite. We have already mentioned that $\{|b_j\rangle\}$ is not essentially a permutation of input basis $\{|a_j\rangle\}$ and the basis vectors of $\{|b_j\rangle\}$ can be in superposition states. Consider, $\{|a_j\rangle\} = \{|0\rangle, |1\rangle\}$ and $\{|b_j\rangle\} =$

$\{|+\rangle, |-\rangle\}$, then U_J = Hadamard. In general, for each combination of $\{|a_j\rangle\}$ and $\{|b_j\rangle\}$ we can have $M!$ gates and there exist infinitely many possible combinations of $\{|a_j\rangle\}$ and $\{|b_j\rangle\}$. For example, in single qubit cases we can think of $\{|b_j\rangle\} = \{\sin(\theta)|0\rangle + \cos(\theta)|1\rangle, \cos(\theta)|0\rangle - \sin(\theta)|1\rangle\}$. For each choice of θ we have a new basis set. So it is straightforward to see that the number of quantum permutation gates is infinite. But for a specific choice of combination of input basis set and output basis set it is finite ($M!$). In this discussion we have considered that$\{|a_j\rangle\}$ is fixed and each permutation of $\{|b_j\rangle\}$ provides a new quantum gate.

Example 4.6: Are these $M!$ gates self-inverse/Hermitian?

Solution: These unitary gates are not essentially self-inverse/Hermitian. Our task is to find out the number of self-inverse permutations on M letters which is known as involutions. For $M = 1, 2, 3, \cdots$ number of alternating permutations are $1, 2, 4, 10, 26, 76, 232, 764, \cdots$. This implies that in C^{2^2} (i.e., for $M = 4$) we can have 10 self-inverse gates for a specific choice of $\{|a_i\rangle\}$ and $\{|b_j\rangle\}$, which implies that $4! - 10 = 14$ two qubit gates are not self-inverse. Similarly, in C^{2^3} we have $8! - 764 = 39556$ non-Hermitian permutation gates and only 764 Hermitian permutation gates. Therefore, 98.10% of the gates are non-Hermitian (nonself-inverse).

We elaborate on this point just to show that most of the classical reversible gates are not self-inverse and most of the quantum gates are not Hermitian. Here it would be apt to note that this apparent non-Hermiticity does not contradict standard quantum mechanics. Quantum mechanics demands that the Hamiltonian of a quantum system should be Hermitian and that leads to the unitary operators. The evolution operators (quantum gates) are required to be unitary only, they are not bound to be Hermitian as they do not represent physical observables. Thus all the unitary but non-Hermitian quantum gates constructed here are physically realizable and perfectly consistent with quantum mechanics.

We have already learned about single qubit, two qubit and three qubit quantum gates, now we may combine them to form some simple quantum circuits. This is what we do in the next section.

4.5 Quantum circuits

The quantum gates are combined to form quantum circuits. In the subsequent chapters we describe several useful quantum circuits in relation to quantum teleportation, dense coding and quantum algorithms. Here we describe a few simple quantum circuits. To begin with, let us consider a simple circuit comprised of a Hadamard gate followed by a CNOT gate as shown in Fig. 4.5. The operation of this circuit can be mathematically understood as follows. We start with a separable state $|00\rangle$. Thus the input state of the circuit is $|00\rangle$. Then a Hadamard gate operates on the first (upper) qubit and transforms the state of the system to another separable

state $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$. Now the CNOT gate operates with the first qubit working as the control qubit and the second qubit working as the target qubit. We have already learned that the CNOT gate flips the target qubit, when the control qubit is $|1\rangle$. Therefore, after the CNOT operation the output state of the circuit is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which is maximally entangled.

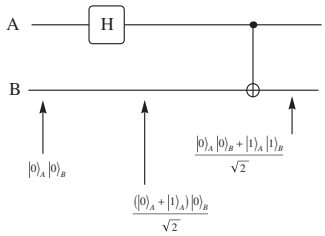


Figure 4.5: EPR circuit.

A computational task can be performed by using more than one quantum circuit. Such an example is shown in Fig. 4.6a and Fig. 4.6b, where both the circuits represent quantum half adder. Now a question naturally appears in our mind: Which of these two circuits is better? To answer this question we need some quantitative measure of the quality of circuits. Normally such a quantitative measure is referred to as cost or cost metric of the circuit. Different quantitative measures of quality of quantum circuits exist and a few of them are described in the following subsection. The circuit shown in Fig. 4.5 is known as an EPR circuit and we can easily justify this nomenclature if we note that when the input state of the EPR circuit is $|1\rangle_A|1\rangle_B$ then the output of the EPR circuit is the singlet state $\left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right)_{AB}$.

4.5.1 Quantitative measures of quality of a circuit

Some of the important quantitative measures of the quality of a quantum circuit are gate count (circuit cost), number of garbage bits, quantum cost and delay. We will briefly introduce each of them in this subsection. Let us begin with gate count, which is usually referred to as circuit cost.

4.5.1.1 Gate count or circuit cost

Gate count or circuit cost is the total number of gates present in a circuit. This is an important measure of quality of circuit. The lesser the circuit cost is the better the circuit is. But unfortunately, circuit cost is not

unique. One may substantially reduce the circuit cost by using complex gate library and/or new gates. For example, let us consider the EPR circuit shown in Fig. 4.5. The circuit is composed of two gates from the universal gate library $\{H, S, T, \text{CNOT}\}$. Therefore, its gate count (circuit cost) is 2. Now we can put the two gates in a box and call it a new gate. The matrix of the new gate would be

$$\begin{aligned}
\text{CNOT}\,(H \otimes I_2) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
&= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \\
&= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}.
\end{aligned}$$

Now if we consider it as a new gate

$$\text{NEWG} = \text{CNOT}\,(H \otimes I_2) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

then we can easily find that this gate maps $|00\rangle$ to $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $|01\rangle$ to $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$, $|10\rangle$ to $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$ and $|11\rangle$ to $\frac{|01\rangle-|10\rangle}{\sqrt{2}}$. Thus this NEWG is a new gate which is equivalent to the EPR circuit and which reduces the circuit cost of the EPR circuit to 1. It may appear advantageous to use such new and complex gates to reduce the circuit cost. However, it is not allowed. If it is allowed then every quantum circuit block without measurement would have reduced to a single gate. This is so because the product of an arbitrary number of unitary operations is always unitary. Circuits are constructed using standard universal gate libraries and circuit cost of a circuit A can be compared with the circuit cost of another circuit B if and only if the circuit costs are calculated using the same gate library. Often we need to compare circuits designed using different gate libraries. In that case we need to transform one of the circuits into a logically equivalent and optimized circuit prepared in the other gate library. In brief, it is important to define a unique gate library for comparison of circuit costs. See the circuits shown in Fig. 4.6. Both represent half adder and both are constructed using the gates from NCV gate library, but the gate count of the circuit shown in Fig. 4.6b is less than the gate count of the circuit shown in Fig. 4.6a.

Irreversible		Reversible	
Input	Output	Input	Output
AB	Z	ABC	XYZ
00	0	000	000
01	0	010	010
10	0	100	100
11	1	110	111

Table 4.1: Irreversible and reversible AND gate. X and Y bits in the output of reversible AND gate are the garbage bits.

Hence the circuit shown in Fig. 4.6b is better than the circuit shown in Fig. 4.6a as far as the circuit cost is concerned.

4.5.1.2 Garbage bit

A garbage bit is the additional output that is used either to make a function reversible or to reduce the gate count. Garbage bits are not used for further computations. Large numbers of garbage bits are undesirable in a quantum/reversible circuit as it increases the width of the circuit. As an example in Table 4.1 we have described the truth table of an irreversible and a reversible AND gate. It is evident that the output Z gives us the required output of AND gate in both the cases. To be precise, we may use a Fredkin gate as AND gate if we use $|AB0\rangle$ as input (i.e., we keep the third input bit at a constant value of 0). In that case we will obtain the truth table of reversible AND gate described in Table 4.1. Here the third output bit of the Fredkin gate will be $Z = AB$, which is the required output of AND gate. As we are interested to implement an AND gate only, the other two outputs of the Fredkin (reversible AND) gate (i.e., X and Y) will not be used for further computation and they are the garbage bits. Similarly, if we use $|A1B\rangle$ as input in a Fredkin gate then we obtain a reversible OR gate. Here the third bit of output is $Z = A + B$, which is the desired output of OR gate and the other two outputs are garbage bits. We can also note that the first two output bits in the half adder circuits shown in Fig. 4.6a and Fig. 4.6b are garbage bits. It is important to note that the garbage bits are often introduced to make a function reversible and there can be many ways in which garbage values can be assigned. A circuit having a lesser number of garbage bits is better than the one performing the same task with a higher number of garbage bits. This is an important quantitative measure of quality of quantum circuit.

4.5.1.3 Quantum cost

The quantum cost of a reversible/quantum gate/circuit is the number of primitive quantum gates needed to implement the gate/circuit. Primitive

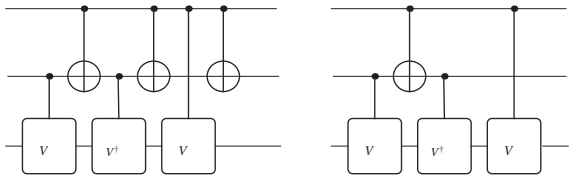


Figure 4.6: Quantum circuit of half adder is presented in two different ways: (a) Circuit cost and quantum cost of this quantum half adder circuit is 6 and width is 3. (b) Circuit cost and quantum cost of this quantum half adder circuit is 4 and width is 3. Circuit (b) is better than (a) as far as circuit cost and quantum cost are concerned. Local optimization tools like moving rule and deletion rule can be used to obtain circuit (b) from circuit (a).

quantum gates are the elementary building blocks, like NOT gate, CNOT gate, controlled-V, controlled-$V^\dagger$, rotation gates, etc. In fact all single qubit and 2-qubit gates are considered as quantum primitive gates and the cost of all quantum primitive gates are considered as one. Since Toffoli gate is not a quantum primitive gate, an NCT circuit (i.e., a circuit built using gates from the gate library $\{\text{NOT}, \text{CNOT}, \text{Toffoli}\}$)[2] cannot be used directly to determine the quantum cost. But Toffoli can be constructed using CNOT gate, controlled-V and controlled-$V^\dagger$ and that may reveal that the quantum cost of Toffoli gate is five. This helps us to convert an NCT circuit into an equivalent NCV circuit and then to optimize the NCV circuit to obtain the quantum cost. It is important to note that while computing the quantum cost we are allowed to combine gates and form new two qubit gates. This important feature isolates quantum cost from the circuit cost obtained in NCV or any other gate library where all the elements of the universal gate set are the quantum primitive gates. Further, quantum cost is often classified as linear quantum cost and nonlinear quantum cost. Given a circuit, if we just add the quantum costs of each of the gates used in the circuit then we obtain the linear quantum cost. However, if we replace all the 3-qubit and larger gates of the given circuit by their equivalent circuits built using quantum primitive gates and subsequently optimize the circuit without restricting us to any gate library then the gate count of the optimized circuit is called nonlinear quantum cost. The lesser the quantum cost, the better the circuit.

Example 4.7: The quantum circuit of a half adder is presented in two

[2] $\{\text{NOT}, \text{CNOT}, \text{Toffoli}\}$ forms a universal gate library for reversible circuits. It is known as the NCT gate library.

different ways in Fig. 4.6. The circuit shown in Fig. 4.6b is better than the circuit shown in Fig. 4.6a as its quantum cost is less.

4.5.1.4 Depth and width of a circuit

In addition to the measures discussed above, Kaye, Laflamme and Mosc [54] have prescribed two more important measures of complexity of a circuit (i) width (number of qubit lines) and (ii) depth (total number of time slices) of a circuit. These two measures are already introduced in Section 2.3. Mohammadi and Eshghi [64] have described another measure called delay which is closely related to the depth of the circuit. Delay is a technology dependent parameter and it provides a measure of how much time is required to evaluate a function. If we approximate that the evolution of each single qubit and two qubit gates require Δ amount of time then delay of a circuit = (depth of the circuit using primitive quantum gates)Δ. Delay is proportional to depth and we may consider them as the same measure.

Now it is easy to note that the more is the number of garbage bits in a circuit the more will be the width of the circuit. Further, a circuit having lesser width requires lesser space. Consequently, if we have two circuits for the same task then the circuit having lesser width is better. Similarly, the lesser the depth of a circuit, the better it is as it would take less time to perform the computational task. Now look at Fig. 4.7, where a schematic diagram of a general quantum circuit is shown. Each rectangular box represents a quantum gate and each vertical line is a separator between two time slices. If we consider Fig. 4.7 as an optimized circuit built using quantum gates from a well defined gate library, then there are 8 quantum gates, so its circuit cost is 8. But there are disjoint quantum gates which can be applied simultaneously as shown in the first, second and the last time slices of Fig. 4.7. So the depth of the circuit is 5. Further, there are 6 qubit lines so the width of the circuit is 6. However, we cannot directly compute the delay as three nonprimitive quantum gates are used here. We may now look back to Fig. 4.6a and Fig. 4.6b. It is easy to observe that width of both the circuits is 3. Depth and delay of the circuit shown in Fig. 4.6a are 6 and 6Δ respectively. Similarly, depth and delay of the circuit shown in Fig. 4.6b are 4 and 4Δ respectively. Consequently, as far as the depth and delay are concerned circuit shown in Fig. 4.6b is better than the circuit shown in Fig. 4.6a.

4.5.1.5 Total cost

A circuit is better if it has a lesser number of garbage bits, circuit cost and quantum cost. But it is often observed that reduction of circuit cost leads to increase in garbage bits and reduction of quantum cost leads to increase in circuit cost [65]. A new parameter called "total cost" (TC), which is the sum of gate count of an optimized circuit, number of garbage

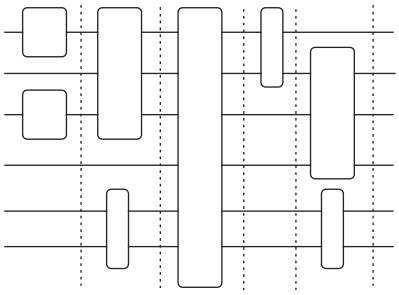


Figure 4.7: A schematic diagram of quantum circuit. Here each vertical line separates two time slices and each rectangular box represents a quantum gate. So depth of the circuit is 5. We cannot directly compute delay as the circuit uses three nonprimitive quantum gates.

bits and quantum cost, is recently introduced [66]. For reduction of TC, we need to simultaneously reduce the circuit cost, garbage count (number of garbage bits) and quantum cost. This is an open problem and at present neither an algorithm for simultaneous reduction of all these measures nor a satisfactory algorithm for reduction of quantum cost exists. Here it would be apt to note that TC is a weak measure of quality of a circuit.

4.5.2 Circuit optimization rules

In the previous section we observed that there exist several measures of quality of a quantum circuit and the lesser the value of a particular measure, the better is the circuit. So we need to optimize quantum circuits. Global optimization of a large quantum circuit is difficult. Most of the tools used for optimization of quantum circuits are actually local optimization tools. To be precise, instead of optimizing the whole circuit, they locally optimize comparatively smaller circuit blocks of the large quantum circuit. Some interesting techniques of circuit optimization are discussed below.

4.5.2.1 Moving rule

Moving rule is a consequence of commutation rule. Let quantum gates U_1, U_2 and U_3 be placed in sequence in a circuit. Thus our circuit is $U_1U_2U_3$. Now if $U_1U_2{=}U_2U_1$ (i.e., if $[U_1, U_2] = 0$) then we can interchange the first two gates (equivalently we can move the first (second) gate in right (left) by one step) to obtain an equivalent circuit $U_2U_1U_3$. A simple example that demonstrates the moving rule is shown in Fig. 4.8. Here it would be apt to note that a specific application of moving rule in the optimization of

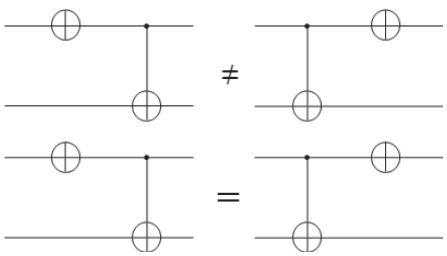


Figure 4.8: An example of commutation rule in context of quantum circuits. If a NOT gate is placed at the control qubit line of a CNOT gate it does not commute with the CNOT gate but if a NOT gate is placed at the target qubit line then it commutes with the CNOT gate.

a quantum circuit can be visualized through deletion rule. If moving rule brings two inverse gates (two CNOT gates or controlled-V and controlled-$V^\dagger$) in two consecutive positions in the same qubit lines then the pair of gates would be deleted and that would lead to optimization of the circuit. Let us now provide two explicit examples to show that moving rule and deletion rule are useful for optimization of the quantum circuits.

Example 4.8: Consider the circuit shown in Fig. 4.6a. Here the last two gates commute. So we can move the last CNOT gate to the left of the adjacent controlled-V gate. This movement brings two CNOT gates in consecutive positions. As CNOT is self-inverse so CNOT(CNOT) = I and we can delete the consecutive CNOTs (here we are applying deletion rule) to obtain the optimized circuit shown in Fig. 4.6b. We have already seen that the circuit shown in Fig. 4.6b is better than the circuit shown in Fig. 4.6a with respect to different cost metrics. Consequently, moving rule and deletion rule are useful for reduction of different quantitative measures of quality of quantum circuits.

Example 4.9: Consider the circuit shown on the left hand side of Fig. 4.9, where the first two gates commute. After application of moving rule we obtain the equivalent circuit where two V gates appear in consecutive positions in the second qubit line. As VV = NOT so we can replace these two V gates by a NOT gate and obtain an optimized circuit comprised of two gates. The optimized circuit is shown on the right hand side of the circuit identity shown in Fig. 4.9.

4.5.2.2 Template matching

A template is a circuit that makes an Identity. A trivial example is $VV\,X = I$. Now in the previous example, two VV gates appeared in consecutive positions on the same qubit line. In that case, we can use the template

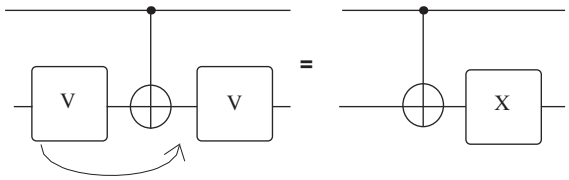


Figure 4.9: Local optimization of a circuit using moving rule and template matching. Here the first V gate commutes with the CNOT gate. The movement of the V gate is shown with the arrow. Subsequently $VVX = I$ template is used to replace two consecutive V gates by a X gate.

$VV\,X = I$ to obtain $VV = X^{-1} = X$ and replace VV by X gate to reduce the gate count. This is a simple example. In general, if more than half of the consecutive quantum gates present in a given template appear in consecutive positions in a quantum circuit then we can use the template to reduce the gate count. For example, look at the schematic diagram of a general quantum circuit shown in Fig. 4.10a. In Fig. 4.10b we show a template. We observe that the three consecutive gates which are shown in a rectangular box in Fig. 4.10a are the same as the first three gates of the template shown in Fig. 4.10b. Now the template shown in Fig. 4.10b implies the circuit identity shown in Fig. 4.10c. We can now use the right hand side of the circuit equation shown in Fig. 4.10c to replace the three gates shown in the rectangular box in Fig. 4.10a. This will lead to reduction of gate count and we will obtain the circuit shown in Fig. 4.10d. This is how template matching works. The template matching is of two types: forward matching and backward matching.

Forward matching and backward matching

Let us consider a template $U_1U_2U_3U_4U_5U_6 = I$. For simplification we assume that $U_i = U_i^{-1}$. Now if a sequence of gates $U_3U_4U_5U_6$ appears in a circuit, then this sequence of gates can be replaced by $U_2^{-1}U_1^{-1}$. If quantum gates are self-inverse then $U_2^{-1}U_1^{-1} = U_2U_1$. This substitution is called forward matching. This type of substitution by template matching reduces the circuit cost provided the number of gates present in the sequence of gates to be replaced is more than half of the template size. Similarly, when a sequence of gates $U_4U_3U_2U_1$ is substituted by U_5U_6 then the template matching is referred to as backward matching.

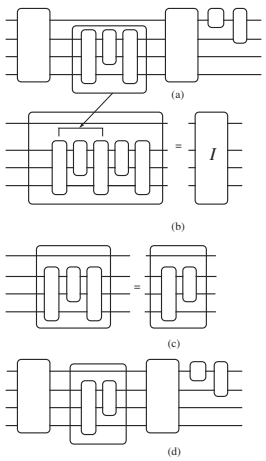


Figure 4.10: Application of template matching tool: (a) An arbitrary quantum circuit, (b) a template, (c) matched sequence that will be substituted by smaller sequence, (d) optimized circuit.

4.5.3 Let us visualize the quantum gate

Time dependent Schrodinger equation is written as

$$H\psi = i\hbar\frac{d\psi}{dt}.$$

For convenience, if we consider $\hbar = 1$ then we can write the time evolution of wave function ψ as

$$\psi(t) = e^{-iHt}\psi(0).$$

If we wish to visualize it as a gate then we have to visualize $\psi(0)$ as an input state and $\psi(t)$ as an output state. In that case we have $\psi_{\text{out}} = U\psi_{\text{in}}$ where $U = e^{-iHt}$ is an operator which may be visualized as a quantum gate or a quantum circuit that maps the input states $\psi_{\text{in}} = \psi(0)$ into the output state $\psi_{\text{out}} = \psi(t)$. Now to achieve a complete circuit we may need to use the output of one operation as the input of the next operation.

4.6 Discussion

In this chapter we have learned about quantum circuits and quantitative measures of their quality. In the next chapter, we will learn about quantum algorithms and will show that quantum circuits play a crucial role in the realization of quantum algorithms. Before we discuss quantum algorithms

it would be appropriate to note that the quantum gates described in the present chapter are experimentally realizable and physical realization of quantum gates and circuits are reported by several groups using different implementations of qubits. For example, in 2003 J. L. O'Brien *et al.* [67] provided a completely optical implementation of a CNOT gate. A CNOT gate is also demonstrated using quantum dot, NMR, ion trap, superconductivity, Rydberg blockade interactions between neutral atoms held in optical traps, etc. (see [68] and references therein). Even larger quantum gates (three qubit gates) are experimentally realized in many different ways. For example, experimental realization of a Toffoli gate is reported using ion trap [69] and superconducting circuits [70]. Further, an optical Fredkin gate [71] is also reported. The point we are trying to make is that at the moment there are several implementations of qubit and each of them may be used to build quantum gates. For example, we may make quantum gates using NMR, optical, ion trap, superconductive techniques. More or less all of the popular quantum gates are successfully constructed using each of these techniques. So in principle, we can construct any quantum circuit and demonstrate quantum algorithms and implement quantum teleportation protocol. However, several problems arise when we try to build a large quantum circuit (quantum computer). The problems associated with the implementation of large quantum circuits and the possible ways to circumvent them are discussed in Chapter 6. Before we describe that, it is tempting to see how the quantum gates introduced in this chapter can be used to implement quantum algorithms. In the next chapter we will discuss quantum algorithms.

4.7 Solved examples

1. Suppose a two-qubit system is in the state $|\psi\rangle = 0.8|00\rangle + 0.6|11\rangle$. A NOT gate is applied to the second qubit and a two qubit measurement is performed in the computational basis. What are the probabilities of the possible measurement outcomes?
   Solution: After application of the NOT gate on the second qubit the state becomes $|\psi\rangle_1 = 0.8|01\rangle + 0.6|10\rangle$. Thus the probability of obtaining $|01\rangle$ as outcome is $(0.8)^2 = 0.64$ and the probability of obtaining $|10\rangle$ is $(0.6)^2 = 0.36$.

2. Show that $P(\pi) = Z$.
   Solution: $P(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z.$

3. Write down the truth table and matrix for Fredkin (CSWAP) gate.
   Solution: Fredkin is Controlled-SWAP gate. If we consider the first bit as the control bit and the last two bits as target bits then the last two bits swap only when the first one is 1. Thus the truth table of

Input state	Output state
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|110\rangle$
$\|110\rangle$	$\|101\rangle$
$\|111\rangle$	$\|111\rangle$

Table 4.2: Truth table of Fredkin gate.

Fredkin is as shown in Table 4.2.

The matrix representation of the gate is already given in the text (see Eqn. (4.23)).

4. Show that it is impossible to define a classical $\sqrt{\text{NOT}}_{\text{cl}}$ gate using binary logic.
Solution: As two consecutive operations of $\sqrt{\text{NOT}}_{\text{cl}}$ should be equivalent to a classical NOT gate so we must have $\sqrt{\text{NOT}}_{\text{cl}}\sqrt{\text{NOT}}_{\text{cl}}|0\rangle = |1\rangle$ and $\sqrt{\text{NOT}}_{\text{cl}}\sqrt{\text{NOT}}_{\text{cl}}|1\rangle = |0\rangle$. Now we ask: What is the output of $\sqrt{\text{NOT}}_{\text{cl}}|0\rangle$? In binary logic there are only two possibilities, $\sqrt{\text{NOT}}_{\text{cl}}|0\rangle = |1\rangle$ and $\sqrt{\text{NOT}}_{\text{cl}}|0\rangle = |0\rangle$. We can analyze these two possibilities separately. (i) If $\sqrt{\text{NOT}}_{\text{cl}}|0\rangle = |1\rangle$ and $\sqrt{\text{NOT}}_{\text{cl}}\sqrt{\text{NOT}}_{\text{cl}}|0\rangle = |1\rangle$ then we must have $\sqrt{\text{NOT}}_{\text{cl}}|1\rangle = |1\rangle$ and consequently we will get $\sqrt{\text{NOT}}_{\text{cl}}\sqrt{\text{NOT}}_{\text{cl}}|1\rangle = |1\rangle \neq |0\rangle$. It cannot implement $\sqrt{\text{NOT}}_{\text{cl}}$ as two consecutive applications of it cannot invert $|1\rangle$. (ii) Now look at the second possibility, i.e., if $\sqrt{\text{NOT}}_{\text{cl}}|0\rangle = |0\rangle$ then $\sqrt{\text{NOT}}_{\text{cl}}\sqrt{\text{NOT}}_{\text{cl}}|0\rangle = |0\rangle \neq 1$. So two consecutive application of $\sqrt{\text{NOT}}_{\text{cl}}$ cannot invert $|0\rangle$. Since there were only two possibilities, we conclude that it is impossible to define a classical $\sqrt{\text{NOT}}_{\text{cl}}$ gate using binary logic.

5. In some books [1] $\sqrt{\text{NOT}}$ gate is given as

$$\sqrt{\text{NOT}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \tag{4.24}$$

In other books [63] it is given as

$$\sqrt{\text{NOT}} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} = \frac{\exp\left(i\frac{\pi}{4}\right)}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}. \tag{4.25}$$

What is the difference between the two? Which one is a better representation in your opinion?

Solution: Differences are here: (i) $\sqrt{\text{NOT}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ maps

$|0\rangle$ and $|1\rangle$ as follows: $\sqrt{\text{NOT}}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) = |+\rangle$ and $\sqrt{\text{NOT}}|1\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = |-\rangle$ whereas $\sqrt{\text{NOT}} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$ maps $|0\rangle$ and $|1\rangle$ as follows: $\sqrt{\text{NOT}}|0\rangle = \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle + i|-\rangle)$ and $\sqrt{\text{NOT}}|1\rangle = \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - i|-\rangle)$. (ii) When $\sqrt{\text{NOT}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ then $\sqrt{\text{NOT}}\sqrt{\text{NOT}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ which is equivalent to NOT as far as its action on $|0\rangle$ and $|1\rangle$ are concerned but when it works on $|+\rangle$ then we obtain $\sqrt{\text{NOT}}\sqrt{\text{NOT}}|+\rangle = -|-\rangle \equiv |-\rangle$ but ideally $\text{NOT}|+\rangle = |+\rangle$. Thus $\sqrt{\text{NOT}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ does not really work as square root of NOT for superposition states. Now for $\sqrt{\text{NOT}} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$ we obtain $\sqrt{\text{NOT}}\sqrt{\text{NOT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X$ which is exactly the matrix of NOT gate, hence its name is even justified for superposition states. Therefore, in our opinion $\sqrt{\text{NOT}} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$ is a better representation.

6. Prove that matrix representation of $\sqrt{\text{NOT}}$ in (4.25) is unitary.
Solution: It is easy to check that

$$\sqrt{\text{NOT}}\sqrt{\text{NOT}}^{\dagger} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}\begin{pmatrix} \frac{1-i}{2} & \frac{1+i}{2} \\ \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I,$$

and

$$\sqrt{\text{NOT}}^{\dagger}\sqrt{\text{NOT}} = \begin{pmatrix} \frac{1-i}{2} & \frac{1+i}{2} \\ \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix}\begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Therefore, $\sqrt{\text{NOT}}$ described in (4.25) is unitary.

7. Is $\sqrt{\text{NOT}}$ described in (4.25) Hermitian operator? Is it a normal operator?
Solution: No it is not Hermitian as $\sqrt{\text{NOT}} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \neq \begin{pmatrix} \frac{1-i}{2} & \frac{1+i}{2} \\ \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix} = \left(\sqrt{\text{NOT}}\right)^{\dagger}$. However, it is a normal operator. In the previous problem we have already shown that it is unitary and all unitary operators are normal.

8. Construct a quantum circuit using only Hadamard gates to create the state

$$|\psi\rangle = \frac{(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)}{\sqrt{8}},$$

from three qubits, which are initially in the state $|000\rangle$.
Solution: Just apply three Hadamard gates in parallel on the three input qubits.

9. Show that applying Hadamard transformations individually to N qubits each in the state $|0\rangle$ puts them into an equal superposition of the 2^N possible logical states.
Solution:

$$\begin{aligned} & H^{\otimes N}|0\rangle^{\otimes N} \\ = \; & H|0_1\rangle H|0_2\rangle \cdots H|0_N\rangle \\ = \; & \tfrac{1}{\sqrt{2}}\left(|0_1\rangle + |1_1\rangle\right) \tfrac{1}{\sqrt{2}}\left(|0_2\rangle + |1_2\rangle\right) \cdots \left(|0_N\rangle + |1_N\rangle\right) \\ = \; & \tfrac{1}{\sqrt{2^N}}\left(|0_1 0_2 \cdots 0_N\rangle + |0_1 0_2 \cdots 1_N\rangle + \cdots + |1_1 1_2 \cdots 1_N\rangle\right), \end{aligned}$$

where subscripts are used to denote the qubit number. It clearly shows that $H^{\otimes N}|0\rangle^{\otimes N}$ creates an equal superposition of 2^N possible logical states.

10. Show that $HXH = Z$ and $HZH = X$.
Solution:

$$\begin{aligned} HXH &= \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \tfrac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z. \end{aligned}$$

Now we can prove the second identity either by using the same method or by using the first identity and the fact that $H^2 = I$ as $HZH = H(HXH)H = H^2XH^2 = IXI = X$.

11. Write down the truth table corresponding to the following gate:

$$\begin{aligned} G &= \tfrac{1}{\sqrt{2}}\left((|00\rangle + |01\rangle)\langle 00| + (|01\rangle - |11\rangle)\langle 01|\right. \\ &+ \left.(|11\rangle - |00\rangle)\langle 10| + (|11\rangle + |10\rangle)\langle 11|\right) \end{aligned}$$

and also provide the matrix that represents this gate. How will you check whether G is a valid quantum gate or not?
Solution: The truth table is shown in Table 4.3 and we can obtain the matrix by replacing $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ by their equivalent column matrices and the corresponding bras by row matrices. Then the simple matrix multiplication and addition will yield the equivalent matrix as

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

Input state	Output state
$\|00\rangle$	$\frac{\|00\rangle+\|01\rangle}{\sqrt{2}}$
$\|01\rangle$	$\frac{\|01\rangle-\|11\rangle}{\sqrt{2}}$
$\|10\rangle$	$\frac{\|11\rangle-\|00\rangle}{\sqrt{2}}$
$\|11\rangle$	$\frac{\|11\rangle+\|10\rangle}{\sqrt{2}}$

Table 4.3: Truth table of the gate G given in the Solved Example 11.

Now one can easily check that it is not a valid quantum operation as it is not a unitary operator. The same is shown below.

$$\begin{aligned} UU^\dagger &= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 1 & 0 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{3}{2} \end{pmatrix} \neq I. \end{aligned}$$

12. Verify whether the following representation of a CNOT gate is correct or not: $U_{\text{CNOT}} = |0\rangle|0\rangle\langle 0|\langle 0| + |0\rangle|1\rangle\langle 0|\langle 1| + |1\rangle|1\rangle\langle 1|\langle 0| + |1\rangle|0\rangle\langle 1|\langle 1|$.
Solution: This is clearly the representation of a CNOT gate as the operation

$$\begin{aligned} U_{\text{CNOT}} &= |0\rangle|0\rangle\langle 0|\langle 0| + |0\rangle|1\rangle\langle 0|\langle 1| + |1\rangle|1\rangle\langle 1|\langle 0| + |1\rangle|0\rangle\langle 1|\langle 1| \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \end{aligned}$$

maps $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$ to $|00\rangle, |01\rangle, |11\rangle$ and $|10\rangle$ respectively.

13. Find the matrix representation of a NOT gate in the Hadamard basis.
Solution: A NOT gate in Hadamard basis $\{|+\rangle, |-\rangle\}$ implies that it transforms $|+\rangle$ to $|-\rangle$ and $|-\rangle$ to $|+\rangle$. Thus the NOT gate is

$$\begin{aligned} \text{NOT} &= |+\rangle\langle -| + |-\rangle\langle +| \\ &= \tfrac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \end{pmatrix} + \tfrac{1}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

14. Prove that $R_x(\pi)R_y(\frac{\pi}{2}) = H$ up to a global phase factor.

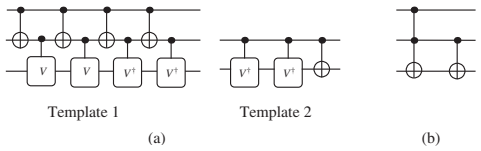


Figure 4.11: (a) Two quantum templates, (b) a quantum circuit to be simplified using the templates shown in (a). For detail see Solved Example 16.

Solution:

$$\begin{aligned} & R_x(\pi)R_y(\tfrac{\pi}{2}) \\ = & \begin{pmatrix} \cos(\frac{\pi}{2}) & -i\sin(\frac{\pi}{2}) \\ -i\sin(\frac{\pi}{2}) & \cos(\frac{\pi}{2}) \end{pmatrix} \begin{pmatrix} \cos(\frac{\pi}{4}) & -\sin(\frac{\pi}{4}) \\ \sin(\frac{\pi}{4}) & \cos(\frac{\pi}{4}) \end{pmatrix} \\ = & \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \\ = -i & \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ = & H. \end{aligned}$$

In the last step we ignored a common phase factor $-i = \mathrm{e}^{i\frac{3\pi}{2}}$.

15. Prove that $XR_Y(\theta)X = R_Y(-\theta)$.
Solution: First we note that

$$XYX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = -Y.$$

Now we know that $R_y(\theta) = I\cos(\frac{\theta}{2}) - iY\sin(\frac{\theta}{2})$. Therefore,

$$\begin{aligned} XR_y(\theta)X &= XIX\cos(\tfrac{\theta}{2}) - iXYX\sin(\tfrac{\theta}{2}) \\ &= I\cos(\tfrac{\theta}{2}) - i(-Y)\sin(\tfrac{\theta}{2}) \\ &= I\cos(-\tfrac{\theta}{2}) - iY\sin(-\tfrac{\theta}{2}) \\ &= R_y(-\theta). \end{aligned}$$

16. Two templates are given in Fig. 4.11a. First convert the NCT circuit shown in Fig. 4.11b to an equivalent NCV circuit and then use the given templates to optimize the NCV circuit. What are the circuit costs of the circuit shown in Fig. 4.11b in an NCT gate library and in an NCV gate library? Also find (a) linear and nonlinear quantum cost (b) depth in an NCT library and in an NCV library and (c) width of the circuit.
Solution: The given circuit is shown in Fig. 4.12a. The circuit can be transformed into an NCV circuit by substituting the Toffoli gate

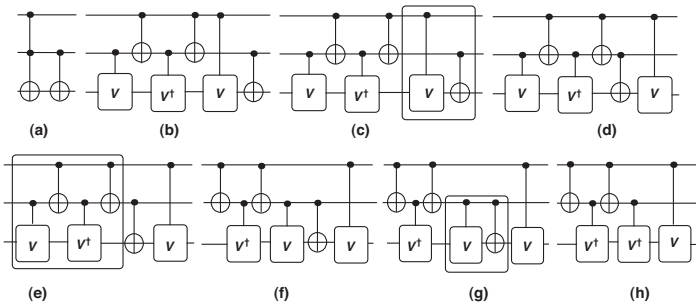


Figure 4.12: Solution of Solved Example 16.

by quantum primitives. The NCV circuit obtained in this way is shown in Fig 4.12b. Commutation rule is applied on the gates shown in a rectangular box in Fig 4.12c and it results in Fig 4.12d. Template 1 from Fig 4.11a is then applied in the rectangular box in Fig 4.12e and it results in Fig. 4.12f. Similarly Template 2 is applied in the rectangular box in Fig 4.12g and it results in Fig 4.12h. The circuit in Fig. 4.12h is the simplified NCV circuit.
Now Fig. 4.12a is the given NCT circuit with two gates, which cannot be further reduced using an NCT library so its circuit cost is 2, width is 3 as there are 3 qubits and depth is 2. Now the linear quantum cost of the circuit is the sum of quantum cost of Toffoli and CNOT, i.e., 5+1=6. To obtain the nonlinear quantum cost we have optimized the equivalent NCV circuit and obtain Fig. 4.12h, from which we can see that the nonlinear quantum cost is 5. Further, from the optimized NCV circuit shown in Fig. 4.12h we find that the depth of the circuit is 5, gate count is 5 and width is 3.
This example clarifies many ideas, for example, values of cost metrics depend on the choice of gate library, linear quantum cost is different from nonlinear quantum cost, NCT circuits need to be transformed to NCV circuits for computation of quantum cost, a template may not reduce the gate count directly as in Fig. 4.12e→Fig. 4.12f, the template matching does not reduce the gate count directly, but it helped us to reduce gate count by using the second template in Fig. 4.12g etc.

17. Obtain nonlinear quantum cost of the circuit of function 3_17 shown in Fig. 4.13. Necessary optimization of the circuit may be done using the commutation rule and matching rule (forward and backward).
Solution: The given circuit (Fig. 4.13 also shown in Fig. 4.14a) is an NCT circuit. To obtain the quantum cost we need to optimize the

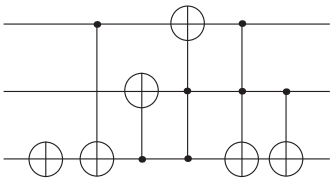


Figure 4.13: Reversible circuit for function 3_17 given in the benchmark page of D. Maslov *et al.* [72]. In Solved Example 17 our task is to find the quantum cost of this circuit.

equivalent NCV circuit. We can either substitute the Toffoli gates present in Fig. 4.14a by the equivalent NCV circuit and then optimize the NCV circuit as we have done in the previous example or we may first try to optimize the given NCT circuit and then replace the Toffoli gate present in the optimized NCT circuit by the equivalent NCV circuit and further optimize the obtained NCV circuit to obtain the quantum cost. Here we have followed the second approach. The given NCT circuit is shown in Fig. 4.14a. In Fig. 4.14b, commutation rule is applied and the arrow shows the movement of the CNOT gate. In Fig. 4.14c we show the NCT circuit obtained after commutation is applied, i.e., before substitution of quantum primitive gates (note that applied commutation rule has not reduced the gate count but will be found useful later when 2 two qubit gates will appear consecutively on the same qubit lines) and in Fig. 4.14d the quantum circuit is obtained by substituting the Toffoli gates with primitives. In Fig. 4.14e, a template matching tool is applied to the circuit (at positions indicated by underbars) to yield Fig. 4.14f where a quantum circuit with reduced gate count is obtained. In Fig. 4.14g, moving rule is applied and two movements have been done in the circuit as indicated by the arrows. As a result of application of moving rule we obtain Fig. 4.14h, where new gates are introduced (each dashed box is a new gate) to obtain a nonlinear quantum cost. Finally the quantum cost of the given circuit is found to be 7.

18. Find the quantum cost of EPR circuit and Toffoli gate.
Solution: Quantum cost of EPR circuit is 1 as the single qubit Hadamard gate can be combined with the CNOT gate. Similarly, quantum cost of Toffoli is 5. See Fig. 4.15, which shows standard implementation of Toffoli using 7 primitive quantum gates. The Hadamard gates present at the beginning and at the end can be combined with the $C-V$ gates and that reduces the quantum cost to 5.

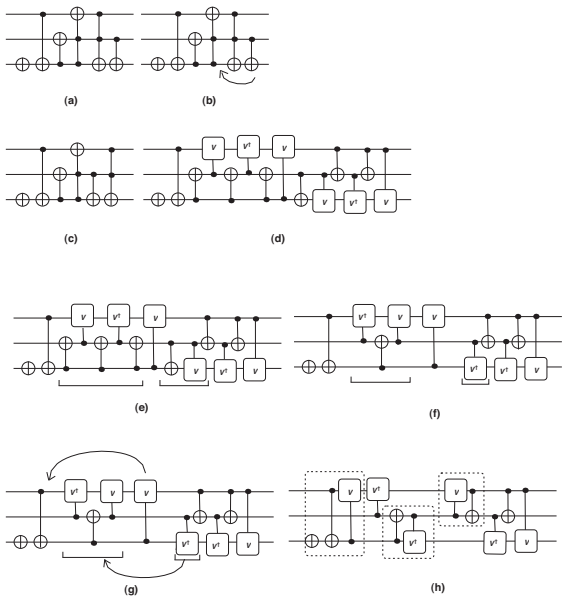


Figure 4.14: Solution of Solved Example 17. (b)-(h) show optimization of (a). From (h) we can observe that the quantum cost of the given circuit is 7.

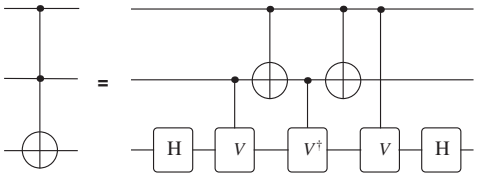


Figure 4.15: Quantum cost of Toffoli gate is 5 as the single qubit gates can be absorbed. For details see Solved Example 18.

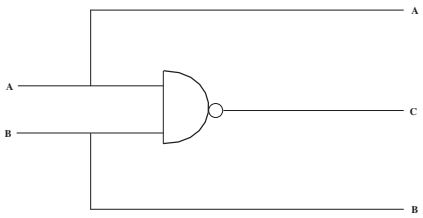


Figure 4.16: Reversible NAND gate constructed using fan-out operations increases number of qubit lines (width). For details see Solved Example 19.

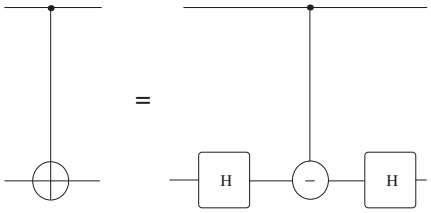


Figure 4.17: A circuit identity. For details see Solved Examples 20 and 21.

19. Can you convert an irreversible NAND gate into a reversible one just by using fan-out operations? If yes, then why don't we use this trick to convert all the existing irreversible circuits into their reversible counterparts, which will be more energy efficient?
Solution: Yes, we can do that by making copy of each input state (using fan-out operations) as shown in Fig. 4.16. However, this process will considerably increase the width (number of qubit lines) of the circuit, which is not desirable.

20. CMINUS gate is defined as $C-Z$ gate. Now provide its matrix and prove the circuit identity shown in Fig. 4.17.
Solution: In matrix form CMINUS $= C-Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$.

Now in the given circuit identity

$$\begin{aligned}
\text{RHS} &= (I_2 \otimes H)\,\text{CMINUS}\,(I_2 \otimes H) \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \\
&\quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\
&= \tfrac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \\
&\quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \\
&= \tfrac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\
&= \text{CNOT} = \text{LHS}.
\end{aligned}$$

21. Show that the CNOT gate can be constructed from Hadamard gates and the controlled$-Z$ gate. Demonstrate that the construction is correct by multiplying the corresponding matrices.
Solution: Same as the previous solved example.

22. Given that if U is an arbitrary single qubit gate (unitary operation) then

$$\text{Controlled}{-}U = \begin{pmatrix} I & O \\ O & U \end{pmatrix},$$

where I, O are respectively the Identity and Null operations (gate) in C^2. Use this general form of controlled gate to explicitly provide the matrix of CNOT and $C-Y$ gates.
Solution: Here I, O and U can be represented by 2×2 matrices. For example, in the first case U is a NOT operation then $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and just by replacing these three

matrices in the given expression we obtain

$$\text{Controlled}-U = \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Similarly, in the second case $U = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. Therefore,

$$\text{Controlled}-Y = C - Y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix}.$$

4.8 Further reading

1. D. P. DiVincenzo, Quantum gates and circuits, Proc. R. Soc. Lond. A, **454** (1998) 261-276, quant-ph/9705009v1.

2. J. L. O'Brien, Optical quantum computing, Science, **318** (2007) 318 1567-1570, quant-ph/0803.1554v1. It is an excellent short review which discusses how one can do all optical quantum computing using only single photon sources, linear optical elements, and single photon detectors.

3. G. F. Viamontes, I. L. Markov and J. P. Hayes, Quantum circuit simulation, Springer, Dordrecht, Netherlands (2009).

4. QuaSi: This is an excellent simulator of quantum circuits in Java. Users can either design and simulate their own circuit or use the existing circuits for Shor's algorithm, Grover's algorithm, etc. This has an applet version which you can run online and a full downloadable version. Documentation is available in English. This can even factorize powers of primes ($25 = 5 \times 5$ or $343 = 7 \times 7 \times 7$) using Shor's algorithm. This particular feature is absent in Open Qubit. This is designed by IAKS, University of Karlsruhe. It's available for free but it needs Java 1.1 or higher version to be installed in your system. All the required links are available at
http://iaks-www.ira.uka.de/home/matteck/QuaSi/aboutquasi.html.

4.9 Exercises

1. Construct AND, NOT, OR, NAND and NOR gates using circuits with just Fredkin gates. Can we consider Fredkin gate as a universal gate?

2. Provide the matrix form of the controlled$-H$ gate, where H is the Hadamard gate.
3. Prove the following useful circuit identity: $HYH = -Y$.
4. Show that up to a global phase $R_z(\theta) = P(\theta)$ and use that to show $R_z\left(\frac{\pi}{4}\right) = T$ up to a global phase.
5. What does a CCFredkin gate do?
6. Provide the matrix representation of CCZ and $CCP\left(\frac{\pi}{6}\right)$.
7. Express Deutsch, Fredkin and Toffoli gates in bra-ket notation.
8. The Hadamard, phase (S), CNOT, and $\frac{\pi}{8}$ gates form a universal gate set. However, one of these gates is unnecessary. Which one, and why? If it is unnecessary why is that kept in the set?
9. Check which of these gates are linear: (a) Hadamard (b) SWAP (c) NOR.
10. Show that AND is a nonlinear gate.
11. Justify following statements: (a) Circuit cost$\leq$ quantum cost, (b) Delay$\geq$ depth, (c) $\{\text{all quantum gates}\} \supset \{\text{all reversible gates}\}$, (d) Hadamard gate cannot be achieved classically.
12. Prove that $XR_Z(\theta)X = R_Z(-\theta)$.
13. Prove that all reversible gates with 2 inputs and 2 outputs are linear.
14. Prove the following circuit identities: (i) NOT $\equiv R_x(\pi)\, Ph\left(\frac{\pi}{2}\right)$, (ii) $\sqrt{\text{NOT}} \equiv R_x\left(\frac{\pi}{2}\right) Ph\left(\frac{\pi}{4}\right)$, (iii) $H \equiv R_x(\pi)\, R_y\left(\frac{\pi}{2}\right) Ph\left(\frac{\pi}{2}\right)$, where $Ph(\theta) = \exp(i\theta)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is equivalent to a global phase.
15. A black box contains a classical gate which accepts n bits as inputs and produces a single bit as its output. Show that 2^n such Boolean gates are possible.
16. In binary logic how many 2-bit irreversible gates are possible? Show that the number is less than the number of possible 2-bit classical reversible gates.
17. Show that in the Bloch sphere, $R_x(\theta)$ and $R_y(\theta)$ can be visualized as rotations through an angle θ about the X axis and Y axis respectively.
18. Express the CNOT gate in the Dirac notation when the second qubit is the control qubit and the first qubit is the target qubit. Also provide its matrix form.

19. Use the circuit identity given in Fig. 4.17 to construct a template.

20. Verify that $\sqrt{\text{SWAP}} = \frac{1}{1+i}\begin{pmatrix} 1+i & 0 & 0 & 0 \\ 0 & 1 & i & 0 \\ 0 & i & 1 & 0 \\ 0 & 0 & 0 & 1+i \end{pmatrix}$. Also check that $\sqrt{\text{SWAP}}$ is a valid quantum gate.

CHAPTER

4

OTHER ADVANCED TOPICS

This chapter is excerpted from

Quantum Mechanics II

by S. Rajasekar, R. Velusamy

Learn more

CHAPTER 9

Some Other Advanced Topics

9.1 INTRODUCTION

In the earlier chapters we presented basic features of certain advanced topics including supersymmetric quantum mechanics, coherent and squeezed states, quantum computers and quantum cryptography. There are several other topics which also received considerable interest and have a wide range of applications. In the present chapter we consider some of them. Particularly, we give a very brief introduction to the following fascinating topics:

1. Quantum gravity
2. Quantum Zeno effect
3. Quantum teleportation
4. Quantum games
5. Quantum cloning
6. Quantum diffusion
7. Quantum chaos.

There are several other interesting and important topics like quantum Hall effect, quantum dots, quantum tomography, quantum decoherence, quantum brain dynamics, etc. These are not covered in this book.

9.2 QUANTUM THEORY OF GRAVITY

Quantum physics deals with the behavior of microscopic objects whereas the general relativity deals with much larger bodies. Both theories have limitations in their abilities to describe the universe. At present we do not have a

full theory because such a theory must be based on a single framework but such a theory is lacking. In the present forms quantum theory and relativity cannot make predictions about certain kinds of physical phenomena. These phenomena are found to occur at extremely small distances of the order of Planck length or at very high energies − some 20 orders of magnitude far from the scales of particle accelerators. Planck units are measurement units defined in terms of five universal constants namely, the gravitational constant ($G = 6.673 \times 10^{-11}\text{m}^3\text{kg}^{-1}\text{s}^{-2}$), reduced Planck constant ($\hbar = 1.055 \times 10^{-34}\text{Js}$), speed of light ($c = 10^8\text{m/s}$), Coulomb constant ($1/(4\pi\epsilon_0) = 9 \times 10^9\text{Nm}^2\text{C}^{-2}$) and Boltzmann's constant ($k_\text{B} = 1.4 \times 10^{-23}\text{JK}^{-1}$). In these units, Planck length $\sqrt{\hbar G/c^3} = 1.616 \times 10^{-35}\text{m}$, Planck mass $\sqrt{\hbar c/G} = 1.2209 \times 10^{19}\text{GeV}/c^2 = 2.17644 \times 10^{-8}\text{Kg}$, Planck time $\sqrt{\hbar G/c^5} = 5.39124 \times 10^{-44}\text{s}$, Planck charge $\sqrt{4\pi\epsilon_0\hbar c} = 1.8755 \times 10^{-18}\text{C}$, Planck energy $\sqrt{c^5\hbar/G} \sim 10^{19}\text{GeV}$ and Planck temperature $\sqrt{\hbar c^5/(Gk_\text{B}^2)} = 1.416785 \times 10^{32}\text{K}$. A theory of quantum gravity is essential to describe the situations at these Planck's scales. For example, understanding the universe where it was at a time less than one Planck time ($\sim 10^{-44}\text{s}$) old needs a theory of quantum gravity. At the Planck temperature ($\sim 10^{32}\text{K}$) all the forces of nature may be unified. At energies of the order of Planck energy the gravitational interactions are strong enough and we cannot neglect them. The theory we are looking for must unify Einstein's theory of gravity, relativity and also the quantum theory and hence is called a *quantum theory of gravity*.

Because the problems in quantum gravity are so big and very fundamental, there is generally more than one place to begin. Some of the starting points are the following:

1. Modification of quantum theory by taking account of the gravitational force.

2. Modification of quantum theory by incorporating the principles of relativity.

3. Stating the general relativity in quantum mechanical description.

There are groups of people focusing with different starting points. We now have various approaches to quantum gravity, with different names such as string theory, loop quantum gravity, twistor theory, random geometry, toposes and so on. In this section we present some basic ideas and the features of quantum gravity.

9.2.1 Three Approaches of Quantum Gravity [1]

In the following we give a compact summary of fundamental ideas of the approaches of semiclassical gravity, loop quantum gravity and string theory.

1. Semiclassical Gravity

The coupling of quantum theory and classical gravity, called *semiclassical gravity*,was proposed by Jesper Moller Grimstrupb and Leon Rosenfeld in which the Einstein field equations are written as

$$G_{\mu\nu} = 8\pi G \langle\psi|T_{\mu\nu}|\psi\rangle \ . \tag{9.1}$$

Here $T_{\mu\nu}$ is an operator. The energy-valued tensor of matter $T_{\mu\nu}$ is replaced by an expectation value. This model gives rise to a nonlinear Schrödinger equation. So, the principle of superposition here fails and further it violates the basics of quantum mechanics. Therefore, to couple a quantum system to classical gravity, we need to modify either the general relativity or quantum mechanics.

In the semiclassical approach, matter is dealt with quantum mechanically and space-time is treated as per the general theory of relativity. Certain intriguing predictions are made by this approach. For example, a particle detector accelerated, say, with the acceleration g in a vacuum will behave as if it was kept in a thermal bath at temperature $hg/(2\pi c)$. According to this, a black hole appears as a hot thermodynamic system with a temperature inversely proportional to its mass and entropy.

2. Loop Quantum Gravity

In this theory, the effects of quantum gravity are not treated as excitations of a classical geometry. It predicts that measures like areas and volumes are discrete. These quantities are represented by operators and possess discrete spectra. This theory succeeds in problems where string theory fails and vice-versa. In this sense, the loop quantum gravity is thought of as a complementary to string theory.

3. String Theory

String theory is formulated as a theory of everything with gravity and the other fundamental interactions. In this theory, gravitons are regarded as particles travelling in a fixed non-dynamical space-time. These particles scatter and interact weakly with each other. Further, they are the excitations of one-dimensional curves known as *strings* instead of point-like objects. All the other particles and forces in nature are thought of as arising from the excitations of the strings. Thus, particles such as electrons, quarks, photons correspond to modes of vibration of the string. The strings possess a characteristic length scale. Experiments at energies below the Planck energy cannot resolve distances which are as small as Planck length. Thus, at such energies, strings can be approximated by point-like particles.

Five consistent string theories are known. Four of them have only closed strings forming closed loops. Of these four, two are based on unoriented strings: One has an open string and the other a closed string. Two other theories are formulated with oriented closed strings differing in internal symmetry. One of these is called *type-II string theory* and other as *heterotic string theory*.

It is indeed remarkable that the spectra of the classical solutions of all the string theories have exactly one massless spin graviton. In physical theories, the number of dimensions is generally a free parameter and usually fixed to three. But string theory predicts 9 spatial dimensions. This is the only theory known so far that unifies the quantum theory and general relativity. It was realized that every string theory describes a limit of an underlying general theory called *M-theory* defined in 11 dimensions of space.

9.2.2 Pictures of the Physical World [1]

Combining the predictions of different approaches of quantum gravity we will be able to describe the physical world. This picture may not be correct, but provides a certain kind of complete picture that experimentalists may realize if they probe the Planck scale. Some of the main features are the following:

1. Space, time and all physical quantities are regarded as relations between things in the world. The theory knows nothing of points in space or events in time. It knows only details of relations between things that occur.

2. The fundamental of the world is essentially information instead of fields.

3. Quantities such as area, volume and electric charge are discrete.

4. The basic excitations are not thought of as point-like but are one or more dimensional.

5. Observable quantities are only connected with information flowing across the boundaries between the observer and the system. The theory does not predict the events happening in space-time but provides information reached by an observer.

6. There is a restriction on the quantum of information flowing across any surface in space. There will not be more bits of information than the surface area, measured in units of the Planck area - $G\hbar/c^3 \approx 10^{-70}\mathrm{m}^2$. In other words, only one bit of information can flow across every $10^{-70}\mathrm{m}^2$.

7. The value of electric charge, masses of particles, etc. may vary with time.

8. Distinctions between different particles and forces are because of symmetry breaking.

9.2.3 Implications of Quantum Gravity

There are many different approaches for quantizing gravity. A fully acceptable theory is yet to emerge. However, many implications of quantum gravity found to exist for a range of phenomena in our every day physics. Some of them are listed below [2]:

TABLE 9.1 Upper limits of certain physical quantities estimated by the theory of quantum gravity.

Physical quantities	Upper limit
Cosmic ray particle energies	10^{28}eV
Elastic modulus	10^{112}dyne/cm
Density	$c^5/(G^2\hbar)$
Electric/magnetic fields strength	$c^{7/2}/(G\sqrt{\hbar}\,)$
Temperature	$\sqrt{\hbar c^5/G}\,/k_{\rm B} \sim 10^{32}$degree
Surface tension	10^{80}dyne/cm^2

1. It has been estimated that in sun, 10^9W of thermal gravitational radiation could be generated because of Coulomb collisions in the plasma core. The number of gravitons, $N_{\rm g}$, emitted in an explosion of energy E is worked out as
$$N_{\rm g} = \frac{GE^2}{\hbar c^5}\ . \tag{9.2}$$
For a 100 megaton nuclear explosion, the above predicts a dimensionless strain of 10^{-31}.

2. The life-time of a 3d-1s transition in hydrogen with the emission of graviton is
$$\frac{Gm_{\rm e}^2\omega_{\rm hyd}\alpha^4}{\hbar c} \sim 10^{35}{\rm s}\ , \tag{9.3}$$
where $m_{\rm e}$ is the mass of the electron, $\omega_{\rm hyd}$ is the frequency of the 3d-1s transition and α is the fine structure constant.

3. For a gravitating body with mass m, the minimum radius into which it may collapse in a comoving frame is
$$R_{\rm min} = \left(\frac{G^3\hbar m^2}{c^7}\right)^{1/4}\ . \tag{9.4}$$

4. Table 9.1 gives upper limits of certain physical quantities.

5. A possible smallest time interval is $\sqrt{\hbar G/c^5} \sim 10^{-43}$s.

6. The highest power which can be generated or emitted by a physical system is
$$P_{\rm max} \sim \frac{c^5}{G} \sim 3\times 10^{59}{\rm ergs}. \tag{9.5}$$
This means a universal bound on the rate of information processing is
$$f = \sqrt{P_{\rm max}/\hbar} \sim 10^{44}{\rm bits/s}. \tag{9.6}$$

7. It is possible to have photons with energies $\sim 10^{20}$eV or larger.

8. Photons with a few TeV energy will be able to travel freely through the background of microwave or infrared photons.

9. String theory implies a modification of the Heisenberg's uncertainty principle. The uncertainties in the position and momentum of a string are
$$\Delta x \approx \sqrt{\hbar/T} \text{ and } \Delta p_x \approx \sqrt{\hbar T}\,, \tag{9.7}$$
where T is the string tension.

10. The energy eigenvalues of a hydrogen atom are
$$E_n = B\left[-\frac{1}{n^2} + 4\left(\frac{l_{\rm s}}{a_0}\right)^2\right]\frac{\left(4n - 3\left(l+\frac{1}{2}\right)\right)}{n^4\left(l+\frac{1}{2}\right)}\,, \tag{9.8}$$
where $l_{\rm s}$ is the minimal length scale and a_0 is Bohr radius.

So far there is no experimental evidence for quantized gravity. If the gravitational field is not quantized then violation of the uncertainty principle will result [3].

9.2.4 Tests Proposed to Detect Quantum Gravity

The characteristic energy scale for quantum gravity is the Planck energy $\sim 10^{19}$GeV. This is so far out of the range of experiment. Hence direct tests appear impossible. However, certain tests have been proposed.

1. Quantum gravity may lead to violation of the equivalence principle. This may be detectable in precision tests in atomic and neutron interferometry.

2. It may lead to violations of CPT invariance, for example, with the formation of virtual black holes. Present experimental techniques are greatly improving and thus such effects may be observable.

3. Quantum gravity may distort the dispersion relations over long distances for light and neutrinos. This leads to a frequency-dependent speed of light. This effect can be testable with the observations of gamma ray bursts.

4. Quantum fluctuations may be noticeable in the geometry of space with the help of a sensitive interferometer suitable for gravitational wave detection.

5. It has been suggested that the use of lasers to accelerate electrons may open the possibility to indirectly observe Unruh radiation (a black-body radiation observed by an accelerated observer) which is the counterpart of Hawking radiation for the case of an accelerating particle in flat space-time.

6. Another test is from condensed matter analogs of black holes which emit Hawking radiation phonons from sonic horizons, regions where the fluid flow attains the speed of sound.

Though these experiments open the possibility of detecting quantum gravitational effects, at present it is not at all certain that they are feasible. For more discussions on quantum gravity one may refer to refs.[4-8].

9.3 QUANTUM ZENO EFFECT

The effect of a measurement on a quantum state is usually described by the projection postulate of von Neumann and Gerhart Lüders. According to this, depending on the result of a measurement, the wave function of the system is projected onto the eigenspaces of the observable. This is also called *collapse of the wave function* in a measurement. Before a measurement, the wave function is a superposition of all states − an arbitrary quantum state. At the time of measurement it collapses into a particular state. Baidyanaith Misra and Ennackal Chandy George Sudarshan raised the question: *What would happen if we observe the system all the time?* With some reasonable assumptions, they have investigated the influence of rapidly repeating measurements at times Δt apart on a system [9]. They found a slow down of time development of the system in the limit $\Delta t \to 0$, called the *quantum Zeno paradox* as it is reminiscent of Zeno's *arrow paradox*. The quantum Zeno effect refers to a freezing of a quantum state. Even a system with high energy and highly unstable will remain in the same initial state, as long as it is observed, like an unmoved rabbit when a bright light is shined on its eyes.

Zeno of Elea (490 BC–425 BC) was a pre-Socretic Greek philosopher of southern Italy. He formulated many paradoxes to show that *all is one*. His most famous paradoxes are Achilles (the legendary Greek warrior) and the tortoise and the arrow paradox. In a race, the quickest runner cannot overtake the slowest, because the pursuer must first reach the point whence the pursued started (ahead), so that the slower must always have a lead. If a tortoise will be allowed to start from a point ahead of Achilles then the tortoise when running will not be overtaken by Achilles. To overtake the tortoise, Achilles first must reach the point from which the tortoise started. Then by that time the tortoise will have moved a distance. That is, the tortoise must always be some distance ahead of Achilles. The arrow paradox is that if everything when it occupies an equal space is at rest, and if that which is in locomotion is always occupying such a space at any time, the flying arrow is thus motionless. Consider an arrow in motion. Suppose we divide the time into a number of

indivisible instants. Then at any given instant if we see the arrow it has an exact position. It is thus not moving. Therefore, if we continuously observe the arrow then it is at rest all the time.

9.3.1 Theoretical Consideration

Consider a quantum system Q with its states belonging to the Hilbert space $\mathcal{H}$. The evolution of it is described by the unitary operator $U(t) = \mathrm{e}^{-\mathrm{i}Ht/\hbar}$ where H is the Hamiltonian. Let E be a projection operator such that $E\mathcal{H}E = \mathcal{H}_E$ where $\mathcal{H}_E$ is the subspace spanned by its eigenstates. The initial density matrix $\rho(0)$ of Q belongs to $\mathcal{H}_E$. For an undisturbed evolution at time T

$$\rho(T) = U(T)\rho(0)U^\dagger(T) \; . \tag{9.9}$$

The probability $P(T)$ for Q to be in $\mathcal{H}_E$ at T is

$$P(T) = \mathrm{Tr}\left[U(T)\rho(0)U^\dagger(T)E\right] \; . \tag{9.10}$$

$P(T)$ is called *survival probability* and is < 1.

By definition

$$\rho(0) = E\rho(0)E \; , \quad \mathrm{Tr}[\rho(0)E] = 1 \; . \tag{9.11}$$

When a measurement is made at t then $\rho(t)$ becomes

$$\rho(t) = EU(t)\rho(0)U^\dagger(t)E \; . \tag{9.12}$$

Now

$$P(T) = \mathrm{Tr}\left[U(t)\rho(0)U^\dagger(t)E\right] \; . \tag{9.13}$$

Suppose we carry out a series of observations at $t_n = nT/N$, $n = 1, 2, \cdots, N$. After N measurements the state of Q is given by

$$\rho^{(N)}(T) = V_N(T)\rho(0)V_N^\dagger(T) \; , \quad V_N(T) = [EU(T/N)E]^N \tag{9.14}$$

and

$$P^{(N)}(T) = \mathrm{Tr}\left[V_N(T)\rho(0)V_N^\dagger(T)\right] \; . \tag{9.15}$$

Define

$$\nu(T) = \lim_{N\to\infty} V_N(T) \; . \tag{9.16}$$

Then in the limit of $N \to \infty$ (continuous observation)

$$\dot{\rho}_f(T) = \nu(T)\rho(0)\nu^\dagger(T) \tag{9.17}$$

and

$$\begin{aligned} P_f(T) &= \lim_{N\to\infty} P^{(N)}(T) \\ &= \mathrm{Tr}\left[\nu(T)\rho(0)\nu^\dagger(T)\right] \; . \end{aligned} \tag{9.18}$$

Misra and Sudarshan assumed that $\lim_{t\to 0}\nu(t) = E$ and proved that $\nu(T)$ exists for all real T and $\nu^\dagger(T) = \nu(-T)$ so that $\nu^\dagger\nu = E$. Then by Eq. (9.11)

$$\begin{aligned}\rho_f(T) &= \mathrm{Tr}\left[\rho(0)\nu^\dagger\nu\right] \\ &= \mathrm{Tr}\left[\rho(0)E\right] \\ &= 1\,. \end{aligned} \tag{9.19}$$

The significant implication is that if the system is continuously observed then it will never undergo a transition to $\mathcal{H} - \mathcal{H}_E$. In other words, continuous observation of a time-independent projection operator prevents a change of state. Thus, an unstable quantum state that is observed continuously is never found to decay or a *watched pot never boils* [10] or a *watched clock does not move*. This is the *quantum Zeno paradox*. By repeating the same measurement considerably large number of times in a finite time the system can be arrested in its initial state. The paradoxial point[1] is that the system is found to have its decay influenced by the presence of a measuring device. The Zeno paradox differs from the two other famous paradoxes: the Schrödinger cat and the EPR. Those two are paradoxes of interpretation. The Zeno paradox is a prediction and can be tested.

9.3.2 Quantum Zeno Effect in a Neutron Spin System

Consider the evolution of the neutron spin subjected to a magnetic field [11]. The interaction of a neutron with a static field B is given by $H = \mu B\sigma_1$ where μ is the magnetic moment of the neutron and σ_i, $i = 1, 2, 3$ are the Pauli matrices. Denote the spin states of neutron along the z-axis as $|\uparrow\rangle$ and $|\downarrow\rangle$. Assume the initial state of neutron as $\rho(0) = \rho_{\uparrow\uparrow} = |\uparrow\rangle\langle\uparrow|$. $\rho^{(N)}$ is then obtained as [11]

$$\rho^{(N)}(T) = \left[\cos^2\left(\frac{\pi}{2N}\right)\right]^N \rho_{\uparrow\uparrow}\,. \tag{9.20}$$

Further,

$$P_\uparrow^{(N)}(T) = \left[\cos^2\left(\frac{\pi}{2N}\right)\right]^N\,. \tag{9.21}$$

This is the survival probability − the probability that neutron spin is in $|\uparrow\rangle$ state at every measurement time t_n. We note that $P_\uparrow^{(N)}(T) > P_\uparrow^{(N-1)}(T)$ for $N \geq 2$. As N increases the evolution is slowed down. In the limit $N \to \infty$

$$\begin{aligned}P_f(T) &= \lim_{N\to\infty} P_\uparrow^{(N)}(T) \\ &= 1\,. \end{aligned} \tag{9.22}$$

The significant effect of frequent observations is to *freeze* the system in its initial state, by delaying (for $N \geq 2$) and hindering (for $N \to \infty$) transitions

[1] In the words of John Gribbin "If, as quantum theory suggests, the world only exists because it is being observed, then it is also true that the world only changes because it is not being observed all the time."

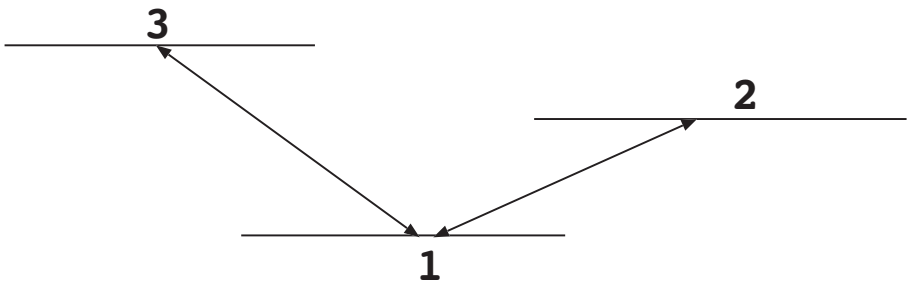


FIGURE 9.1 Energy level diagram for Cook's proposal.

to other states. *What is the essence of the quantum Zeno effect?* The essential point is that when the number of measurements is *finite* the decay rate is slowed and we have the *quantum Zeno effect*. When the number of measurements becomes *infinite* the transition is completely frozen and the result is the *quantum Zeno paradox*. The quantum Zeno effect was shown theoretically about three decades ago. However, interest on it was renewed by the idea of Cook [12] and its subsequent experimental verification.

9.3.3 Experimental Verification

Richard J. Cook [12] proposed an experiment on a trapped ion to test the quantum Zeno effect on induced transitions. Suppose the ion has three levels as shown in Fig. 9.1. Level-1 is the ground state. Level-2 is an excited metastable state. Cook's suggestion was to drive $1 \to 2$ transition with a π-pulse (a square-pulse of duration $T = \pi/\Omega$) while simultaneously applying a sequence of short measurement pulses. Suppose the ion is in level-1 at time $t = 0$. The π-pulse is applied at $t = nT/N = n\pi/(N\Omega)$ where $n = 1, 2, \cdots, N$.

In the rotating wave approximation the evolution equations for the density matrix ρ_{ij}, $i, j = 1, 2$ are given by

$$\dot{\rho}_{11} = \frac{1}{2}\mathrm{i}\Omega\left(\rho_{21} - \rho_{12}\right), \tag{9.23a}$$

$$\dot{\rho}_{12} = \frac{1}{2}\mathrm{i}\Omega\left(\rho_{22} - \rho_{11}\right), \tag{9.23b}$$

$$\dot{\rho}_{22} = \frac{1}{2}\mathrm{i}\Omega\left(\rho_{12} - \rho_{21}\right). \tag{9.23c}$$

Define

$$R_1 = \rho_{12} + \rho_{21}, \quad R_2 = \mathrm{i}\left(\rho_{12} - \rho_{21}\right), \tag{9.24a}$$

$$R_3 = \rho_{22} - \rho_{11} = P_2 - P_1 \tag{9.24b}$$

with $P_1 + P_2 = 1$. In terms of $\mathbf{R} = (R_1, R_2, R_3)$ and $\Omega = (\Omega, 0, 0)$ Eqs. (9.23) become

$$\dot{\mathbf{R}} = \Omega \times \mathbf{R}\,. \tag{9.25}$$

At $t = 0$ we have $\mathbf{R} = (0, 0, -1)$. The applied pulse induces transition from level 1 to 3. Subsequently, a spontaneous emission of a photon happens. The measurement pulse projects the system into level-1 or level-2. The measurement kills the terms ρ_{12} and ρ_{21} and leave ρ_{11} and ρ_{22} as such. Now, $\mathbf{R}$ becomes

$$\mathbf{R} = \left[0,\ \sin\left(\frac{\pi}{N}\right),\ -\cos\left(\frac{\pi}{N}\right)\right] . \tag{9.26}$$

Setting $R_2 = 0$ gives $\mathbf{R} = [0,\ 0,\ -\cos(\pi/N)]$. At $t = \pi/(N\Omega)$, $\mathbf{R}$ is the same at $t = 0$, however, the magnitude of it is reduced by a factor of $\cos(\pi/N)$. After the first measurement, $\mathbf{R}^{(1)}$ is given by

$$\begin{aligned} \mathbf{R}^{(1)} &= -\cos\left(\frac{\pi}{N}\right) \\ &= P_2^{(1)} - P_1^{(1)} , \end{aligned} \tag{9.27}$$

where $P_j^{(1)}$ is the occupation probability of level-j ($j = 1, 2$) at time $t = \pi/(N\Omega)$ [13]. We have

$$\begin{aligned} P_2^{(1)} &= \frac{1}{2}\left(1 + R_3^{(1)}\right) \\ &= \sin^2\left(\frac{\pi}{2N}\right) , \end{aligned} \tag{9.28a}$$

$$\begin{aligned} P_1^{(1)} &= 1 - P_2^{(1)} \\ &= \cos^2\left(\frac{\pi}{2N}\right) . \end{aligned} \tag{9.28b}$$

The survival probability, namely, the probability of finding the system in level-1 both in the first and second measurements is given by

$$\begin{aligned} P_1^{(1,2)} &= \cos^2\left(\frac{\pi}{2N}\right)\cos^2\left(\frac{\pi}{2N}\right) \\ &= \cos^4\left(\frac{\pi}{2N}\right) . \end{aligned} \tag{9.29}$$

The survival probability after N measurements is

$$P_1^{(N)}(T) = \cos^{2N}\left(\frac{\pi}{2N}\right) , \tag{9.30}$$

$$P_2^{(N)}(T) = 1 - P_1^{(N)}(T) . \tag{9.31}$$

Cook considered a slight variance of the quantum Zeno effect of Misra and Sudarshan with

$$\dot{P}_1 = \frac{\Omega\pi}{2N}\left(P_2 - P_1\right) , \tag{9.32}$$

$$\dot{P}_2 = \frac{\Omega\pi}{2N}\left(P_1 - P_2\right) . \tag{9.33}$$

From this set of equations we have [12]

$$P_2(T) = \frac{1}{2}\left[1 - \mathrm{e}^{-\pi^2/(2N)}\right] . \tag{9.34}$$

$P_2(T)$ is the occupation probability of level-2 with the transitions $1 \to 2 \to 1$ and so on. Note that P_2 given by Eq. (9.34) is not the one given by Eq. (9.30).

Itano and his coworkers [14] did an experiment with $^9Be^+$, similar to the one proposed by Cook [12]. The time development was given by a π-pulse tuned to the $1-2$ transition frequency. A π-pulse (a radio frequency (RF) pulse) transformed the initial state $|1\rangle$ into $|2\rangle$ at the end of the pulse, provided there was no measurement. The population of lower level was measured nonselectively and also without recording the results in rapid succession by the fluorescence induced by very short pulses of laser which coupled level-1 with the level-3. The population at time T was measured by a final pulse and recorded. The experimental result was found to be in good agreement with prediction of the quantum Zeno effect. The P_2 calculated for $N = 1, 2, 4, 8, 16, 32$ are $0.995, 0.5, 0.335, 0.194, 0.103, 0.013$ respectively. These values are in agreement with (9.34).

9.3.4 Further Development on Zeno Effect

The quantum Zeno effect has been shown theoretically for two states wave functions like spin particles [15], right- and left-isomers [16], two-state model of the localized Born–Oppenheimer states [17], multi-level system [18], a system of particles with spin-1/2 interacting with a magnetic field [19], quantum version of an inverted pendulum [20], neutron spin [21], Raman scattering [21] and models of trapped ions [22]. Experimental verification of quantum Zeno effect has been done with the system of $^{172}Yb^+$ ion [23] and $^{171}Yb^+$ ion [24], in an optical pumping [25], systems with forced Rabi oscillations between discrete atomic levels [14] and spontaneously decaying systems [26]. It was predicted that there are regimes in which repeated measurements can accelerate transitions [27-32] and this phenomenon was found experimentally [26] as well. This effect is known as *anti-Zeno effect* or *anti-Zeno paradox* or *inverse Zeno effect*. Specifically, the quantum Zeno and anti-Zeno paradoxes arise due to infinitely frequent measurements of time-independent and time-dependent projection operators respectively. It is shown that the transition from coherent to incoherent fluorescence energy transfer can be regarded as a demonstration of quantum Zeno or anti-Zeno effect [33].

Some applications of quantum Zeno effect are suggested. Numerical simulation of a new method of quantum Zeno tomography in which a Mach–Zehnder interferometer is adopted to measure transmissivity of gray samples was considered [34]. In contrast to standard tomography, considerable reduction of false reproduced points is demonstrated. A possible construction of photon-phonon interferometer is suggested, where interference between an optical mode in a cavity and one-dimensional vibration phonon mode of an ion trapped in the same cavity takes place [35]. Its inner degrees of freedom are removed with the application of Zeno effect by freezing the ion in its initial state. The effect has explained the suppression of the conversion decay of an isomer of uranium-235 in the lattice of silver [36].

The occurrence of quantum Zeno effect does not depend on whether information is taken from the measurements or not. Therefore, decoherence processes, such as optical pumping and coupling to stochastic external fields can result in the quantum Zeno effect. This also points out that there exists a classical counterpart. Quantum Zeno effect has been found in wave or oscillatory systems [37] and optical fibers [38]. The quantum Zeno effect is found to vanish at all orders in $\hbar$, when $\hbar \to 0$. This implies that it is a quantum phenomenon without a classical analog [39].

Quantum Zeno effect is important in understanding quantum theory of measurement and is in fact a vital tool in quantum computing. Due to decoherence, storing a quantum state for a long time is impossible. Quantum Zeno effect may be utilized to store a quantum state as long as we wish. For a detailed discussion on mathematical and physical aspects of Zeno dynamics one may refer to ref. [40].

9.4 QUANTUM TELEPORTATION

Classically, transport of an object is to transport all the particles of it. An object to be teleported can be characterized by its properties. These properties can be determined by measurement in classical physics. Scanned information is useful for reconstructing the object and notably the original parts of the object are not needed. But a fundamental question is *what is the case if an object is a quantum state? What does happen to the quantum properties of the system, that are not measurable with desired accuracy due to Heisenberg's uncertainty principle?*

Reconstructing the quantum state of a system on another system of the same type at a distant place is termed as *quantum teleportation*. The point is that the quantum state of the system to be teleported is unknown and in fact we cannot find it. Therefore, quantum teleportation is the transmission and reconstruction of an unknown quantum state of a system over arbitrary distances. Essentially, in quantum teleportation the system is not to be teleported but only its state is to be teleported to another system of same kind. In quantum teleportation the original state is destroyed and an exact copy of the quantum state is produced. In the case of fax copy, the original is preserved and only a partial copy is made. The quantum teleportation was first discussed by Yakir Aharonov and D. Albert using the method of nonlocal measurements [41].

9.4.1 A Three Stage Scheme

Charles H. Bennett and his co-workers [42] have pointed out that the quantum state of a particle can be transferred to another particle provided one does not get any information about the state during the course of transportation. The above can be realized by using entanglement. The scheme of Bennett et al consists of essentially three stages:

1. An EPR source of entangled particles is prepared. Sender and receiver share each particle from a pair emitted by the source.
2. Sender performs a Bell-operator measurement on his EPR and the teleportation-target particles.
3. Sender transmits the result of the measurement to the receiver through a classical channel. Then the receiver performs a suitable unitary operation on the EPR particle.

Let us describe the above three stages scheme in detail. Suppose Alice (sender) has two two-level particles, say, particle-1 and particle-2. A two-level quantum system is a *qubit*. Bob (receiver) who is at a distant location has a particle, say, particle-3. The two states of a particle are labelled as $|0\rangle$ and $|1\rangle$. The superposition state is $|\psi\rangle = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$. Alice wants Bob, to have the particle-3 with the state of the particle-1. Since properties of quantum systems cannot be fully obtained by measurements Alice is unable to provide required information of the particle-1 to Bob by carrying out the measurements on it.

The joint state of particles 2 and 3 is, for example,

$$|\psi\rangle_{\rm AB} = \frac{1}{\sqrt{2}}\Big(|0\rangle_{\rm A}|0\rangle_{\rm B} + |1\rangle_{\rm A}|1\rangle_{\rm B}\Big)\,. \tag{9.35}$$

This state is *entangled* because it is not possible to write it as a product of the individual states, like $|00\rangle$. $|\psi\rangle_{\rm AB}$ gives no information about the individual particles but points out that the particles 2 and 3 are in same states. *What is the feature of the above entangled state?* A measurement on, say, particle-2 gives the state of the particle-3 and vice-versa.

Suppose the state of the particle-1 is labelled as $|\phi\rangle = a|0\rangle + b|1\rangle$ with the unknown a and b: $|\phi\rangle$ is to be teleported to Bob. Now the total state of the three particles is

$$|\phi\rangle_{\rm AB} := |\phi\rangle|\psi\rangle_{\rm AB} = \frac{1}{\sqrt{2}}\left(a|0\rangle + b|1\rangle\right)\left(|00\rangle + |11\rangle\right)\,. \tag{9.36}$$

Write the above state as

$$\begin{aligned} |\phi\rangle_{\rm AB} &= \frac{1}{\sqrt{2}}\left[a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right] \\ &= \frac{1}{2}\left[|\phi^+\rangle(a|0\rangle + b|1\rangle) + |\phi^-\rangle(a|0\rangle - b|1\rangle)\right. \\ &\quad \left. + |\psi^+\rangle\left(a|1\rangle + b|0\rangle\right) + |\psi^-\rangle\left(a|1\rangle - b|0\rangle\right)\right], \end{aligned} \tag{9.37a}$$

where

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right], \quad |\phi^-\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle - |11\rangle\right], \tag{9.37b}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left[|01\rangle + |10\rangle\right], \quad |\psi^-\rangle = \frac{1}{\sqrt{2}}\left[|01\rangle - |10\rangle\right]\,. \tag{9.37c}$$

$|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ form an orthonormal basis for Alice's two particles. This basis is called the *Bell basis*. In the above $|01\rangle$ indicates that particle-1 is in the state $|0\rangle$ while the particle-2 is in $|1\rangle$. Similar meaning for $|00\rangle$, $|10\rangle$ and $|11\rangle$. The protocol then proceeds as follows:

1. Alice will carry out projection measurements on her particles. She will get any one of the four Bell states randomly with equal probability.

2. Suppose the state got by Alice is $|\psi^+\rangle$. Then in the state $|\phi\rangle_{\mathrm{AB}}$ the three particles collapse into the state

$$|\phi\rangle_{\mathrm{AB}} = |\psi^+\rangle\,[a|1\rangle + b|0\rangle]\ , \tag{9.38}$$

   where $a|1\rangle + b|0\rangle$ represents the state of the particle-3 (of Bob). Now, Alice wants to convey this result to Bob by a classical channel, for example, over the phone. She informs the difference in the state of the particles 2 and 3.

3. *What does Bob do now?* The state $|\psi^+\rangle$ indicates that (refer to Eq. (9.37c)) the states of the particles 1 and 2 are orthogonal (opposite). But the states of particles 2 and 3 are prepared as in Eq. (9.35) which means their states are the same. The state of the particle-2 is hence opposite to 1 but the same as 3. This is true only if particles 1 and 3 are orthogonal. The states of them are thus opposite. Since the state of particle-1 is $|\phi\rangle = a|0\rangle + b|1\rangle$ the state of particle-3 is $a|1\rangle + b|0\rangle$. Therefore, Bob has to do the NOT operation that changes the state of particle-3 into $a|0\rangle + b|1\rangle$. This completes the protocol.

   What has to be done if Alice got some other Bell state instead of $|\psi^+\rangle$*?*

9.4.2 Features of the Three Stage Scheme

Some of the features of the above teleportation scheme are summarized as follows:

1. During the Bell-state measurement particle-1 is set entangled with particle-2. Hence, particle-1 lost its identity. The state $|\phi\rangle$ on Alice's side during teleportation is destroyed.

2. Alice need not know the location of Bob.

3. The initial state of particle-1 is unknown to anyone and even undefined at the time of measurement.

4. The measurements of Alice and the operations of Bob are local.

5. Bob's operations are independent of the state of the particle-1 state.

6. The classical communication used is local.

7. The measurement does not provide information of the particles involved. Thus, no damage to the no-cloning theorem of Wooters and Zuerk [43].

8. According to the theory of relativity, information transfer faster than light is not possible. Quantum teleportation does not take place faster than light, because the communication channel used is classical.

Motivated by the proposal of Bennett and his coworkers various groups have initiated investigation on experimental quantum teleportation. Bouwmeester et al [44] reported the first experimental quantum teleportation. They used pairs of polarization entangled photons produced through pulsed down-conversion. Two photon interferometric method is employed to transfer the state of one photon onto another. Furasawa et al [45] demonstrated teleportation using the protocol in ref.[46] with squeezed state entanglement. The experiment of Boschi et al [47] involved a quantum optical implementation.

The teleportation schemes could be used to setup links between quantum computers. Research on quantum teleportation also opens new types of experiments and investigation on the fundamentals of quantum mechanics. It can be used to transmit information desirably in a noisy environment. Quantum teleportation can be used to construct quantum gates. As the particle is not sent, a quantum teleportation is a novel scheme of secure transfer of information. For more details on teleportation one may refer to refs.[41-49].

Solved Problem 1:

To teleport an EPR pair, we require a maximally entanglement of three particles. Find out the useful initial states.

The wave function of an entangled pair can be

$$|\psi_{12}\rangle = \alpha|00\rangle + \beta|11\rangle, \tag{9.39}$$

where $|\alpha|^2 + |\beta|^2 = 1$ or $|\psi_{\rm EPR}\rangle = \alpha|01\rangle + \beta|10\rangle$. The possible maximally entangled states are

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), \quad \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle), \\ &\frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle), \quad \frac{1}{\sqrt{2}}(|100\rangle \pm |011\rangle). \end{aligned} \tag{9.40}$$

We can choose a triplet in the form of GHZ

$$|\psi_{\rm GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle). \tag{9.41}$$

Then the initial state is $|\psi\rangle = |\psi_{\rm EPR}\rangle \otimes |\psi_{\rm GHZ}\rangle$.

9.5 QUANTUM GAMES

Game theory is referred to as the study of decision making in conflict situation. It has applications in military warfare, anthropology, social psychology, economics, politics, business and philosophy [50-53]. Interest has been paid on extending classical game theory to the quantum domain to study the problems of quantum computation, information and communication. Quantum game theory began with the seminal work of David A. Meyer (1999). It deals with classical games in the realm of quantum mechanics. Considerable progress has been made in this area. Several protocols have been proposed and certain classical games have been extended to the quantum case. The interesting point is that quantum superposition and entanglement between the states of the players ensure the players to outperform the classical moves through quantum mechanical strategies.

9.5.1 Classical Game

In classical game theory, a game essentially consists of

1. a set of players,
2. a set of strategies dictating the actions of players and
3. a payoff function specifying the reward for a set of strategy choices. The payoff to a player is a numerical value.

In a game theory the goal of a player is to optimize his payoff. In a game, a dominant strategy is that the player has to do at least as well as any other competing strategy. The *Nash equilibrium* is the most important among the possible equilibria [52,54]. It is the combination of strategies with which none of the players can improve his/her payoff by a unilateral change of strategy. A *Pareto optimal* outcome is that from which no player is able to obtain a higher profit without reducing the utility of another.

9.5.2 Quantum Game

A quantum system manipulated by players, where the usefulness of the possible moves are defined, can be thought of as a quantum game [54-56]. A two player game $\Gamma = (\mathcal{H}, P, P_{\mathrm{A}}, P_{\mathrm{B}})$ is specified by

1. the Hilbert space $\mathcal{H}$ of the system,
2. the initial state $P \in \mathcal{P}(\mathcal{H})$, with $\mathcal{P}(\mathcal{H})$ being the state space,
3. $P = P_{\mathrm{A}} \otimes P_{\mathrm{B}}$ describing the players, say Alice (A) and Bob (B) and
4. initial strategies P_{A} and P_{B}.

$P_{\rm A}$ and $P_{\rm B}$ specify the payoff or utility for the players. Quantum tactics $S_{\rm A}$ and $S_{\rm B}$ are linear quantum operations mapping the state space on itself and are positive trace-preserving. A change of strategy of the players is represented by a linear map. Schematically, we have

$$P \stackrel{S_{\rm A},S_{\rm B}}{\longrightarrow} \sigma \Rightarrow (P_{\rm A}, P_{\rm B}) \, . \tag{9.42}$$

The generalization of the above for the N players is straight-forward. A most notable feature of quantum game theory is that effects not possible in the classical case can occur due to quantum entanglement and interference. Quantum game theory differs from classical game theory by using superposed initial states, quantum entanglement of initial states and superposition of strategies to be used in the initial states. Quantum game approach has been applied to typical classical games such as coin tossing [54,57], the prisoners' dilemma [58-62], the Monty Hall problem [63,64], the battle of the sexes [65,66], rock-scissors-paper [67] and others [68-70].

9.5.3 Parrondo's Games

Juan Manuel RodrÃŋguez Parrondo has discovered an apparent and fascinating paradox called *Parrondo paradox* in game theory. In it, two games when played individually are losing can be combined to yield a winning game [71-74]. That is, Parrondo paradox results when a losing game is played by disturbing the winning feedback by a second losing game so that the first losing game becomes a winning.

9.5.3.1 Classical Games

Classical Parrondo's games is cast in the form of gambling games by utilizing a set of biased coins. However, here we first illustrate the paradox with a deterministic game [75] and then that of Parrondo. Suppose the current capital of a player is M (even) dollars.

Game A:

The player wins 1 dollar if M is even, otherwise loses 3 dollars.

Game B:

The player wins 1 dollar if M is odd, otherwise loses 3 dollars.

Playing only the game A or B repeatedly leads to a steady loss of 1 dollar per play. *What will happen if these two games are played alternately?* Playing $\mathrm{ABAB}\cdots$ gives a steady win of 1 dollar per play: a combination of two losing games results in a winning game. So, Parrondo's paradox seems to be conveying that playing the sequence $(\mathrm{AB})^m$ is better than $\mathrm{A}^m\mathrm{B}^m$. *What is the outcome of the game if we replace the loss of* 3 *dollars by the loss of* 1 *dollar and the sequence* $\mathrm{ABAB}\cdots$ *is followed?*

TABLE 9.2 The choice of the coin to be tossed at nth game.

Game_{n-2}	Game_{n-1}	Coin chosen
Loss	Loss	2
Loss	Win	3
Win	Loss	3
Win	Win	4

The original games of Parrondo is capital-dependent (CD) requiring feedback loops [74]. Parrondo, Gregory P. Harmer and Derek Abbott [73] proposed a capital-independent but history-dependent (HD) game with feed-forward loops. The construction of the games is the following.

Game A:

It involves tossing a weighted coin 1 with probability $p_{\text{w}} = 0.5 - \epsilon$, $0 < \epsilon \ll 1$ for winning and $p_{\text{l}} = 1 - p_{\text{w}}$ for losing.

Game B:

CD and HD types of games differ. There are two biased coins (coins 2 and 3) in the CD game and $p_{2\text{w}} = 0.1 - \epsilon$ and $p_{3\text{w}} = 0.75 - \epsilon$. Coin 2 or 3 is tossed depending on the capital M at the instant and hence the name CD game. Coin 2 is tossed if M is a multiple of 3, otherwise coin 3. Note that, on the average, coin 3 will be played more frequently than coin 2. However, coin 2 outweighs coin 3 because of its poor winning probability. As a result, game B is overall a losing game.

In an HD game 3 coins are used. One of them is tossed based on the outcome of the previous game. This is illustrated in table 9.2. *What are the probabilities of the three coins?* Evidently, coin 3 is tossed more often than the other coins, and hence this is a losing game.

In the Parrondo's games both A and B are losing games for small positive values of ϵ. However, simulation of the games have predicted that switching between the losing games, e.g., playing two times A, two times B, two times A, and so on result in winning. That is, a player can play the two losing games A and B in such an order to realize a winning expectation. For detailed results see refs.[73-76]. Promising application areas for Parrondo's paradox are in biogenesis spin systems, stochastic signal processing, economics and sociological modeling [76].

9.5.3.2 Quantum Version of Parrondo's Games

We present the quantum version of the HD Parrondo's games formulated by Flitney, Ng and Abbott [77] A quantum version CD Parrondo's games is reported in ref.[78]. In classical gambling games there is a random element. It

is replaced by a superposition of all the possible results in quantum games. We can realize new behavior by this. The coin tossing game can be quantized by an $SU(2)$ operation on a qubit. A physical system may be a collection of polarized photons with $|0\rangle$ and $|1\rangle$ representing horizontal and vertical polarizations respectively.

An arbitrary $SU(2)$ operation on a qubit is expressed as

$$\begin{aligned}\widehat{A}(\theta,\gamma,\delta) &= \widehat{P}(\gamma)\widehat{R}(\theta)\widehat{P}(\delta) \\ &= \begin{pmatrix} \mathrm{e}^{-\mathrm{i}(\gamma+\delta)/2}\cos\theta & -\mathrm{e}^{-\mathrm{i}(\gamma-\delta)/2}\sin\theta \\ \mathrm{e}^{\mathrm{i}(\gamma-\delta)/2}\cos\theta & \mathrm{e}^{\mathrm{i}(\gamma+\delta)/2}\cos\theta \end{pmatrix}, \end{aligned} \tag{9.43}$$

where $\theta \in [-\pi, \pi]$ and $\gamma, \delta \in [0, 2\pi]$. This is the quantum analogue of the game A−a single toss of a biased coin. Game B consists of four $SU(2)$ operations, each of the form of Eq. (9.43):

$$\widehat{B} = \begin{pmatrix} A(\phi_1,\alpha_1,\beta_1) & 0 & 0 & 0 \\ 0 & A(\phi_2,\alpha_2,\beta_2) & 0 & 0 \\ 0 & 0 & A(\phi_3,\alpha_3,\beta_3) & 0 \\ 0 & 0 & 0 & A(\phi_4,\alpha_4,\beta_4) \end{pmatrix}. \tag{9.44}$$

This acts on the state

$$|\psi(t-2)\rangle \otimes |\psi(t-1)\rangle \otimes |i\rangle\ , \tag{9.45}$$

where $|\psi(t-1)\rangle$ and $|\psi(t-2)\rangle$ represent the results of the two previous games. $|i\rangle$ is the qubit's initial state. We write

$$\widehat{B}|q_1 q_2 q_3\rangle = |q_1 q_2 b\rangle\ , \tag{9.46}$$

where $q_i \in \{0, 1\}$ and b is the output of the game B. The result of n successive games of B is found by

$$|\psi_f\rangle = \left(\widehat{I}^{n-1} \otimes \widehat{B}\right)\left(\widehat{I}^{n-2} \otimes \widehat{B} \otimes \widehat{I}\right) \cdots \left(\widehat{B} \otimes \widehat{I}^{n-1}\right)|\psi_i\rangle\ , \tag{9.47}$$

where $|\psi_i\rangle$ is the initial state of $n+2$ qubits.

Suppose a player plays AAB n times. Then

$$\begin{aligned}|\psi_f\rangle &= \left\{\widehat{I}^{3n-3} \otimes \left[\widehat{B}\left(\widehat{A} \otimes \widehat{A} \otimes \widehat{I}\right)\right]\right\} \\ &\quad \times \left\{\widehat{I}^{3n-6} \otimes \left[\widehat{B}\left(\widehat{A} \otimes \widehat{A} \otimes \widehat{I}\right)\right] \otimes \widehat{I}^3\right\} \\ &\quad \cdots \left\{\left[\widehat{B}\left(\widehat{A} \otimes \widehat{A} \otimes \widehat{I}\right)\right]\widehat{I}^{3n-3}\right\}|\psi_i\rangle \\ &= \widehat{G}^n|\psi_i\rangle\ , \end{aligned} \tag{9.48}$$

where $\widehat{G}^n = \widehat{B}\left(\widehat{A} \otimes \widehat{A} \otimes \widehat{I}\right)$ and $|\psi_i\rangle$ is an initial state of $3n$ qubits.

The classical game can be reproduced by $|\psi_i\rangle = |00\cdots0\rangle$. Suppose $|\psi_i\rangle$ is the entangled state

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}\left(|00\cdots0\rangle + |11\cdots1\rangle\right) \ . \tag{9.49}$$

In this case interference effects enhance or reduce the success of the player. The addition of nonzero phases in the operators $\widehat{A}$ and $\widehat{B}$ alter this interference. Let the payoff for a $|1\rangle$ state be 1 and for a $|0\rangle$ state be -1. Since quantum mechanics is a probabilistic theory $\langle$ payoff $\rangle$ is important and is given by

$$\langle \text{ payoff } \rangle = |\$\rangle = \sum_{j=0}^{n}\left[(2j-n)\sum_{j'}|\langle\psi_j^{j'}|\psi_f\rangle|^2\right] \ . \tag{9.50}$$

In Eq. (9.50) the second summation is over all basis states $\langle\psi_j^{j'}|$ with $n-j$ zero's and j ones.

For the sequence AAB with $|\psi_i\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ we have

$$\begin{aligned}\langle\$_{\text{AAB}}\rangle \quad = \quad & \frac{1}{2}\cos 2\theta\,(\cos 2\phi_4 - \cos 2\phi_1) \\ & + \frac{1}{4}\sin^2 2\theta\,[\cos(2\delta+\beta_1)\sin 2\phi_1 \\ & - \cos(2\delta+\beta_2)\sin 2\phi_2 \\ & - \cos(2\delta+\beta_3)\sin 2\phi_3 \\ & + \cos(2\delta+\beta_4)\sin 2\phi_4] \ .\end{aligned} \tag{9.51}$$

The maximum payoff is for $\beta_1 = \beta_4 = -2\delta$ and $\beta_2 = \beta_3 = \pi - 2\delta$. The result is minimum for $\beta_1 = \beta_4 = \pi - 2\delta$ and $\beta_2 = \beta_3 = -2\delta$. Observe that the values of ϕ_i's are irrelevant. $\langle\$_{\text{AAB}}\rangle$ varies between $-0.812 + 0.03\epsilon$ and $0.812 + 0.24\epsilon$. The classical payoff is $1/60 - 28\epsilon/15$. The classical and quantum payoffs for the sequence AAB$\cdots$AAB are $1/60 - 28\epsilon/15$ and $2\epsilon/15$ respectively. For more results see ref. [77].

9.5.4 Prisoners' Dilemma

The prisoners' dilemma (PD) is an another famous classical game extended into quantum domain [58]. The Parrondo's games are played by a single player whereas PD game is played by two players. It is a nonzero sum game. The two players are not in opposition to each other. They may benefit from mutual cooperation.

9.5.4.1 A Classical Game

In the classical version of the PD game the two players, say, Alice and Bob, decide independently to choose defect (strategy D) or cooperate (strategy C). Depending on their own decision they receive a certain payoff as in table 9.3.

TABLE 9.3 Payoff for the PD. The first and second entries in the parenthesis denote the payoffs of Alice and Bob respectively. (Reproduced with permission from J. Eisert, M. Wilkens and M. Lewenstein, *Phys. Rev. Lett.* 83:3077, 1999. Copyright 1999, American Physical Society.)

	Bob:C	Bob:D
Alice:C	$(3,3)$	$(0,5)$
Alice:D	$(5,0)$	$(1,1)$

There exists a dominant strategy, that of always defecting, because it gives a better payoff when if the other player cooperates (5 instead of 3) or if the other player defects (1 instead of 3). If both players have a dominant strategy then this combination is the Nash equilibrium. The Nash equilibrium outcome {D,D} is not a good one for the players. However, since both the players would receive a payoff of 3 if they cooperate, the Pareto optimal results. Here no player will be able to improve his/her payoff by unilaterally changing own strategy. *This is the dilemma.*

9.5.4.2 A Quantum PD Game

Does a quantum version of the PD game have a different solution? A quantum model of the PD is proposed by Eisert et al [58]. In this model the two players escape the dilemma by carrying out quantum strategies. The quantum version is depicted in Fig. 9.2. To get nonclassical results entanglement between the players' moves is created. Initial state of the qubits is $|\psi_i\rangle = |\mathrm{C}\rangle|\mathrm{C}\rangle = |\mathrm{CC}\rangle$. The final state is

$$|\psi_f\rangle = \widehat{J}^{\dagger}\left(\widehat{U}_{\mathrm{A}} \otimes \widehat{U}_{\mathrm{B}}\right)\widehat{J}|\psi_i\rangle\ , \tag{9.52}$$

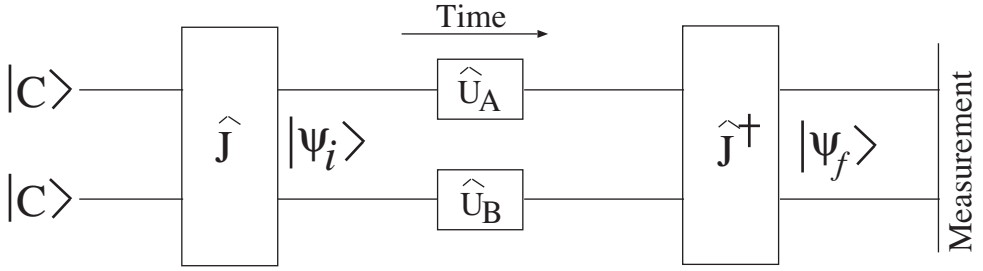


FIGURE 9.2 The setup for the two player PD quantum game showing the flow of information. (Reproduced with permission from J. Eisert, M. Wilkens and M. Lewenstein, *Phys. Rev. Lett.* 83:3077, 1999. Copyright 1999, American Physical Society.)

where $\widehat{J}$ is an operator entangling the qubits of the players. Strategic moves are associated with $\widehat{U}_{\rm A}$ (Alice) and $\widehat{U}_{\rm B}$ (Bob). A disentangling gate $\widehat{J}^{\dagger}$ is used for a measurement on the final state. The expectation value of payoff of Alice is

$$\begin{aligned}\langle \$_{\rm A}\rangle &= P_{\rm CC}|\langle\psi_f|{\rm CC}\rangle|^2 + P_{\rm CD}|\langle\psi_f|{\rm CD}\rangle|^2 \\ &\quad + P_{\rm DC}|\langle\psi_f|{\rm DC}\rangle|^2 + P_{\rm DD}|\langle\psi_f|{\rm DD}\rangle|^2 \,, \end{aligned} \tag{9.53}$$

where P_{ij}, $i,j \in \{{\rm C},{\rm D}\}$ is the payoff for Alice with the game outcome ij. Interchanging i and j in P_{ij} in Eq. (9.53) gives the payoff of Bob. We note that expected payoff of Alice depends on $\widehat{U}_{\rm A}$ and also on Bob's choice $\widehat{U}_{\rm B}$. If the players play with classical strategies the quantum game gives nothing surprise. However, if they utilize quantum strategies the entanglement opens the opportunity for their moves to interact in ways which have no classical analogue.

Suppose we have quantum strategies of the form

$$\widehat{U}(\theta,\phi) = \begin{pmatrix} {\rm e}^{{\rm i}\phi}\cos(\theta/2) & {\rm i}\sin(\theta/2) \\ {\rm i}\sin(\theta/2) & {\rm e}^{-{\rm i}\phi}\cos(\theta/2) \end{pmatrix} \,, \tag{9.54}$$

where $\theta \in [0,\pi]$, $\phi \in [0,\pi/2]$ and consider the entangling operator in the form

$$\widehat{J} = \exp\left({\rm i}\gamma \widehat{D}\otimes\widehat{D}/2\right), \quad \gamma \in [0,\pi/2] \,. \tag{9.55}$$

The strategy that *always cooperate* is $\widehat{C} = \widehat{U}(0) = \widehat{I}$ and *always defect* strategy is $\widehat{D} = \widehat{U}(\pi) = \widehat{F}$. Against a classical Alice playing with $\widehat{U}(\theta)$, a quantum Bob can play Eisert's *miracle* move [58]

$$\begin{aligned}\widehat{M} &= \widehat{U}(\pi/2,\pi/2) \\ &= \frac{\rm i}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{aligned} \tag{9.56}$$

that gives $\langle \$_{\rm B}\rangle = 3 + 2\sin\theta$ for Bob and only $\langle \$_{\rm A}\rangle = (1-\sin\theta)/2$. The dilemma is removed. It has been demonstrated that there was a new Nash equilibrium producing a payoff of 3 to both the players and is Pareto optimal. In ref.[79] a quantum PD with Eisert et al's scheme was achieved on a two qubit NMR computer with various degrees of entanglement from a classical to a maximally entangled quantum game. Good agreement between theory and experiment was obtained.

Solved Problem 2:

In the quantum version of prisoners' dilemma game what is the state of the game after passing the state $|CC\rangle$ through the gate $\hat{J}$? What are the explicit expressions of both players' payoff?

We obtain

$$\begin{aligned} |\psi_i\rangle &= \hat{J}|CC\rangle \\ &= \cos(\gamma/2)|CC\rangle + \mathrm{i}\sin(\gamma/2)|DD\rangle. \end{aligned} \tag{9.57}$$

For the case of payoff in table 9.3 we obtain

$$\$_{\mathrm{A}} = 3P_{\mathrm{CC}} + 1P_{\mathrm{DD}} + 0P_{\mathrm{CD}} + 5P_{\mathrm{DC}}, \tag{9.58a}$$

$$\$_{\mathrm{B}} = 3P_{\mathrm{CC}} + 1P_{\mathrm{DD}} + 5P_{\mathrm{CD}} + 0P_{\mathrm{DC}}. \tag{9.58b}$$

9.5.5 Relativistic Quantum Games in Noninertial Frames [80]

The behavior of prior entanglement shared among the two spatially separated partner can be extended to the relativistic setup in noninertial frames [80-82]. In the following we consider the quantum PD and show that the playoff functions of the players are influenced by the acceleration of the noninertial frame and the symmetry of the game is affected [80]. We will notice that the dominance of the player ceases due to the acceleration of the frame.

Assume that Alice and Bob share the initial state $|\psi_i\rangle = \widehat{J}|CC\rangle_{\mathrm{A,B}}$. This state after applying entangling operator

$$\widehat{D}_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{9.59}$$

is

$$|\psi_i\rangle = \cos(\gamma/2)|CC\rangle_{\mathrm{A,B}} + \mathrm{i}\sin(\gamma/2)|DD\rangle_{\mathrm{A,B}}\ . \tag{9.60}$$

$|\psi_i\rangle$ is maximally entangled for $\gamma = \pi/2$.

Suppose Alice stays stationary. Bob moves with a uniform acceleration. Introduce two different sets of Rindler coordinates[2] (τ, ζ). They differ by a change in sign to cover Minkowski space[3]. Let us define two Rindler regions I and II as shown in Fig. 9.3. An observer in a region cannot access the message leaking to the other region. Call the observer in the region-II as antiobserver (or antiparticle). Consider the creation and annihilation operators a_k (of particle) and b_k (of antiparticle) in Minkowski space and k represents a single-mode. They are related to the creation operator c_k^I (in the region-I) and the annihilation operator d_k^{II+} (in region-II) by the transformation

$$a_k = \cos r\, c_k^I - \mathrm{e}^{-\mathrm{i}\phi}\sin r\, d_k^{II\dagger}\ , \tag{9.61a}$$

$$b_k^\dagger = \mathrm{e}^{\mathrm{i}\phi}\sin r\, c_k^I + \cos r\, d_k^{II\dagger}\ . \tag{9.61b}$$

[2] A uniformly accelerated observer will follow a hyperbolic path. This means that we can write a coordinate transformation from the stationary reference frame to the moving one by using hyperbolic functions. An observer at rest in Rindler coordinates has a constant acceleration.

[3] Minkowski space is a four-dimensional space where three coordinates specify the position of a point in space and the fourth one represents the time at which an event occurs at that point.

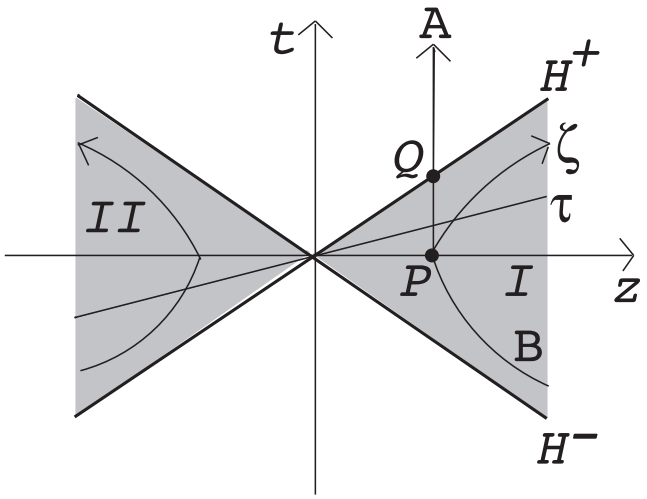


FIGURE 9.3 Rindler space time diagram. A and B refer to Alice and Bob respectively. The lines $H^{\pm}$ represent Bob's future and past and correspond to $\tau = \infty$ and $-\infty$. Alice and Bob share an entangled initial state at P. Q is the point where Alice crosses Bob's future horizon. (Reproduced with permission from S. Khan and M. Khalid Khan, *J. Phys. A: Math. Theor.* 44:355302, 2011. Copyright 2011, Institute of Physics.)

ϕ is an unimportant phase and r is defined through $\cos r = \left(\mathrm{e}^{-2\pi\omega c/a} + 1\right)^{-1/2}$. r is the dimensionless acceleration parameter. The constants a, c and ω are the acceleration of Bob, speed of light in vacuum and the frequency of the Dirac's particle respectively. $r = 0$ and $\pi/4$ for $a = 0$ and $a = \infty$ respectively. From Eq. (9.61a) the Minkowski vacuum state is given by

$$|0\rangle_M = \cos r \; |C\rangle_I |C\rangle_{II} + \sin r \; |D\rangle_I |D\rangle_{II} \; . \tag{9.62}$$

Using the adjoint of Eq. (9.61a) the excited state in Minkowski space-time is related to Rindler modes as

$$|D\rangle_M = |D\rangle_I |C\rangle_{II} \; . \tag{9.63}$$

Then the entangled initial state given by Eq. (9.60) becomes

$$\begin{aligned} |\psi_{\mathrm{A},I,II}\rangle \;\; = \;\; & \cos(\gamma/2)\, \cos r \, |C\rangle_{\mathrm{A}} |C\rangle_I |C\rangle_{II} \\ & + \cos(\gamma/2)\, \sin r \, |C\rangle_{\mathrm{A}} |D\rangle_I |D\rangle_{II} \\ & + \mathrm{i} \sin(\gamma/2)\, \sin r \, |D\rangle_{\mathrm{A}} |D\rangle_I |C\rangle_{II} \; . \end{aligned} \tag{9.64}$$

Because Bob is disconnected from II, we take trace over all the modes in this

TABLE 9.4 The payoff of the players as a function of the acceleration of Bob's frame. (Reproduced with permission from S. Khan and M. Khalid Khan, *J. Phys. A: Math. Theor.* 44:355302, 2011. Copyright 2011, Institute of Physics.)

	Bob: $\widehat{C}$	Bob: $\widehat{D}$
Alice: $\widehat{C}$	$3\cos^r,\ 4-\cos 2r$	$3\sin^2 r,\ 4+\cos 2r$
Alice: $\widehat{D}$	$3+2\cos 2r,\ \sin^2 r$	$3-2\cos 2r,\ \cos^2 r$

region. Then the density matrix between the two players is [80]

$$\rho_{\mathrm{A,B},I} = \begin{pmatrix} \cos^2 r\cos^2\dfrac{\gamma}{2} & 0 & 0 & -\dfrac{\mathrm{i}}{2}\cos r\,\sin\gamma \\ 0 & \cos^2\dfrac{\gamma}{2}\sin^2 r & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \dfrac{\mathrm{i}}{2}\cos r\,\sin\gamma & 0 & 0 & \sin^2\dfrac{\gamma}{2} \end{pmatrix}. \tag{9.65}$$

The unitary operators representing the moves of Alice and Bob are

$$\widehat{U}_N(\alpha,\theta) = \begin{pmatrix} \mathrm{e}^{\mathrm{i}\alpha_N}\cos(\theta_N/2) & \mathrm{i}\sin(\theta_N/2) \\ \mathrm{i}\sin(\theta_N/2) & \mathrm{e}^{-\mathrm{i}\alpha_N}\cos(\theta_N/2) \end{pmatrix}, \tag{9.66}$$

where $N = \mathrm{A},\mathrm{B}$, $\theta \in [0,\,\pi]$ and $\alpha \in [0,\,2\pi]$. The cooperation and defection correspond to $\widehat{U}_N(0,0)$ and $\widehat{U}_N(0,\pi)$ respectively. After making the decisions but before the measurement [58]

$$\rho = \widehat{J}^\dagger(U_\mathrm{A}\otimes U_\mathrm{B})\rho_{\mathrm{A},I}(U_\mathrm{A}^\dagger\otimes U_\mathrm{B}^\dagger)\widehat{J}\,. \tag{9.67}$$

We can find the players' expected payoffs from

$$P_N^{j_1,j_2} = \sum_i \$_N^{j_1(i)j_2(i)}\rho_{ii}\,, \tag{9.68}$$

where $j_1,\,j_2 \in [C,D]$ are classical payoffs of the players. Table 9.4 gives the payoffs of the players corresponding to the unentangled initial state ($\gamma = 0$). Here $\widehat{C} = \widehat{U}_N(0,0)$ or $\widehat{D} = \widehat{U}_N(0,\pi)$.

For $0 < r \le \pi/4$, $\widehat{D}$ is always winning while $\widehat{C}$ is losing for Alice. For $r = \pi/4$ (infinite acceleration) we notice $(\widehat{C},\widehat{C}) = (\widehat{C},\widehat{D}) = (3/2,4)$. That is, if Alice chooses $\widehat{C}$ then the strategy of Bob is irrelevant (*Who wins all the times?*). *Who will be the winner for the strategy* $(\widehat{D},\widehat{C}) = (\widehat{D},\widehat{D}) = (3,3/2)$*? What about Pareto optimal and Nash equilibrium?*

The different situation arises for $\gamma = \pi/2$ (the maximal entangled state). The payoffs for the classical moves are [80]

$$P_{\mathrm{A,B}}^{CC} = 1 + \cos r + \cos^2 r + \frac{5}{4}\sin^2 r \ , \tag{9.69a}$$

$$P_{\mathrm{A,B}}^{DD} = \frac{1}{8}(17 - 8\cos r - \cos 2r) \ , \tag{9.69b}$$

$$P_{\mathrm{A}}^{CD} = P_{\mathrm{B}}^{DC} = \frac{1}{2}\cos\left(\frac{r}{2}\right)(9 + \cos r) \ , \tag{9.69c}$$

$$P_{\mathrm{A}}^{DC} = P_{\mathrm{B}}^{CD} = \frac{1}{2}(9 - \cos r)\sin^2\left(\frac{r}{2}\right) \ . \tag{9.69d}$$

We notice the following:

- $(\widehat{C}, \widehat{C})$ and $\widehat{D}, \widehat{D})$ are equilibrium points.
- The strategy $\widehat{C}$ becomes the dominant and yields in payoffs > 2.83.
- $(\widehat{C}, \widehat{C})$ and $(\widehat{D}, \widehat{D})$ are the Nash equilibrium and the Pareto optimal respectively.
- Playing $\widehat{C}$ is the best option for any player.

Now, analyze the case of players opting quantum strategic space. For the quantum strategy

$$\widehat{Q} = \widehat{U}(0, \pi/2) = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} \tag{9.70}$$

$P_{\mathrm{A,B}}^{Q\theta_{\mathrm{B}}}$ is obtained as

$$P_{\mathrm{A,B}}^{Q\theta_{\mathrm{B}}} = \frac{1}{4}\left\{9 - \cos r\left[(\cos r \mp 5)\cos\theta_{\mathrm{B}} + 2\cos 2\alpha_{\mathrm{B}}(\cos\theta_{\mathrm{B}} + 1) \pm 5\right]\right\} , \tag{9.71}$$

where $\theta_{\mathrm{B}} = 0$ (or π) corresponding to $\widehat{C}$ (or $\widehat{D}$). The following results are evident [80]:

- If Bob opts $\widehat{C}$ then $P_{\mathrm{A}}^{QC} = P_{\mathrm{B}}^{QC}$ is an equilibrium point.
- If Bob chooses $\widehat{D}$ then $P_{\mathrm{B}}^{QD} = P_{\mathrm{A}}^{CD} > P_{\mathrm{B}}^{QC} > P_{\mathrm{A}}^{QD}$. $\widehat{D}$ is the dominant strategy for Bob against Alice's $\widehat{Q}$. The same is result for Alice, if Bob considers $\widehat{Q}$.
- A Pareto optimal is $(\widehat{Q}, \widehat{C})$ or $(\widehat{C}, \widehat{Q})$.
- If Alice and Bob choose $\widehat{Q}$ then $P_{\mathrm{A}}^{QQ} = P_{\mathrm{B}}^{QQ} = P_{\mathrm{A,B}}^{CC}$. This implies that $(\widehat{Q}, \widehat{Q})$ is the Nash equilibrium.

In the case of inertial frame, if one player opts the classical strategy while the other plays the quantum strategy then all the time the quantum player outsmarts the classical player for the so-called miracle move $\widehat{M}$ [58],

$$\begin{aligned}\widehat{M} &= \widehat{U}\left(\frac{\pi}{2},\frac{\pi}{2}\right)\\ &= \frac{\mathrm{i}}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.\end{aligned} \tag{9.72}$$

This is shown to be not the case in noninertial frames. Suppose Bob is in classical region while Alice is with $\widehat{M}$ then

$$P_{\mathrm{A}}^{M\theta_{\mathrm{B}}} = \frac{1}{4}\left[-3\cos^2 r\,\sin\theta_{\mathrm{B}} + \cos r\,(\sin\theta_{\mathrm{B}} - 7) + 9\right], \tag{9.73}$$

$$P_{\mathrm{B}}^{M\theta_{\mathrm{B}}} = \frac{1}{4}\left[7\cos^2 r\,\sin\theta_{\mathrm{B}} + \cos r\,(\sin\theta_{\mathrm{B}} + 3) + 9\right]. \tag{9.74}$$

Now, $P_{\mathrm{A}}^{M\theta_{\mathrm{B}}} < P_{\mathrm{B}}^{M\theta_{\mathrm{B}}}$. The quantum player should never choose the miracle move of the inertial frames. However, $\widehat{M}$ always yields a winning payoff against the quantum move $\widehat{Q}$.

9.5.6 Why are Quantum Games Interesting? What are the Possible Uses of Quantum Games?

There are several reasons for interest on quantum games [58]. Some of them are listed below.

1. Classical game theory has applications in various fields. Because it is based on probabilities, there is a fundamental interest in generalizing the theory to quantum probabilities.

2. Most of the applications of game theory in science have been in biology, in particular the competition and cooperation between species in individual animals. We believe that survival games are played on the molecular level where quantum mechanics is the ruler.

3. Whenever a player conveys his/her decision to the other player he/she communicates information. Thus, there exists a link between game theory and quantum communication.

4. Eavesdropping in quantum communication and quantum cloning can be conceived in a strategic game between two or more players.

5. Quantum mechanics may be useful to certain specially designed games such as PQ penny flip [54] and may assure fairness in remote gambling.

6. Quantum games provide a deeper insight into quantum complexity particularly in the design of quantum algorithms.

9.6 QUANTUM CLONING

Quantum cloning is a process of setting identical quantum mechanical particle(s) from the given same type of single quantum particle. *Is quantum cloning possible theoretically and experimentally?* It has been shown that [43] any transformation that begins with a single particle in an arbitrary state and end up with two particles in the state must violate the governing rules of quantum mechanics. This means that perfect cloning is impossible. This result is known as the *no-cloning theorem* proven by William Wooters and Wojciech Zurek [43].

9.6.1 A Quantum Cloner

To clone an unknown state, $|\psi\rangle$, a device called a *quantum cloner* is needed. Suppose it is prepared initially in a state $|s\rangle$ which does not depend on $|\psi\rangle$. Let $|0\rangle$ be a known state of a particle onto which the information has to be copied and U be the cloning operator. Denote the state of the quantum copies after $|\psi\rangle$ and $|\bar{\psi}\rangle$ have been cloned as $|s'\rangle$ and $|s''\rangle$ respectively.

The cloning process for two initial states $|\psi\rangle$ and $|\bar{\psi}\rangle$ are written as

$$U\left(|\psi\rangle|0\rangle|s\rangle\right) = |\psi\rangle|\psi\rangle|s'\rangle, \tag{9.75}$$

$$U\left(|\bar{\psi}\rangle|0\rangle|s\rangle\right) = |\bar{\psi}\rangle|\bar{\psi}\rangle|s''\rangle. \tag{9.76}$$

Rewriting Eq. (9.76) as

$$\left(\langle s|\langle 0|\langle\bar{\psi}|\right)U^{-1} = \langle s''|\langle\bar{\psi}|\langle\bar{\psi}| \tag{9.77}$$

and multiplication of Eq. (9.75) by Eq. (9.77) give

$$\langle\bar{\psi}|\psi\rangle = \left(\langle\bar{\psi}|\psi\rangle\right)^2\langle s''|s'\rangle. \tag{9.78}$$

Since the magnitudes of $\langle\bar{\psi}|\psi\rangle$ and $\langle s''|s'\rangle$ must be ≤ 1 Eq. (9.78) is satisfied only if

$$|\langle\bar{\psi}|\psi\rangle| = |\langle s''|s'\rangle| = 1. \tag{9.79}$$

Therefore, perfect cloning is possible if $|\psi\rangle$ and $|\bar{\psi}\rangle$ are either orthogonal or identical. Thus, we conclude that ideal cloning device for arbitrary states does not exist. This is the greatest difference between classical and quantum information − classical can be copied perfectly while the quantum cannot be.

The no-cloning theorem implies that eavesdroppers cannot clone each qubit of a transmission successfully in quantum cryptography. Further, it is not possible to prepare a copy (as a backup) of the state of a quantum computer. Even though it is not possible to copy quantum information perfectly, one may wish to know the extent to which splitting of the message in a given qubit is possible. This is crucial because quantum copying is essential in storage and recovery of information in quantum computers.

The no-cloning theorem is manifested in several versions. In terms of CNOT gate we have the relations [83]

$$\begin{aligned}
\mathrm{CNOT}(\sigma_x \otimes I)\mathrm{CNOT} &= \sigma_x \otimes \sigma_x \,, && \text{(9.80a)}\\
\mathrm{CNOT}(I \otimes \sigma_x)\mathrm{CNOT} &= I \otimes \sigma_x \,, && \text{(9.80b)}\\
\mathrm{CNOT}(\sigma_z \otimes I)\mathrm{CNOT} &= \sigma_z \otimes I \,, && \text{(9.80c)}\\
\mathrm{CNOT}(I \otimes \sigma_z)\mathrm{CNOT} &= \sigma_z \otimes \sigma_z. && \text{(9.80d)}
\end{aligned}$$

These imply that the bit flip operation can be copied from first qubit to second qubit and the phase flip operation can be copied backwards. However, they cannot be copied simultaneously.

9.6.2 The Pauli Channel

Let us present the quantum cloning machine called *Pauli channel* [83,84]. Consider an arbitrary quantum pure state $|\psi\rangle = x_0|0\rangle + x_1|1\rangle$, $|x_1|^2 + |x_2|^2 = 1$. A maximally entangled state is given by

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{9.81}$$

The complete quantum state of three particles can be written as

$$\begin{aligned}
|\psi\rangle_{\mathrm{A}}|\psi^+\rangle_{\mathrm{BC}} &= \frac{1}{2}\big[|\psi^+\rangle_{\mathrm{AB}}|\psi\rangle_{\mathrm{C}} \\
&\quad + (I\otimes X)|\psi^+\rangle_{\mathrm{AB}} X|\psi\rangle_{\mathrm{C}} \\
&\quad + (I\otimes Z)|\psi^+\rangle_{\mathrm{AB}} Z|\psi\rangle_{\mathrm{C}} \\
&\quad + (I\otimes XZ)|\psi^+\rangle_{\mathrm{AB}} XZ|\psi\rangle_{\mathrm{C}}\big], \qquad \text{(9.82)}
\end{aligned}$$

where I is the identity, X, Z are Pauli matrices and XZ is another Pauli matrix up to a factor i.

Let $U_{m,n} = X^m Z^n$, $m, n = 0, 1$ be the unitary transformation. We rewrite (9.82) as

$$|\psi\rangle_{\mathrm{A}}|\psi^+\rangle_{\mathrm{BC}} = \frac{1}{2}\sum_{m,n}\left(I \otimes U_{m,-n} \otimes U_{m,n}\right)|\psi^+\rangle_{\mathrm{AB}}|\psi\rangle_{\mathrm{C}} \tag{9.83}$$

and perform the unitary transformation as

$$\begin{aligned}
&\sum_{\alpha,\beta} a_{\alpha,\beta}\left(U_{\alpha,\beta}\otimes U_{\alpha,-\beta}\otimes I\right)|\psi\rangle_{\mathrm{A}}|\psi^+\rangle_{\mathrm{BC}} \\
&\quad = \frac{1}{2}\sum_{\alpha,\beta,m,n}\left(U_{\alpha,\beta}\otimes U_{\alpha,-\beta}U_{m,-n}\otimes U_{m,n}\right)|\psi^+\rangle_{\mathrm{AB}}|\psi\rangle_{\mathrm{C}} \\
&\quad = \sum_{m,n} b_{m,n}\left(I\otimes U_{m,-n}\otimes U_{m,n}\right)|\psi^+\rangle_{\mathrm{AB}}|\psi\rangle_{\mathrm{C}}, \qquad \text{(9.84a)}
\end{aligned}$$

where

$$b_{m,n} = \frac{1}{2}\sum_{\alpha,\beta}(-1)^{\alpha m-\beta m}a_{\alpha,\beta} \tag{9.84b}$$

and

$$\sum_{\alpha,\beta}|a_{\alpha,\beta}|^2 = \sum_{m,n}|b_{m,n}|^2 = 1. \tag{9.84c}$$

This is a quantum cloning machine. The quantum states of A and C are found to be

$$\rho_{\rm A} = \sum_{\alpha,\beta}|a_{\alpha,\beta}|^2 U_{\alpha,\beta}|\psi\rangle\langle\psi|U^{\dagger}_{\alpha,\beta}, \tag{9.85a}$$

$$\rho_{\rm C} = \sum_{m,n}|b_{m,n}|^2 U_{m,n}|\psi\rangle\langle\psi|U^{\dagger}_{m,n}. \tag{9.85b}$$

After cloning $\rho_{\rm A}$ is the original quantum state and $\rho_{\rm C}$ is the copy.

In recent years many quantum cloning machines producing approximate copies of an unknown input have been proposed [83-90]. In a cloning device [89] a pump pulse is split at a beam splitter. The main part of the pump is directed at a nonlinear crystal, and the smaller part is reflected from a mirror and then enters a second crystal. In this second crystal a photon pair is produced. One of these photons serves as a trigger. The other is to be cloned. This photon is directed at the first crystal. It simulates the emission of photons with the same polarization and direction. The emitted photons are the clones. As the cloner requires only a linear and phase-insensitive amplifier (such as a laser amplifier) and various beam splitters it will be possible to construct a cloning device in a laboratory in the future. A lower bound for the noise induced by quantum copying of two arbitrary vectors in a two-dimensional state space has been obtained [91]. A no-cloning theorem of observable and joint measurements of noncommuting observables are elucidated in ref.[92].

Solved Problem 3:

Show that for a d-dimensional system (d is prime) the set of maximally entangled states $\{|\psi_j\rangle\}_{j=0}^{N-1}$ given by $|\psi_j\rangle = (U_j \otimes I)|\Phi^+\rangle$, $U_j = \sum_{j=1}^{N-1}\omega^{jk}|k\rangle\langle k|$ can be locally copied.

To clone the states we defined the generalized CNOT gate as

$$\text{CNOT}: \ |a\rangle|b\langle \rightarrow |a\rangle|b+a\rangle, \tag{9.86}$$

where $|a+b\rangle$ is mod d. Suppose an ancilla (an extra auxiliary bit) state $|\Phi^+\rangle$ is shared between Alice and Bob and both perform the generalized CNOT gate. We get the perfect copies $|\psi_j\rangle^{\otimes 2}$.

We know that

$$\text{CNOT}^\dagger : \ |a\rangle|b\langle \rightarrow |a\rangle|b-a\rangle. \tag{9.87}$$

We have the properties

$$\begin{aligned} |\Phi^+\rangle_{12}|\Phi^+\rangle_{34} &= \text{CNOT}_{13}^\dagger \otimes \text{CNOT}_{24}^\dagger |\Phi^+\rangle_{12}|\Phi^+\rangle_{34} \\ &= \text{CNOT}_{13} \otimes \text{CNOT}_{24} |\Phi^+\rangle_{12}|\Phi^+\rangle_{34}. \end{aligned} \tag{9.88}$$

Then we obtain [93]

$$\begin{aligned} &\text{CNOT}_{13} \otimes \text{CNOT}_{24} |\psi_j\rangle_{12}|\Phi^+\rangle_{34} \\ &\quad = \text{CNOT}_{13} \otimes \text{CNOT}_{24} \left(U_j \otimes I\right)_{13} |\Phi^+\rangle_{12}|\Phi^+\rangle_{34} \\ &\quad = \text{CNOT}_{13} \left(U_j \otimes I\right)_{13} \text{CNOT}_{13}^\dagger |\Phi^+\rangle_{12}|\Phi^+\rangle_{34}. \end{aligned} \tag{9.89}$$

We have the result

$$\text{CNOT} \left(U_j \otimes I\right) \text{CNOT}_{13}^\dagger = U_j \otimes U_j. \tag{9.90}$$

The operator U_j is copied. That is, by the above method $\{|\psi_j\rangle\}_{j=0}^{N-1}$ are locally copied.

9.6.3 Other No-Go Theorems

Apart from no-cloning there are few other impossibilities in quantum information. The impossibility theorems are consequences of linearity and unitarity properties of quantum theory. We briefly point out the various no-go theorems.

1. **No-Broadcast Theorem:** Because quantum states cannot be copied (in general), they cannot be conveyed to two or more recipients. That is, from a given single copy of a quantum state, we cannot create a state with one part of it the same as the original state and the other part also the same as the original state. This is called *no-broadcast theorem* [94,95]. Further, a set of states is broadcastable only if they commute pairwise.

2. **No-Hiding Theorem**: As per the *no-hiding theorem* [96] if information is found to be missing in one system, for example due to the interaction of the system with the environment, then it is residing somewhere else in the universe. This means it is not possible to hide the missing information in the correlations between a system and its environment. This theorem addressing about information loss has been proven experimentally [97] on a 3-qubit nuclear magnetic resonance quantum information

processor. The no-hiding theorem is found to have applications in black hole evaporation [98], quantum teleportation and private quantum channels [99].

3. **No-Deletion Theorem:** A given finite number of copies of an unknown quanta state can be partly estimated [100,101] and teleported. But, similar to cloning, deletion of an unknown state from several copies is also not allowed. This is known as *no-deletion principle* [102]. Note that if cloning and deletion of an unknown state are possible then we can transmit signals faster than light using two pairs of EPR states.

4. **No-Splitting Theorem:** Another impossibility theorem is the no-splitting problem [103]. It has been proven that quantum information of an unknown qubit cannot be split into two complementary qubits in a product state. This implies that the information contained in one qubit is inseparable.

5. **No-Partial Erase Theorem:** According to the *no-erase theorem* it is impossible to erase quantum information partially [104]. Here partial erasure refers to reduction of the dimension of the parameter space for the quantum state representing the quantum information, such as a qubit. Suppose a qubit contains information about, say, azimuthal angle and polar angle: $\Omega\rangle = \cos(\theta/2)|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin(\theta/2)|1\rangle$, with $\Omega = (\theta, \phi)$, $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$. Here the states $|0\rangle$ and $|1\rangle$ are the logical zero and one states. Each pure state can be a point on the Poincaré sphere with θ and ϕ being the polar and azimuthal angles respectively. It is impossible to erase, for example, polar angle information keeping the information about the azimuthal angle. In the above complete erasure would result in mapping of all qubit states into a fixed qubit state $|\Omega_0\rangle = |\Sigma\rangle$ whatever the values of θ and ϕ.

9.7 QUANTUM DIFFUSION

Spreading of a wave packet in a dissipative environment at zero temperature is termed as *quantum diffusion*. This phenomenon is theoretically described by means of models of quantum state diffusion [105], quantum Brownian motion [106], quantum drift-motion [107], etc. It is a fundamental phenomenon associated with the atomic migration in crystalline solids where the quantum mechanical tunneling plays key role.

Consider a quantum particle of mass moving in a vacuum [108]. We write the wave function in the polar form as $\psi(r,t) = \sqrt{\rho}\mathrm{e}^{\mathrm{i}S(r,t)/\hbar}$ where $\rho(r,t)$ is the probability density to find the quantum particle at a point r at time t and S is the phase of the wave function. Substituting ψ in the Schrödinger equation

$$\mathrm{i}\hbar\frac{\partial\psi}{\partial t} = -\frac{\hbar^2}{2m}\nabla^2\psi + U\psi \tag{9.91}$$

and equating the real and imaginary parts separately to zero we obtain

$$m\frac{\partial V}{\partial t} + mV\cdot\nabla V = -\nabla U - \nabla\cdot P_{\rm Q}/\rho\,, \tag{9.92a}$$

$$\frac{\partial \rho t}{\partial t} + \nabla\cdot(\rho V) = 0\,, \tag{9.92b}$$

where the velocity $V = \nabla S/m$ represents the flow in the probability space and $P_{\rm Q} = -(\hbar^2/4m)\rho\nabla\otimes\nabla\ln\rho$ is the quantum pressure tensor [108]. When the quantum particle moves in a dissipative medium it will experience a friction force, say, proportional to velocity of the particle. In this case, Eq. (9.92a) becomes

$$m\frac{\partial V}{\partial t} + mV\cdot\nabla V + dV = -\nabla(U+Q)\,, \tag{9.93}$$

where d is the friction constant and

$$Q = -\hbar^2\nabla^2\rho/2m\sqrt{\rho}\,. \tag{9.94}$$

Thus, Eq. (9.92b) describes the probability spreading in a dissipative environment, that is, quantum diffusion.

9.7.1 Free Particle

For a free particle of unit mass the Gaussian wave packet is given by

$$\psi = \left(\frac{1}{\sqrt{2\pi}\,\sigma}\right)^{3/2} {\rm e}^{-r^2/4\sigma^2}\,, \tag{9.95}$$

where $\sigma^2(t)$ is the dispersion of the wave packet. For the ψ given by Eq. (9.95) from (9.92b) we obtain $V = r\dfrac{\rm d}{{\rm d}t}\ln\sigma$. Then Eq. (9.92a) gives

$$\frac{{\rm d}^2\sigma}{{\rm d}t^2} + d\frac{{\rm d}\sigma}{{\rm d}t} = \frac{\hbar^2}{4\sigma^3}\,. \tag{9.96}$$

The above equation describes the evolution of σ. Introducing the change of variables $\xi^2 = 2d\sigma^2/\hbar$ and $\tau = dt$ Eq. (9.96) becomes

$$\xi'' + \xi' - \frac{1}{\xi^3} = 0\,, \quad {}' = \frac{\rm d}{{\rm d}\tau}\,. \tag{9.97}$$

Appropriate initial condition for (9.97) is $\xi(\tau=0) = \xi_0 = \sqrt{2d/\hbar}$ and $\xi'(\tau = 0) = \xi_0' = 0$. For $\tau \gg 1$, one can approximate Eq. (9.97) as $\xi' = 1/\xi^3$. Its solution is $\xi^4 = \xi_0^4 + 4\tau$ giving $\sigma^2 = \sqrt{\sigma_0^4 + \hbar^2 t/d}$. For large τ, $\sigma^2 = \hbar\sqrt{t/d}$, a subdiffusive law. Figure 9.4 shows the plot of ξ^2 and ${\rm d}\xi^2/{\rm d}\tau$ obtained by numerically solving Eq. (9.97) with $\xi_0^2 = 0.1$ and $\xi_0' = 0$. The dispersion increases with time and then for large time it increases according to $\xi^2 = 2\sqrt{\tau}$.

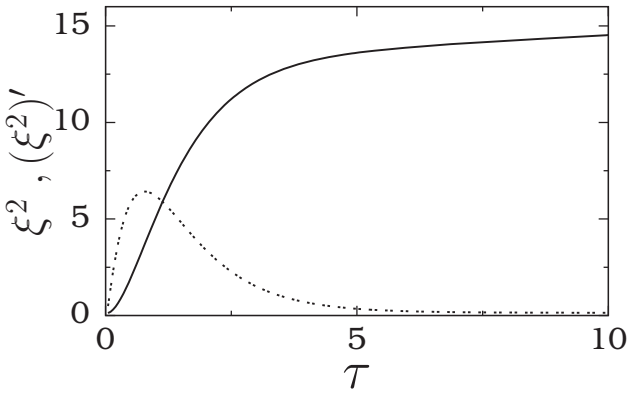


FIGURE 9.4 Variation of dispersion ξ^2 (solid curve) and its rate of change (dashed curve) with time τ where $\xi_0 = \sqrt{0.1}$ and $\xi_0' = 0$.

The maximum of $\mathrm{d}\xi^2/\mathrm{d}\tau$ is called *quantum diffusion constant* because for $\mathrm{d}^2\xi^2/\mathrm{d}\tau^2$, ξ^2 increases linearly with τ.

Numerically computed quantum diffusion constant is found to decrease with an increase in the initial dispersion ξ_0^2. The quantum diffusion constant is obtained as [108]

$$D_{\mathrm{Q}} = \frac{1}{2}\left(\frac{\partial}{\partial t}\sigma^2\right)_{\max} = \frac{\hbar^2}{16md\sigma_0^2}\,. \tag{9.98}$$

We note that the classical Einstein diffusion constant is $D = k_{\mathrm{B}}T/d$. The point is that D_{Q} is not a universal constant and depends on the initial wave packet. This result explains the large spread of quantum surface diffusion coefficient measured at low temperatures [109].

9.7.2 Linear Harmonic Oscillator

For the Guassian wave packet of linear harmonic oscillator with the potential $U = m\omega^2 r^2/2$ we have [110-112]

$$\xi'' + \xi' + \alpha^2\xi = \frac{1}{\xi^3}\,, \quad \alpha = m\omega/d\,. \tag{9.99}$$

Figure 9.5 depicts the dispersion ξ^2 versus time τ. In the limit $\tau \to \infty$, $\xi^2 \to 1$. Due to the friction force the energy drops to the ground state level.

For a discussion on quantum diffusion in a periodic potential system one may refer to ref.[108]. A general theory of quantum diffusion is developed to describe diffusion dynamics in biased semiconductors and semiconductor superlattices [113]. The mechanism responsible for quantum diffusion in the quasiperiodic kicked rotor is studied by Lignier et al.[114]. They reported experimental results on the diffusion constant on the atomic version of the system and proposed a theoretical approach to account for the observed results.

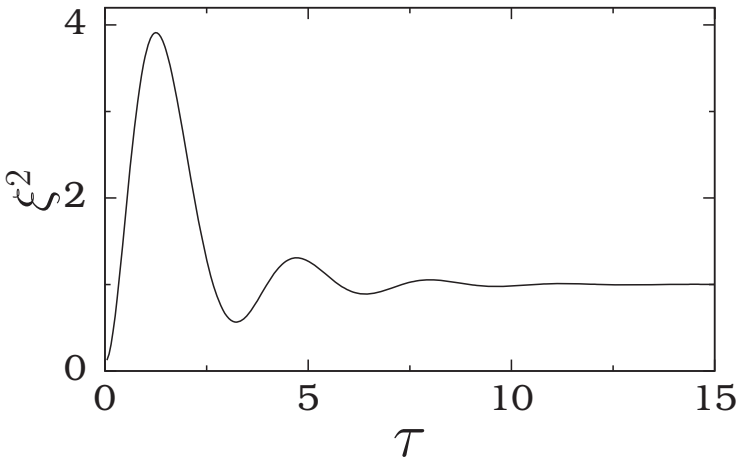


FIGURE 9.5 Variation of dispersion ξ^2 with time τ where $\xi_0 = \sqrt{0.1}$ and $\xi_0' = 0$ and $\alpha = 1$.

Anomalous diffusions of wave packets in quasiperiodic systems has received a considerable interest [115]. Quantum diffusion in the generalized Harper equation is reported in ref.[116]. Transport property of diffusion in a finite translationaly invariant quantum subsystem is analyzed [117].

9.8 QUANTUM CHAOS

In classical physics, dynamical systems are broadly classified into two classes: linear and nonlinear. When the force acting on a system is directly proportional to displacement then it is said to be a *linear force* otherwise a *nonlinear force*. The systems driven by linear forces are termed as *linear systems*. The force acting on a linear harmonic oscillator is $F = -kx \propto x$ and is thus a linear system. For an anharmonic oscillator and the pendulum system the force is essentially nonlinear. Linear systems are described by linear differential equations while the nonlinear systems are described by nonlinear differential equations. *How do we define nonlinear differential equations?* In a differential equation if each of the terms, after rationalization, has a total degree either 1 or 0 in the dependent variables and their derivatives then it is a linear differential equation. Even if one of the terms has a degree different from 0 or 1 in the dependent variables (and their derivatives) then it is *nonlinear*. The presence of independent variables does not affect the linearity and nonlinearity nature. The classical equation of motion of linear harmonic oscillator is linear while those of an anharmonic oscillator and the pendulum system are nonlinear. The Schrödinger equation is linear.

Linear systems display smooth and regular behavior. In contrast, certain nonlinear systems are capable of exhibiting smooth and regular as well as complicated irregular behavior depending upon the various factors. A type of

irregular dynamics exhibited by nonlinear systems with phase space dimension greater than two is the *chaotic motion*. It is a nonperiodic and bounded motion with high sensitive dependence on initial conditions. In a chaotic system two trajectories starting from two nearby initial conditions diverge exponentially until they become completely uncorrelated so that the future state becomes unpredictable. For a detailed discussion on classical chaos one may refer to refs.[118-120]. For microscopic systems one may ask: *What are the features of a quantum system whose classical counterpart exhibits chaotic motion?* In other words, *what are the quantum manifestations of classical chaos?*

It has been argued that anything that erratically 'wiggles' and 'jiggles' in quantum mechanics should be termed as *quantum chaos*. Berry defined quantum chaos as the study of semiclassical, but nonclassical, behavior characteristic of systems whose classical motion exhibits chaos [121]. The problem of characterizing chaos in quantum mechanics naturally divides into two classes [122]:

1. Static properties (eigenvalues and eigenfunctions) and
2. Dynamical properties (time evolution of localized initial states and observables).

For bounded quantum systems the energy eigenvalue spectrum is discrete. Consequently, the dependence of the stationary state wave function on time is always almost periodic. Therefore, stationary state wave function cannot display sensitive dependence on initial conditions. Because the wave function itself is well behaved, it is hard to imagine the sensitivity in the expectation values of observables [123]. On the other hand, for nonstationary problems, for example, for periodic time-dependent Hamiltonians, the existence of the time evolution operator and the Floquet's theorems assert that the wave function to be quasiperiodic and thus sensitivity to initial state is precluded [123]. Therefore, we are compelled to look at the signatures of chaos in the eigenvalues and eigenvectors.

9.8.1 Signatures of Quantum Chaos

From many calculations it has been realized that a very fruitful approach to characterize quantum chaos is the analysis of statistical properties of energy level sequences. Specifically, the distribution ($P(s)$) of energy level spacing is the most significant characteristic of quantum chaos. The Hermitian matrix representation of a Hamiltonian can be parametrized in terms of its energies and the associated states. One can go from probability distribution over matrix elements to a distribution over energies in Hilbert space. Assume that the energy eigenvalues E_i are arranged in increasing order. Then the level spacing between the successive energy levels E_i and E_{i+1} is $E_{i+1} - E_i$. We can find the level spacing distribution $P(s)$ over a set of random Hermitian matrices.

For classically integrable systems it has been proven that in the semiclassical limit, successive energy levels arrive randomly, resulting in a Poisson

distribution for $P(s)$. For general irregular systems (that is, nonintegrable) it has been conjectured [124] that spectral fluctuations are reproduced by appropriate random matrix ensembles like Gaussian orthogonal ensemble (GOE), Gaussian unitary ensemble (GUE) and Gaussian symplectic ensemble (GSE) depending upon the underlying time-reversal symmetry and nature of the spin of the system involved. The remarkable result is that in the case of systems with many symmetries, $P(s)$ reaches a maximum when s approaches zero and it becomes a minimum for the case of few symmetries. That is, quantized regular systems display *level clustering* while quantized chaotic systems show *level repulsion*. Consider the Hamiltonian of the form $H = H_0 + \lambda V$ where λ is the strength of the perturbation. As λ varies, the energy levels change but cannot cross each other unless there is a symmetry in the Hamiltonian. That is, due to lack of symmetries of chaotic systems, energy levels avoid approaching at a short distance from one another.

For a classically integrable system, due to the presence of many symmetries, one can write the Hamiltonian in a block-diagonal form with one block per invariant subspace. This is because two states $|i\rangle$ and $|j\rangle$ cannot have finite matrix elements $\langle i|H|j\rangle$ if H satisfies certain symmetries. These blocks are statistically independent. The point is that within a block, the energy levels are correlated. Levels belonging to different blocks cannot be identified in the spectrum of the entire Hamiltonian. As a result, the energy spacing distribution becomes a Poissonian, a characteristic of uncorrelated random variable.

For intermediate systems the phase space of a classical system consists of infinitely many distinct regions filled with regular or irregular orbits. Assuming that the quantum spectrum is generated by statistically independent superposition of Poisson and Wigner distributions, Berry and Robnik [125] found semiclassical formula for $P(s)$ that interpolates between the two limiting distributions. For a time-dependent periodic Hamiltonians, a continuous transition between Poisson to circular orthogonal ensemble statistics is observed when the corresponding classical system changes from regular to chaotic behavior [126-128]. As far as eigenfunctions are concerned, for integrable systems, regular nodal patterns and strongly correlated wave functions are noticed. In contrast to this, for nonintegrable systems irregular nodal pattern and negligible correlation between wave functions have been found [129].

9.8.2 Random Matrix Theory and Level Statistics

When the classical system is chaotic (nonintegrable) then its corresponding quantum version follows the so-called random matrix theory results. Therefore, we point out the salient features and some important results of random matrix theory relevant for the study of quantum chaos. We mainly follow the ref.[130]. In nuclear physics often finding an appropriate Hamiltonian is very difficult. Wigner suggested to study ensembles of Hamiltonians. The ensembles are usually defined in a matrix space where all the Hamiltonian members

of the ensemble have the same symmetry properties like translational and rotational invariance or time reversal or nontime reversal invariance. For the eigenvalues of these ensemble of matrices we can analyze (i) nearest neighbor spacing distribution (NNSD) and (ii) Δ_3-statistics. NNSD is the probability $P(s)$ for finding a separation s of neighboring levels in the eigenvalue spectrum. For a given subsequence $[\alpha, \alpha + L]$ of the spectrum, $\Delta_3(\alpha, L)$ measures the least-squares deviation of the spectral staircase function from the best straight-line fitting it [131]:

$$\Delta_3(\alpha, L) = \frac{1}{L}\min \int_0^{\alpha+L} [N(\epsilon) - A(\epsilon) - B]^2 \, \mathrm{d}\epsilon \, . \tag{9.100}$$

When the energy eigenvalues ϵ_i are discrete then

$$\begin{aligned} \Delta_3(\alpha, L) \quad = \quad & \frac{n^2}{16} - \frac{1}{L^2}\left[\sum_{i=1}^{n} \hat{\epsilon}_i\right]^2 + \frac{3n}{L^2}\left[\sum_{i=1}^{n} \hat{\epsilon}_i^2\right]^2 \\ & - \frac{3}{L^4}\left[\sum_{i=1}^{n} \hat{\epsilon}_i^2\right]^2 + \frac{1}{L}\left[\sum_{i=1}^{n} (n + 1 - 2i)\hat{\epsilon}_i\right] \end{aligned} \tag{9.101}$$

where $\hat{\epsilon}_i = \epsilon_i - (\alpha + \dfrac{L}{2})$. The NNSD and Δ_3-statistics are known analytically for certain special types of random matrices [132,133]. Some of them are given below.

9.8.2.1 Gaussian Orthogonal Ensemble (GOE)

GOE consists of real symmetric matrices with their elements obeying Gaussian distribution. Classically, chaotic spinless or integral spin systems with time reversal symmetry systems follow the GOE statistics. For GOE [131,134]

$$P(s) \approx \frac{\pi}{2} s \mathrm{e}^{-\pi s^2/4} \tag{9.102}$$

and

$$\Delta_3(L) = \begin{cases} \dfrac{L}{15} \ \text{ for } \ L \ll 1 \\ \\ \ln\left(\dfrac{L}{\pi^2}\right) - 0.00695 \ \text{ for } \ L \gg 1. \end{cases} \tag{9.103}$$

9.8.2.2 Gaussian Unitary Ensemble (GUE)

GUE consists of complex Hermitian matrices whose elements are Gaussian distributed in order to make the statistics of the ensemble invariant under unitary transformations. Usually, GUE is displayed by classically chaotic systems without time reversal symmetry. For GUE [131,134]

$$P(s) \approx \frac{32 s^2}{\pi^2} \mathrm{e}^{-4s^2/\pi} \tag{9.104}$$

and

$$\Delta_3(L) \approx \begin{cases} \dfrac{L}{15} \text{ for } L \ll 1 \\ \\ \ln\left(\dfrac{L}{2\pi^2}\right) + 0.05902 \text{ for } L \gg 1. \end{cases} \tag{9.105}$$

9.8.2.3 Gaussian Symplectic Ensemble (GUE)

GSE consists of quaternion real Hermitian matrices with Gaussian distributed elements which make the ensemble invariant under symplectic transformations. Usually, classically chaotic systems with half-integer spin and with time reversal symmetry follows GSE statistics. For GSE [131,134]

$$P(s) \approx \frac{2^{18}s^4}{3^6\pi^3}\mathrm{e}^{-64s^2/(9\pi)} \tag{9.106}$$

and

$$\Delta_3(L) \approx \begin{cases} \dfrac{L}{15} \text{ for } L \ll 1 \\ \\ \ln\left(\dfrac{L}{4\pi^2}\right) + 0.07832 \text{ for } L \gg 1. \end{cases} \tag{9.107}$$

In addition to the above mentioned random matrix universality classes there are few other universality classes useful for the study of quantum chaos. Some of them are the following.

9.8.2.4 Poisson Statistics

For a classical system exhibiting regular and integrable dynamics the short range properties, such as NNSD, of the corresponding energy level spectrum of the quantum mechanical system tend to resemble that of Poisson spectrum. This is because the integrable or near integrable properties translate into a number of independent conserved operator quantities and each energy level can be characterized by the associated quantum numbers. Superposing terms arising from independent contributions from the various quantum numbers generate a spectrum that closely resembles a spectrum of random numbers. The NNSD for Poisson spectrum is [121] $P(s) = \mathrm{e}^{-s}$ while $\Delta_3(L) = L/15$. Note that Poisson statistics are identified with clustering of levels so that there is a large probability for small spacing while random matrix ensemble statistics are associated with level repulsion.

9.8.2.5 Intermediate Statistics

Many of the classical conservative systems are neither purely regular nor purely chaotic, but show mixed behavior. For the corresponding quantum

mechanics systems the spectral statistics will interpolate between those of the Poisson and the appropriate random matrix universality classes. In this case

$$P(s) = (1+q)\alpha s^q \mathrm{e}^{-\alpha s^{q+1}} \ , \tag{9.108a}$$

where

$$\alpha = \Gamma\left[\left(\frac{q+2}{q+1}\right)^{q+1}\right] \tag{9.108b}$$

and q represents the chaotic fraction of the classical phase space volume. The above distribution is known as a *Brody distribution*. It become Poisson distribution for $q = 0$ and GOE for $q = 1$. Generally, near-integrable systems show this kind of statistic.

9.8.3 Hydrogen Atom in a Generalized van der Waals Potential

In the following we discuss the features of quantum chaos in the hydrogen atom in a generalized van der Waals potential [130,135]. The Hamiltonian of this system is

$$H = \frac{1}{2}\mathbf{p}^2 - \frac{1}{r} + \gamma\left[r^2 + \left(\beta^2 - 1\right)z^2\right] \ , \tag{9.109}$$

where γ and β have different meanings under different physical situations. For example, $\gamma = B/(2.35 \times 10^5\mathrm{T})$ (the magnetic field parameter) and $\beta = 0$ correspond to the quadratic Zeeman effect problem and $\gamma = -1/(16d^3)$ where d represents the distance from the atom to a metal surface and $\beta = \sqrt{2}$, the system corresponds to the instantaneous van der Waals interaction existing between the atom and nearby metal surface. Further, the Hamiltonian (9.109) has a very close analogy with the Paul-trap Hamiltonian realized in precision atomic spectroscopy for ion confinement.

The time-independent Schrödinger equation of the problem is

$$\left\{\frac{1}{2}r\mathbf{P}^2 - 1 + \gamma r\left[r^2 + \left(\beta^2 - 1\right)z^2\right] - rE\right\}\psi = 0 \ , \tag{9.110}$$

where $\mathbf{P} = -\mathrm{i}\nabla$. For convenience introduce a scaling parameter b so that (9.110) becomes

$$\left\{\frac{1}{2b}r\mathbf{P}^2 - 1 + \gamma b^3 r\left[r^2 + \left(\beta^2 - 1\right)z^2\right] - Ebr\right\}\psi = 0 \ . \tag{9.111}$$

It is possible to solve the eigenvalue Eq. (9.111) in many ways. A useful scheme is the Crawford algorithm [136]. Ganesan and Lakshmanan [130,135] investigated the quantum manifestation of chaos in the system with the Hamiltonian (9.109). They noticed that in the classical system as the parameter β increases for arbitrary γ, there is a remarkable

$$\textit{chaos} \to \textit{order} \to \textit{chaos} \to \textit{order} \to \textit{chaos} \to \textit{order} \to \textit{chaos} \tag{9.112}$$

TABLE 9.5 Comparison of classical and quantum results of Hamiltonian (9.109). (Reproduced with permission from K. Ganesan and M. Lakshmanan, *Phys. Rev. A* 48:964, 1993. Copyright 1993, American Physical Society.)

β	Classical results	Quantum results
1/4	Completely chaotic (nonintegrable)	GOE statistics
1/2	Integrable	Poisson statistics
$\sqrt{0.4}$	Small-scale chaos (near-integrable)	Intermediate statistics
1	Integrable	Poisson statistics
1.5	Small-scale chaos (near-integrable)	Intermediate statistics
2	Integrable	Poisson statistics
3	Completely chaotic (nonintegrable)	GOE statistics

type of transition. Further, the system is found to be exactly integrable at $\beta = 1/2$, 1 and 2. In the quantum case as the parameter increases the level statistics has shown

$$GOE \rightarrow Poisson \rightarrow Brody \rightarrow Poisson \rightarrow Brody \rightarrow Poisson \rightarrow GOE \tag{9.113}$$

type of transitions [130,135]. Table 9.5 summarizes classical and quantum results [135].

9.9 CONCLUDING REMARKS

Advanced research topics in quantum mechanics arise on the fundamental levels, quantum analogue of newly observed classical phenomena, application of quantum theoretical treatment and ideas to other branches of science and on the technological side. Deeper study of basic quantum mechanical systems leads to the concepts like quantum revivals [137,138] and quantum carpets [139-141]. Certain classical nonlinear systems display novel phenomena such as stochastic resonance [142], vibrational resonance [143], auto-resonance [144,145], ghost resonance [146,147], synchronization [148], amplitude death [149] to mention a few. Quantum version of stochastic resonance is realized in certain quantum systems [150,151]. The quantum analogue of other nonlinear dynamics has to be explored.

Until recently, biology and quantum mechanics were thought of as independent branches of science. Interestingly experimental data have opened the possible realization of quantum superposition, quantum entanglement and quantum coherence during certain biological processes and systems [152-154]. It has been proposed that the so-called Fenna–Mathews–Olson (FMO)

pigment protein complex executes a kind of quantum search algorithm which is seen to be considerably more efficient than a classical random hopping mechanism [152].

Quantum mechanical description is needed for describing cellular biochemical reactions, energy metabolism in eukaryotes interaction of light and biological photo-receptors, etc. These opened a new branch called quantum biophysics or quantum biology.

Quantum technology is occuping certain technologies such as image processing, metrology and lithography. In the next concluding chapter we bring out the underlying basics and the developments in them.

9.10 BIBLIOGRAPHY

[1] L. Smolin, *Physics World*, December 1999 pp.79.

[2] C. Sivaram, *Current Science* 79:413, 2000.

[3] K. Eppley and E. Hannah, *Found. Phys.* 7:51, 1977.

[4] J.H. Schwarz, *Current Science* 81:1547, 2001.

[5] A. Sen, *Current Science* 81:1561, 2001.

[6] I. Antoniads, *Current Science* 81:1609, 2001.

[7] R.P. Woodard, *Rep. Prog. Phys.* 72:122501, 2009.

[8] C. Rovelli, *Quantum Gravity.* Cambridge Monographs on Mathematical Physics, Cambridge, 2004.

[9] B. Misra and E.C.G. Sudarshan, *J. Math. Phys.* 18:756, 1977.

[10] A.M. Wolsky, *Found. Phys.* 6:367, 1976.

[11] K. Machida, H. Nakazato, S. Pascazio, H. Rauch and S. Yu, *Phys. Rev. A* 60:3448, 1999.

[12] R.J. Cook, *Phys. Scr.* 21:49, 1988.

[13] H. Nakazato, M. Namiki, S. Pascazio and H. Rauch, *Phys. Lett. A* 217:203, 1996.

[14] W.H. Itano, D.J. Heinzen, J.J. Bollinger and D.J. Wineland, *Phys. Rev. A* 41:2295, 1990.

[15] Y. Aharonov and M. Vardi, *Phys. Rev. D* 21:2235, 1980.

[16] R.A. Harris and L. Stodolsky, *J. Chem. Phys.* 74:2145, 1981.

[17] M. Bixon, *Chem. Phys.* 70:199, 1982.

[18] D. Bar, *Physica A* 280:374, 2000.

[19] D. Bar, *Physica A* 267:434, 1999.

[20] P. Facchi, H. Nakazato, S. Pascazio, J. Perina and J. Rehacek, *Phys. Lett. A* 279:117, 2001.

[21] K. Thun, J. Perina and J. Krepelka, *Phys. Lett. A* 299:19, 2002.

[22] B. Militello, A. Messina and A. Napoli, *Phys. Lett. A* 286:369, 2001.

[23] C. Balzer, R. Huesmann, N. Neuhauser and P.E. Toschek, *Opt. Commun.* 180:115, 2000.

[24] C. Balzer, R. Huesmann, N. Neuhauser and P.E. Toschek, *Opt. Commun.* 211:1235, 2002.

[25] K. Molhave and M. Drewsen, *Phys. Lett. A* 268:45, 2000.

[26] M.C. Fisher, B.G. Medlna and M.G. Ralzen, *Phys. Rev. Lett.* 87:040402, 2001

[27] G. Bernardini, L. Maiani and M. Testa, *Phys. Rev. Lett.* 71:2687, 1993.

[28] P. Facchi and S. Pascazio, *Phys. Lett. A* 241:139, 1998.

[29] P. Facchi and S. Pascazio, *Phys. Rev. A* 62:023804, 2000.

[30] P. Facchi, H. Nakazato and S. Pascazio, *Phys. Rev. Lett.* 86:2699, 2001.

[31] S.M. Roy, *Pramana J. Phys.* 56:169, 2001.

[32] A.P. Balachandran and S.M. Roy, *Phys. Rev. Lett.* 84:4019, 2000.

[33] S.K. Sekatsii, *Phys. Lett. A* 317:1, 2003.

[34] P. Facchi, Z. Hradil, G. Krenn, S. Pascazio and J. Rehacek, *Phys. Rev. A* 66:012110, 2002.

[35] A. Luis, *J. Opt. B.* 3:238, 2001.

[36] A.D. Panov, *Annals Phys.* 249:1, 1996.

[37] M. Kitano, *Opt. Commun.* 141:39, 1997.

[38] K. Yamane, M. Ito and M. Kitano, *Opt. Commun.* 192:299, 2001.

[39] P. Facchi, S. Graffi and M. Ligabo, *J. Phys. A: Math. Theor.* 43:032001, 2010.

[40] P. Facchi and S. Pascazio, *J. Phys. A: Math. Theor.* 41:493001, 2008.

[41] O.Y. Aharonov and D.Z. Albert, *Phys. Rev. D* 24:359, 1981.

[42] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K. Wooters, *Phys. Rev. Lett.* 70:1895, 1993.

[43] W.K. Wooters and W.H. Zurek, *Nature* 299:802, 1992.

[44] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, *Nature* 390:575, 1997.

[45] A. Furasawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble and E.S. Polzik, *Science* 282:706, 1998.

[46] S.L. Braunstein and H.J. Kimble, *Phys. Rev. Lett.* 80:869, 1998.

[47] D. Boschi, S. Branca, F. de Martini, L. Hardy and S. Popescu, *Phys. Rev. Lett.* 80:1121, 1998.

[48] L. Vaidman, *Phys. Rev. A* 49:1473, 1994.

[49] T. Sudbery, *Nature* 390:551, 1997.

[50] K.C. Binmore, *Fun and Games: A Text on Game Theory.* Heath, Lexington, 1992.

[51] K. Sigmund, *Games of Life: Explorations in Ecology, Evolution and Behaviour.* Penguin, London, 1995.

[52] E. Rasmusen, *Games and Information.* Blackwell, Oxford, 1995.

[53] R.B. Myerson, *Game Theory: An Analysis of Conflict.* MIT Press, Cambridge, 1991.

[54] D. Meyer, *Phys. Rev. Lett.* 82:1052, 1999.

[55] A.P. Flitney and D. Abbott, *Fluct. Noise Lett.* 02:R175, 2002.

[56] J. Sladkowski, *Physica A* 324:234, 2003.

[57] J. Ng and D. Abbott in Annals of the International Society on Dynamic Games. A. Nowac (Ed.) Birkhauser, Boston, 2003.

[58] J. Eisert, M. Wilkens and M. Lewenstein, *Phys. Rev. Lett.* 83:3077, 1999; 87:069802, 2001.

[59] S.C. Benjamin and P.M. Hayden, *Phys. Rev. Lett.* 87:069801, 2001.

[60] H. Li, X. Xu, M. Shi, J. Wu, X. Zhou and R. Han, *Phys. Rev. Lett.* 88:137902, 2002.

[61] A. Iqbal and A.H. Tour, *Phys. Lett. A* 280:249, 2001.

[62] C.F. Lee, N.F. Johnson, *Physics World* October, 2002 pp.25.

[63] C.F. Li, Y.S. Zhang, Y.F. Huang and G.C. Guo, *Phys. Lett. A* 280:257, 2001.

[64] A.P. Flitney and D. Abbott, *Phys. Rev. A* 65:062318, 2002.

[65] L. Marinatto and T. Weber, *Phys. Lett. A* 272:291, 2000; 277:183, 2000.

[66] J. Du, X. Xu, H. Li, X. Zhou and R. Han, quant-ph/0010050.

[67] A. Iqbal and A.H. Toor, *Phys. Rev. A* 65:022036, 2002.

[68] N.F. Johnson, *Phys. Rev. A* 63:020302, 2001.

[69] S.C. Benjamin and P.M. Hayden, *Phys. Rev. A* 64:030301, 2001.

[70] A. Iqbal and A.H. Tour, *Phys. Rev. A* 65:052328, 2002; *Phys. Lett. A* 286:245, 2001; 294:261, 2002.

[71] G.P. Harmer, D. Abbott, P.G. Taylor and J.M.R. Parrondo in Proceedings of the Second International Conference on *Unsolved Problems of Noise and Fluctuations*. Adelaide, Australia, 511:189, 1999.

[72] P.V.E. McClintock, *Nature* 401:23, 1999.

[73] J.M.R. Parrondo, G.P. Harmer and D. Abbott, *Phys. Rev. Lett.* 85:5226, 2000.

[74] G.P. Harmer and D. Abbott, *Nature* 402:864, 1999.

[75] S.B. Ekhad and D. Zeilberger, Remarks on the Parrondo's Paradox, preprint.

[76] G.P. Harmer, D. Abbott, P.G. Taylor and J.M.R. Parrondo, *Chaos* 11:705, 2001.

[77] A.P. Flitney, J. Ng and D. Abbott, *Physica A* 314:35, 2002.

[78] A.P. Flitney and D. Abbott, *Physica A* 324:152, 2003.

[79] J.F. Du, J.H. Wu, M.J. Shi, L. Han, X.Y. Zhou, B.J. Ye, H.M. Weng and R.D. Han, *Chin. Phys. Lett.* 17:64, 2000.

[80] S. Khan and M. Khalid Khan, *J. Phys. A: Math. Theor.* 44:355302, 2011.

[81] Q. Pan and J. Jing, *Phys. Rev. A* 77:024302, 2008.

[82] P.M. Alsing, I. Fuentes-Schuller, R.B. Mann and T.E. Tessier, *Phys. Rev. A* 74:032326, 2006.

[83] H. Fan, Y.N. Wang, L. Jing, J.D. Yue, H.D. Shi, Y.L. Zhang and L.Z. Mu, arXiv:1301.2956v3, 2003.

[84] N.J. Cerf, *Phys. Rev. Lett.* 84:4497, 2000.

[85] V. Buzek and H.M. Hillery, *Phys. Rev. A* 54:1844, 1996; *Physics World* November 2001 pp.25.

[86] F. De Martini, V. Mussi and F. Bovino, *Opt. Commun.* 179:581, 2000.

[87] N. Gisin and S. Massar, *Phys. Rev. Lett.* 79:2153, 1997.

[88] Y.F. Huang, W.L. Li, C.F. Li, Y.S. Zhang, Y.K. Jiang and G.C. Guo, *Phys. Rev. A* 64:012315, 2001.

[89] C. Simon, G. Weihs and A. Zeilinger, *Phys. Rev. Lett.* 84:2993, 2000.

[90] R.F. Werner, *Phys. Rev. A* 58:1827, 1998.

[91] M. Hillery and V. Buzek, *Phys. Rev. A* 56:1212, 1997.

[92] A. Ferraro, M. Galbiati and M.G.A. Paris, *J. Phys. A: Math. Theor.* 39:L129, 2006.

[93] H. Fan, Y.N. Wang, L. Jing, J.D. Yue, H.D. Shi, Y.L. Zhang and L.Z. Mu, arXiv:1301.2956v3, 2003.

[94] H. Barnum, C.M. Caves, C.A.Fuchs, R. Jozsa and B. Schumacher, *Phys. Rev. Lett.* 76:2818, 1996.

[95] H. Barnum, J. Barrett, M. Leicer and A. Wilce, *Phys. Rev. Lett.* 99:240501, 2007.

[96] S.L. Braunstein and A.K. Pati, *Phys. Rev. Lett.* 98:080502, 2007.

[97] J.R. Samal, A.K. Pati and A. Kumar, *Phys. Rev. Lett.* 106:080401, 2011.

[98] S.W. Hawking, *Nature* 248:30, 1974.

[99] M. Mosca, A. Tapp, R. Wolf, arXiv:quant-ph/0003101.

[100] S. Massar and S. Popescu, *Phys. Rev. Lett.* 74:1259, 1995.

[101] R. Derka, V. Buzek and A. Ekert, *Phys. Rev. Lett.* 80:1571, 1998.

[102] A.K. Pati and S.L. Braunstein, *Nature* 404:164, 2000.

[103] D.L. Zhou, B. Zheng and L. You, *Phys. Lett. A* 352:41, 2006.

[104] A.K. Pati and B.C. Sanders, *Phys. Lett. A* 359:31, 2006.

[105] I.C. Percival, *Quantum State Diffusion.* Cambridge University Press, Cambridge, 1998.

[106] J. Ankerhold, *Quantum Tunneling in Complex Systems.* Springer, Berlin, 2007.

[107] A. Jungel, *Transport Equations for Semiconductors.* Springer, Berlin, 2009.

[108] R. Tsekov, *Phys. Scr.* 83:035004, 2011.

[109] D. Drakova and G. Doyen, *J. Surf. Sci. Nanotechnol.* 8:6, 2010.

[110] H. Dekker, *Phys. Rep.* 80:1, 1981.

[111] R. Tsekov and G.N. Vayssilov, *Chem. Phys. Lett.* 195:423, 1992.

[112] A.B. Nassar, J.M.F. Bassalo, P.T.S. Alencar, L.S.G. Cancela and M. Cattani, *Phys. Rev. E* 56:1230, 1997.

[113] V.V. Bryksin and P. Kleinert, *J. Phys. Condens. Matter* 15:1415, 2003.

[114] H. Lignier, J.C. Garreau, P. Szriftgiser and D. Delande, *Europhys. Lett.* 69:327, 2005.

[115] H.Q. Yuan, U. Grimm, P. Repetowicz and M. Schreiber, *Phys. Rev. B* 62:15569, 2000 and references therein.

[116] G.S. Jeon, B.J. Kim, S.W. Yi and M.Y. Choi, *J. Phys. A: Math. Gen.* 31:1353, 1998.

[117] M. Esposito and P. Gaspard, *J. Stat. Phys.* 121:463, 2005.

[118] M. Lakshmanan and S. Rajasekar, *Nonlinear Dynamics: Integrability, Chaos and Pattern.* Springer, Berlin, 2003.

[119] H.G. Schuster and W. Just, *Deterministic Chaos: An Introduction.* Wiley VCH, Weinheim, 2005.

[120] G.M. Zaslavsky, *The Physics of Chaos in Hamiltonian Systems.* Imperial College Press, London, 2007.

[121] M.V. Berry, *Proc. R. Soc. Lond. A* 413:183, 1987.

[122] B. Eckhardt, *Phys. Rep.* 163:205, 1988.

[123] J.V. Jose in *New Directions in Chaos.* Volume-II, Hao Bai Lin, (Ed.) World Scientific, Singapore, 1988.

[124] O. Bohigas, M.J. Giannoni and C. Schmit, *Phys. Rev. Lett.* 52:1, 1984.

[125] M.V. Berry and M. Robnik, *J. Phys. A: Math. Gen.* 17:2413, 1984.

[126] R.V. Jensen, *Phys. Rev. Lett.* 49:1365, 1982.

[127] R.V. Jensen, *Phys. Rev. A* 30:386, 1984.

[128] J.V. Jose and R. Cordery, *Phys. Rev. Lett.* 56:290, 1986.

[129] M. Shapiro and G. Goelman, *Phys. Rev. Lett.* 53:1714, 1984.

[130] K. Ganesan, *Classical and Quantum Chaos of the Hydrogen Atom in a Generalized van der Waals Potential.* Ph.D. Thesis, Bharathidasan University, Tiruchirapalli, 1993.

[131] F.J. Dyson and M.L. Mehta, *J. Math. Phys.* 4:701, 1963.

[132] M.L. Mehta, *Random Matrices and the Statistical Theory of Energy Levels.* Academic Press, London, 1967.

[133] M. Carmeli, *Statistical Theory and Random Matrices.* Marcd Dekker Inc., New York, 1983.

[134] C.E. Porter, *Statistical Theories of Spectra: Fluctuations.* Academic Press, New York, 1965.

[135] K. Ganesan and M. Lakshmanan, *Phys. Rev. A* 48:964, 1993.

[136] C.R. Crawford, *Commun. ACM* 16:41, 1973.

[137] R.W. Robinett, *Phys. Rep.* 392:1, 2004.

[138] T. GarcÃŋa, N.A. Cordero and E. Romera, *Phys. Rev. B* 89: 075416, 2014.

[139] A.E. Kaplan, I. Marzoli, W.E. Lamb and W.P. Schleich, *Phys. Rev. A* 61:032101, 2000.

[140] M. Berry, I. Marzoli and W. Schleich, *Phys. World* June 2001 pp.39.

[141] P. Kazemi, S. Chaturvedi, I. Marzoli, R.F. O'Connell and W.P. Schleich, *New J. Phys.* 15:013052, 2013.

[142] M.D. McDonnell, N.G. Stocks, C.E.M. Pearce and D. Abbott, *Stochastic Resonance.* Cambridge University Press, Cambridge, 2008.

[143] P.S. Landa and P.V.E. McClintock, *J. Phys. A: Math. Gen.* 33:L433, 2000.

[144] B. Meerson and L. Friedland, *Phys. Rev. A* 41:5233, 1990.

[145] J. Fajans and L. Friedland, *Am. J. Phys.* 69:1096, 2001.

[146] D.R. Chialvo, O. Calvo, D.L. Gonzalez, O. Piro and G.V. Savino, *Phys. Rev. E* 65:050902(R), 2002.

[147] G. Van der Sande, G. Verschaffelt, J. Danckaert and C.R. Mirrasso, *Phys. Rev. E* 72:016113, 2005.

[148] A. Pikovsky, M. Rosenblum and J. Kurths, *Synchronization - A Universal Concept in Nonlinear Science.* Cambridge University Press, Cambridge, 2001.

[149] G. Saxena, A. Prasad and R. Ramaswamy, *Phys. Rep.* 521:205, 2012.

[150] R. Lofstedt and S.N. Coppersmith, *Phys. Rev. Lett.* 72:1947, 1994.

[151] A. Buchleitner and R.N. Mantegna, *Phys. Rev. Lett.* 80:3932, 1998.

[152] G.S. Engel, T.R. Calhoun, E.L. Read, T.K. Ahn, T. Mancal, Y.C. Cheng, R.E. Blankenship and G.R. Fleming, *Nature* 446:782, 2007.

[153] G. Panitchayangkoon, D.V. Voronine, D. Abramavicius, J.R. Caram, N.H.C. Lewis, S. Mukamel and G.S. Engel, *PNAS* 108:20908, 2011.

[154] N. Lambert, Y.N. Chen, Y.C. Cheng, C.M. Li, G.Y. Chen and F. Nori, *Nature Phys.* 9:10, 2013.

9.11 EXERCISES

9.1 Assume a quantum system with a decay rate proportional to t^m for short times. Evaluate the probability of survival to time t_0. Now imagine a measurement of survival is made at $t = t_0/2$. Evaluate the probability of survival at $t = t_0$ after the measurement. Compare the two probabilities to show that the probability of decay at time t_0 is reduced by a factor 2^{m-1} due to measurements at $t_0/2$ for $m > 1$. Hence, establish quantum Zeno effect.

9.2 In quantum teleportation, find out the operations that Bob has to perform if Alice finds (i) $|\phi^+\rangle$, (ii) $|\phi^-\rangle$ and (iii) $|\psi^-\rangle$.

9.3 For the prisoners' dilemma game set out possible payoffs for zero-sum game, that is $\langle \$_A \rangle + \langle \$_B \rangle = 0$. Formulate a quantum game circuit for the same and calculate the probabilities of A and B to win.

9.4 One Sunday evening a husband and wife wanted to watch a cricket (C) match on a television and a movie (M) in a theatre respectively. They also are happier to stay together rather than far apart. The payoff table is as given below. Assume that $\alpha > \beta > \gamma$. Analyze the classical version of this game, specifically, obtain and analyze the Nash equilibria.

	Husband:M	Husband:C
Wife:M	(α, β)	(γ, γ)
Wife:C	(γ, γ)	(β, α)

9.5 For the quantum version of the husband and wife game obtain the payoffs of the players for the factorizable quantum states (unentangled).

9.6 Suppose in the Pauli channel considered in sec.9.6.2 we have $b_{0,0} = 1$, $b_{0,1} = b_{1,0} = b_{1,1} = 0$. What are the quantum states of A and C? What do you conclude from the obtained result?

9.7 Analyze the partial erasure of two nonorthogonal qubit states $|\Omega\rangle = |\theta, \phi\rangle = \cos(\theta/2)|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin(\theta/2)|1\rangle$ and $|\Omega'\rangle = |\theta', \phi'\rangle$ by removing the azimuthal angle information. What is the result if $\phi = \phi' + 2n\pi$ where n is an integer?

9.8 A quantum deleting machine involves two initially identical qubits in some state $|\psi\rangle$ and an ancilla in some initial state $|A\rangle$. A quantum deleting operation on an input $|\psi\rangle|\psi\rangle$ is defined by $|\psi\rangle|\psi\rangle|A\rangle \rightarrow |\psi\rangle|\Sigma\rangle|A_\psi\rangle$ where a copy of $|\psi\rangle$ is replaced by some standard state of a qubit $|\Sigma\rangle$ and $|A_\psi$ is the final state of the ancilla. What does the deleting machine yield for the input state $|\psi\rangle = \alpha|\mathrm{H}\rangle + \beta|\mathrm{V}\rangle$ where H and V refers to horizontal and vertically polarized photons?

9.9 Consider the previous problem. Express the output state in density matrix form after the deleting operation.