Quantum Information and Computing
Topic- 20 : Quantum Error Correction

Dipan Kumar Ghosh
Physics Department,
Indian Institute of Technology Powai, Mumbai 400076

April 17, 2017

1 Introduction-

Till now we have been discussing essentials of quantum computation and algorithms. However, over the years use of computer is not restricted to computation alone but have extended it to communication. The latter has overtaken the original use for which computers were originally intended. In this and the next few lectures we will explore this aspect of communication.

In its simplest form, communication from one person to another is in spoken or written language. For those who are visually or hearing impaired, man developed sign language and Braille. A major innovation in communication between people who are not in proximity of each other after the invention of telephone. The simple model of communication consists of a sender at one end and a receiver at the other end with a communication channel such as a wired telephone line connecting the two. Over the years there has been many changes. For instance, the intermediate connectivity is not required to be physical wire but could be wireless in the form of radio or microwave.The essential features of communication however remains the same, viz., a sender, a receiver and a communication link. In these lectures, we will look at how the communication protocol will change with the arrival of quantum computers.

An important aspect of communication is its robustness against errors that might creep in, its tolerance to fault. This is also true of computation. An illustration of fault tolerance is in telephonic conversation. Human speech is in the range of 20 Hz to 20,000 Hz. However, telephone transmission is limited to 5000 Hz. This does not cause any problem in understanding what the person at the other end may be speaking about. This is because human hearing does not distinguish such wide range of voice except for keen listeners of classical music. This is the principle behind “fault tolerant computing”. In this lecture we introduce the subject of errors and their correction using quantum com-

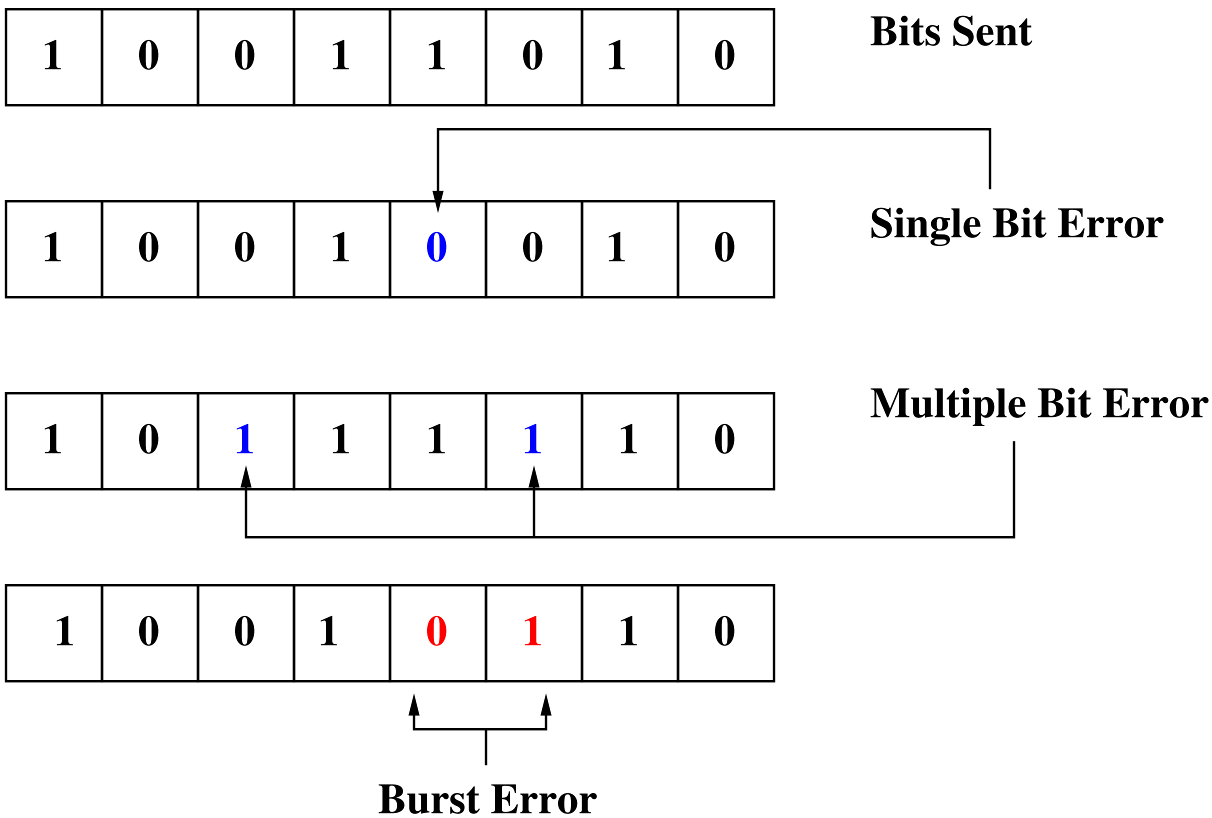

Figure 1: Errors in Classical Communication

munication protocol. The intermediary between the sender and a receiver is a channel is noisy and thereby introduces errors in communication.

2 Errors in Classical Communication

Let us first look at what are the errors and how to detect them. We begin by looking at errors using a classical computer where the message is sent by binary strings. The only type of error that may arise is flipping of a bit which may occur during transmission, i.e. a bit 0 may become 1 or vice versa. Such error may occur in isolation or may occur in a group. This leads to "corruption" in communication which implies that the data received by the receiver is different from what was sent by the sender. The communication protocol provides for detection and correction of such errors. Figure 1 gives the types of errors that arises in classical communication.

The first row shows the bit string that was sent. The second row shows the string to be received with an isolated bit flip in the 5th position. The third row shows multiple bit errors where the bit flips are not contiguous. The last row shows "burst error" where the flips occur in adjacent bits. Various methods have been used to detect errors.One such protocol could be the sender adding a parity bit to the strings sent such that (for instance) the number of 1s could become even. If there is a departure from this rule in receiving, the sender could be asked to send it again. For example suppose the sender intends to send the string 10110010 which has 4 1s which is already even and hence the parity bit to be added is a 0 at the end which makes the sender send 101100100 as the string. Suppose, however, the receiver receives a string like 10100010 which has three 1s, the string must have an error as the number of 1s in the string is 3 which is odd. The parity bit added by the sender is 1 if the original message had odd number of 1s. (It is unimportant whether the protocol selects the number of 1s to be even or odd as long as the same protocol is understood by the receiver.

The above procedure is clumsy. What is a more effective protocol is to build a redundancy. In this method each bit is send a multiple bunch of odd number. If we choose to triplicate each bit, the bit 0 will be sent as 000 and bit 1 as 111. This will be designated as "logical bit". : $0_L = 000$ and $1_L = 111$. When the communication is received the system monitors whether every group of three bits are identical. If not, it can autocorrect it by what is known as "majority votes" which simply implies that in a bunch of three, if the bits are not identical, the bit that occurs twice is taken to be the actual bit sent. Thus the message received is 111 011 000 111 000 001, the bit that was intended to be sent is 110100. There is no special reason for sending three as the logical bunch it could be five or seven or any odd number.

3 Errors In Quantum Communication

In view of Quantum No cloning theorem, duplicating or triplicating quantum states in not an option. We recall that in quantum communication the qubit that is sent need not be 0 or 1 alone but could be a linear combination of the two. Had it been the former, No-Cloning theorem would not be an issue because the theorem does allow cloning of orthogonal qubits; it is the duplication arbitrary quantum state that cannot be duplicated. The second issue is that even if in some way we could create the triplets, determining the majority is not possible because a measurement would cause a collapse of each qubit to the measurement basis. For instance if the logical qubit triplet that was sent is $(a \mid 0\rangle + b \mid 1\rangle)(a \mid 0\rangle + b \mid 1\rangle)(a \mid 0\rangle + b \mid 1\rangle)$, a measurement in computational basis would collapse it to any of the 8 possibilities $000, 001, \ldots 111$ which does not allow us to infer either the qubit that was sent or use a majority vote to correct errors if any.

One of the problems connected with quantum communication arises due to the fact that that quantum states are extremely fragile and easily "decohere" because of interaction with the environment. Decoherence implies loss of phase relationship between components of a quantum states in a superposition of states. Maintaining coherent superposition of multi-qubit quantum system over a period long enough to complete a quantum algorithm is a difficult task. Unlike classical situation, bit flips are not the only errors that occur in classical communication. Continuous evolution of quantum states may introduce phase

errors as well in addition to changing the amplitudes of components.
Suppose we started with a state $\mid \psi\rangle = \dfrac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}$. Suppose as a result of decoherence a relative phase was introduced between the two components making the state $\mid \psi'\rangle = \dfrac{\mid 0\rangle + e^{i\alpha} \mid 1\rangle}{\sqrt{2}}$ which can be written as a matrix $\dfrac{1}{\sqrt{2}} e^{i\alpha/2} \begin{pmatrix} e^{-i\alpha/2} \\ e^{i\alpha/2} \end{pmatrix}$. If we measure σ_z, the distribution of the components would remain the same, the states $\mid 0\rangle$ and $\mid 1\rangle$ occurring with probability 1/2 each. However, if we measure σ_x, we would measure either eigenvalue $+1$ or -1. The probability with which the eigenvalue $+1$ would appear is obtained by applying the projection operator $P_+ = \dfrac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ on the state $\mid \psi'\rangle$, which gives $\dfrac{1}{\sqrt{2}} e^{i\alpha/2} \cos(\alpha/2) \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, i.e. the eigenvalue $+1$ occurs with probability $\cos^2 \alpha/2$.

4 Three Qubit Error Code for bit flip errors

An arbitrary error in quantum combination can be considered to be a combination of both bit flip error and phase flip error. We will first consider bit flip errors and methods to correct such errors. Subsequently we will take up the more general case of bit flip as wqell as phase flip.

4.1 Generating Logical Qubits

Let us assume that sender Alice wishes to send a state $\mid \psi\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle$ to receiver Bob. Instead of sending the single qubit, Alice would like to build in some redundancies but it cannot be done in the classical way. What she does (Figure 1) is to introduce two ancilla bits, which are initialized to $\mid 0\rangle$ each. She performs two CNOT operation as shown in the figure. The result of the CNOT operations is as follows:

$$(\alpha \mid 0\rangle + \beta \mid 1\rangle) \otimes \mid 0\rangle \otimes \mid 0\rangle \rightarrow \alpha \mid 000\rangle + \beta \mid 111\rangle \equiv \mid \psi_L\rangle$$

Note that the logical qubit is different from the corresponding classical case, in the sense that the quantum state itself is not triplicated but the state is a linear combination of the state $\mid 000\rangle$ and $\mid 111\rangle$ with the same coefficients as in the original state.
Now suppose we have a noisy channel which flips one of the qubits with a probability p, and leaves it unchanged with a probability $1 - p$. The state received by Bob is $\mid \psi_2\rangle_L$. This gives rise to the following states and the corresponding probabilities with which they are received:

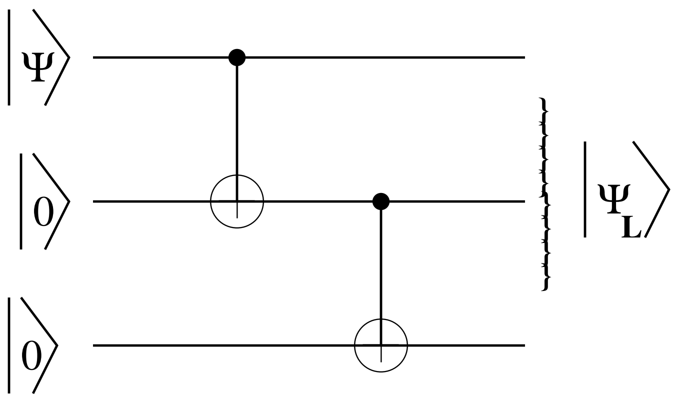

Figure 2: Generating Logical Qubits

state received	probability	comments
$\alpha \mid 000\rangle + \beta \mid 111\rangle$	$(1-p)^3$	No error in any qubit
$\alpha \mid 100\rangle + \beta \mid 011\rangle$	$p(1-p)^2$	one error
$\alpha \mid 010\rangle + \beta \mid 101\rangle$	$p(1-p)^2$	one error
$\alpha \mid 001\rangle + \beta \mid 110\rangle$	$p(1-p)^2$	one error
$\alpha \mid 110\rangle + \beta \mid 001\rangle$	$p^2(1-p)$	two errors
$\alpha \mid 101\rangle + \beta \mid 010\rangle$	$p^2(1-p)$	two errors
$\alpha \mid 011\rangle + \beta \mid 100\rangle$	$p^2(1-p)$	two errors
$\alpha \mid 111\rangle + \beta \mid 000\rangle$	p^3	three errors

It may be noted that probability of no error in any of the qubits is $(1-p)3$, of error in one qubit is $3p(1-p)^2$, of case where two qubits are flipped two is $3(1-p)p^2$ and of the case where all three qubits are flipped is p^3.

4.2 Corrective steps taken by Bob

At Bob's end, he is aware that there is a probability with which there are errors in the bits that have been received. To remedy the situation, he takes the following steps (Figure 2). He introduces two additional ancilla (the 4th and the 5th lines in the figure), each initialized to $\mid 0\rangle$. Having done that, he applies two CNOT gates on the 4th line with the first and the second qubits received by him. He applies two CNOTS on the 5th qubit as well but with the first and the third qubits as control. The result of the CNOT depends on what was the state of the three qubits received by him and is summarized on the table below. IT may be noted that the first three qubits are now coupled with the 4th and 5th qubits.

First three qubits ($\mid \psi_2\rangle$)	Resulting 5 qubit state ($\mid \psi_3\rangle$)
$\alpha \mid 000\rangle + \beta \mid 111\rangle$	$\alpha \mid 00000\rangle + \beta \mid 11100\rangle$
$\alpha \mid 100\rangle + \beta \mid 011\rangle$	$\alpha \mid 10011\rangle + \beta \mid 01111\rangle$
$\alpha \mid 010\rangle + \beta \mid 101\rangle$	$\alpha \mid 01010\rangle + \beta \mid 10110\rangle$
$\alpha \mid 001\rangle + \beta \mid 110\rangle$	$\alpha \mid 00101\rangle + \beta \mid 11001\rangle$
$\alpha \mid 110\rangle + \beta \mid 001\rangle$	$\alpha \mid 11001\rangle + \beta \mid 00101\rangle$
$\alpha \mid 101\rangle + \beta \mid 010\rangle$	$\alpha \mid 10110\rangle + \beta \mid 01010\rangle$
$\alpha \mid 011\rangle + \beta \mid 100\rangle$	$\alpha \mid 01111\rangle + \beta \mid 10011\rangle$
$\alpha \mid 111\rangle + \beta \mid 000\rangle$	$\alpha \mid 11100\rangle + \beta \mid 00000\rangle$

It may be noted that two flips due to both controls being 1 restores the original qubit. The last column gives the entangled five qubit states that has been generated. However, an inspection shows the states are not really entangled as in each case the 4th and 5th qubits are the same. If at this stage, if we measure the ancilla bits, we would get 00, 01, 10 or 11 with different probabilities. Each result arises in two different situations. For instance, if the ancilla bit is found to be 00, this could have arisen from the top or the bottom row of the table, the former with a probability $(1-p)^3$ and the latter with a probability p^3. Since p is usually small, it is likely to be an error free state. Based on this probability, Bob does not take any corrective action, though the state actually received by him, may have error in all the three qubits.

Consider the case where the ancilla measures $\mid 01\rangle$, which again arises in two situations. It could either be a state received with an error in one qubit $\alpha \mid 001\rangle + \beta \mid 110\rangle$ with error in the third qubit or a state $\alpha \mid 110\rangle + \beta \mid 001\rangle$ with errors in the first and second qubit, the former with a probability $p(1-p)^2$ and the latter with a probability $p^2(1-p)$. Bob now decides to take a chance with the former and applies an X-gate on the third qubit. This will clearly restore the first alternative to its correct form but make the situation

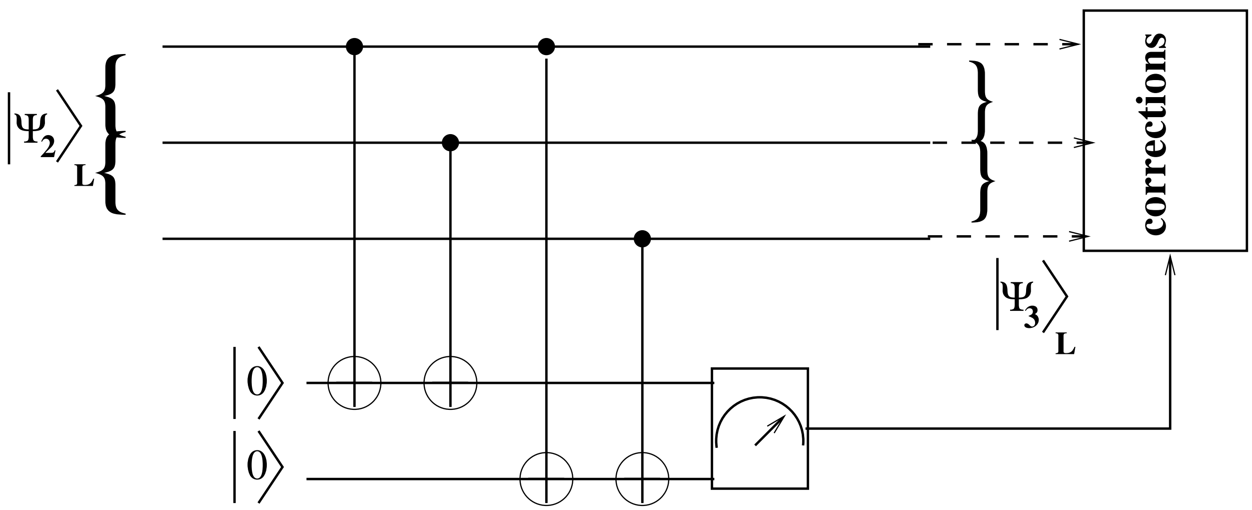

Figure 3: Error correction circuit

worse for the second alternative making the state have errors in all the three qubits.
If the ancilla state is measured to be $|10\rangle$, once again there are two possibilities, one with a single error in the second position or two errors in the first and the third positions. The step that Bob will take is to apply σ_x on the second qubit. In a similar way if the ancilla bit measures $|11\rangle$, Bob will apply X-gate to the first qubit.
The net effect of Bob's corrective measures is to reduce errors substantially. Note that he will take no action with a probability of $(1-p)^3$ and with apply x-gate on one of the qubits with a probability of $3p(1-p)^2$. The failure rate is $p^3 + 3p^2(1-p) = 3p^2 - 2p^3$ which is less than p. For instance for $p = 0.01$, this works out to 3×10^{-4} which is a reduction of error by a factor of 300.

5 Shor's 9-qubit code

In the last section we discussed 3 qubit code which takes care of bit flips. Quantum states have another possible error, viz., in addition to bit flips it may have phase errors which does not exist in case of classical codes. The phase errors result in decoherence which requires that quantum measurements must be fast enough compared to the decoherence time. Consider the following situation in which a state which was initially $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ decohere and pick up a relative phase between its components giving rise to a state $\dfrac{|0\rangle + e^{i\alpha}|1\rangle}{\sqrt{2}}$. We have seen that while a measurement of σ_z still yields eigenvalues ± 1 with a probability of half each, this is not so if one measures the x-component of spin. The probability of measuring eigenvalue $+1$ is $\cos^2(\alpha/2)$ and that of getting -1 is $\sin^2(\alpha/2)$. In this lecture we would look at both these aspects, i.e., bit flip error and phase error, and see that this can be considered together in what is known as Shor's 9-qubit error code.

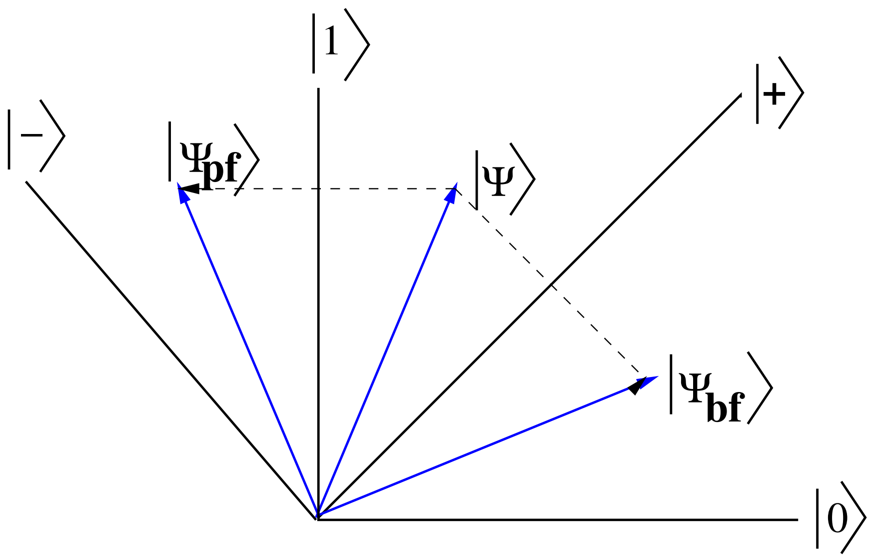

Figure 4: Geometrical representation of phase flip and bit flip

5.1 Conversion of Phase Error to Bit error

Phase errors occur due to a rotation of a qubit by an arbitrary angle φ which converts a state $a \mid 0\rangle + b \mid 1\rangle$ to a state $a \mid 0\rangle + be^{i\alpha} \mid 1\rangle$. Let us consider the simple case of a phase flip (i.e. the case of $\varphi = \pi$ in which a state $a \mid 0\rangle + b \mid 1\rangle$ gets converted to $a \mid 0\rangle - b \mid 1\rangle$. It may be observed that the special case in which the state $\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}$ becomes $\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$ is simply a bit flip in the diagonal basis in which $\mid +\rangle \leftrightarrow \mid -\rangle$. A geometrical interpretation is shown in figure 1 where the computational basis $\mid 0\rangle$ and $\mid 1\rangle$ are taken respectively along the Cartesian x and y axes. The diagonal basis makes an angle of 45° with these. Consider an arbitrary state $\mid \psi\rangle$. If there is a bit flip, it makes the state become $\mid \psi_{bf}\rangle$ as shown in the figure. Geometrically, this is equivalent to reflection of the state $\mid \psi\rangle$ about the direction $\mid +\rangle$. The phase flip can also be similarly looked at. In the figure, the state $\mid \psi_{pf}\rangle$ represents a state where the phase is flipped by π. This can be obtained by reflecting the state $\mid \psi\rangle$ about the state $\mid 1\rangle$.

Thus one of the ways of handling such phase flip will be to treat it as a bit flip in the diagonal basis and encode it as a triplet in this basis, i.e. $\mid \psi\rangle = a \mid +++\rangle + b \mid ---\rangle$. In the computational basis the state is obtained by expressing $\mid \pm\rangle = \frac{1}{\sqrt{2}}(\mid 0\rangle \pm \mid 1\rangle)$, which gives

$$\frac{a+b}{2\sqrt{2}} \left[\mid 000\rangle + \mid 011\rangle + \mid 101\rangle + \mid 110\rangle\right] + \frac{a-b}{2\sqrt{2}} \left[\mid 001\rangle + \mid 010\rangle + \mid 100\rangle + \mid 111\rangle\right]$$

Suppose we now measure any of the qubits in the computational basis. Measurement of the first qubit would make the state collapse either to the state

$$\frac{a+b}{\sqrt{2}}[|\,000\rangle+|\,011\rangle]+\frac{a-b}{\sqrt{2}}[|\,001\rangle+|\,010\rangle]$$

or to

$$\frac{a+b}{\sqrt{2}}[|\,101\rangle+|\,110\rangle]+\frac{a-b}{\sqrt{2}}[|\,100\rangle+|\,111\rangle]$$

Suppose it collapsed to the former. We now do a parity check in the *diagonal basis* by introducing two ancilla and measure the antilla after the CNOT operation, as we had done in the bit flip case. In the diagonal basis the collapsed state may be expressed as $[a\,|+++\rangle+b\,|---\rangle]$ or $[a\,|-++\rangle+b\,|+--\rangle]$. Thus the state is either without any error or with a single bit flip error, which can be corrected after an appropriate corrective action on the antilla.
Lets now discuss how to take care of both bit flip and phase flip in the same error code. This is known as **Shor's 9-qubit error code.** It may be observed that bit flip is corrected by application of an X gate, phase flip by a Z gate while a simultaneous bit and phase flip by a product of the two gates, which is essentially a Y-gate but for an overall phase factor.

6 Shor's 9- Qubit Code - Encoding

in this method the qubit $|\,0\rangle$ is encoded as $|\,0\rangle_L=|+++\rangle$ and $|\,1\rangle$ as $|\,1\rangle_L=|---\rangle$. The encoding is done by the circuit shown in figure 2.

Let us try to understand how the encoding circuit works. We shall encode the state $a\,|\,0\rangle+b\,|\,1\rangle$ using this code. We first do a phase flip encoding. This is done by introducing two ancilla, initialized to state $|\,0\rangle$. This is shown in the left half of the figure. First we apply a CNOT gate on each of the ancilla using $|\,\psi\rangle$ as the control. This would make the the three qubit state become $a\,|\,000\rangle+b\,|\,111\rangle$. After this we apply a Hadamard gate on each of the qubits. The result is easily calculated and is

$$a\left[\frac{|\,0\rangle+|\,1\rangle}{\sqrt{2}}\otimes\frac{|\,0\rangle+|\,1\rangle}{\sqrt{2}}\otimes\frac{|\,0\rangle+|\,1\rangle}{\sqrt{2}}\right]+b\left[\frac{|\,0\rangle-|\,1\rangle}{\sqrt{2}}\otimes\frac{|\,0\rangle-|\,1\rangle}{\sqrt{2}}\otimes\frac{|\,0\rangle-|\,1\rangle}{\sqrt{2}}\right]=$$

$$\frac{a}{2\sqrt{2}}[|\,000\rangle+|\,001\rangle+|\,010\rangle+|\,011\rangle+|\,100\rangle+|\,101\rangle+|\,110\rangle+|\,111\rangle]+$$

$$\frac{b}{2\sqrt{2}}[|\,000\rangle-|\,001\rangle-|\,010\rangle+|\,011\rangle-|\,100\rangle+|\,101\rangle+|\,110\rangle-|\,111\rangle]$$

At this stage we introduce with each of the three qubits, we introduce two ancilla each, making total number of qubits to be 9, which is the origin of the name of the code. The right half of the figure illustrates this.
Now using the three qubits of the previous step as control, we perform a CNOT operation

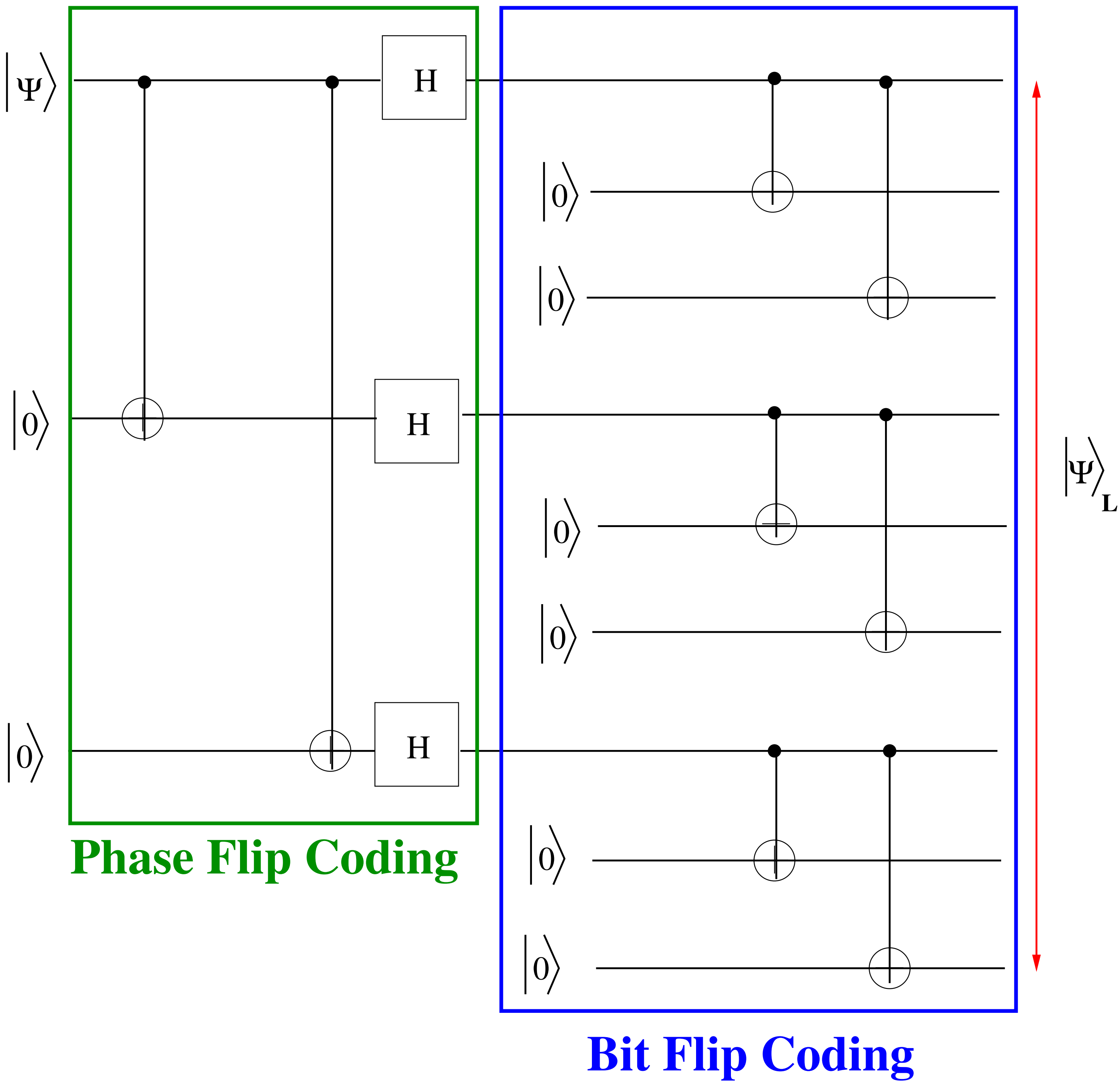

Figure 5: Encoding circuit for Shor Code

on each of the 6 new ancilla which were all initialized to $\mid 0\rangle$. The result of the CNOT gates is to produce the state

$$\frac{a}{2\sqrt{2}}\left[(\mid 000\rangle + \mid 111\rangle)\otimes(\mid 000\rangle + \mid 111\rangle)\otimes(\mid 000\rangle + \mid 111\rangle)\right] +$$

$$\frac{b}{2\sqrt{2}}\left[(\mid 000\rangle - \mid 111\rangle)\otimes(\mid 000\rangle - \mid 111\rangle)\otimes(\mid 000\rangle - \mid 111\rangle)\right]$$

where the terms have been kept distinct so as to identify them with the first three being the original state and the two new ancilla, the second triplet consisting of one of the previous ancilla along with the two additional ones and finally, the second stage 1 ancilla with the two new ones. We use a short hand notation in which we represent $\frac{1}{\sqrt{2}}(\mid 000\rangle + \mid 111\rangle$ as $\mid +\rangle$ and $\frac{1}{\sqrt{2}}(\mid 000\rangle - \mid 111\rangle)$as $\mid -\rangle$. This enables us to write the state as $a \mid + + +\rangle + b \mid - - -\rangle$. (Caution: the notation $\mid +\rangle$ here does not stand for the diagonal basis state).

We now assume that there may be an error in one, *and only one* qubit and the nature of the error in this qubit may be either a bit flip, a phase flip or a simultaneous bit and phase flip. Let p be the probability of such an error, which is usually a small quantity, less than 1%. Let us calculate various probabilities. Probability that none of the qubits is affected is $(1-p)^9 \approx 1 - 9p + 36p^2$. The probability that any of the 9 qubits is affected is $9p(1-p)^8 = 9p(1-8p) \simeq 9p - 72p^2$. Thus, the probability that either there is no error or at best one error in transmission is $1 - 36p^2$ so that the probability that there are more than one error is $36p^2$, which is a small quantity.

In the next section , we will discuss how the decoding circuit works.

7 The Decoding Circuit

A point to note about the phase flip is that though we assumed that the error occured in the first qubit, in principle, it is indistinguishable from the case where the error occurs in qubit 2 or 3 as it would only give a relative minus sign. Assuming that the first qubit has an σ_y error, i.e. both a bit flip and a phase flip.The state that we then have is

$$\frac{a}{2\sqrt{2}}\left[(\mid 100\rangle - \mid 011\rangle)\otimes(\mid 000\rangle + \mid 111\rangle)\otimes(\mid 000\rangle + \mid 111\rangle)\right] +$$

$$\frac{b}{2\sqrt{2}}\left[(\mid 100\rangle + \mid 011\rangle)\otimes(\mid 000\rangle - \mid 111\rangle)\otimes(\mid 000\rangle - \mid 111\rangle)\right]$$

For the purpose of analysis, it is convenient to group the 9 qubits as 3 groups of three qubits each. In each of the three groups we carry out the following operations. (a) Using the first of the triplets as the control, we apply CNOT gates on the second and third member of the triplet. After this we apply (b) a CCNOtTon the first qubit using

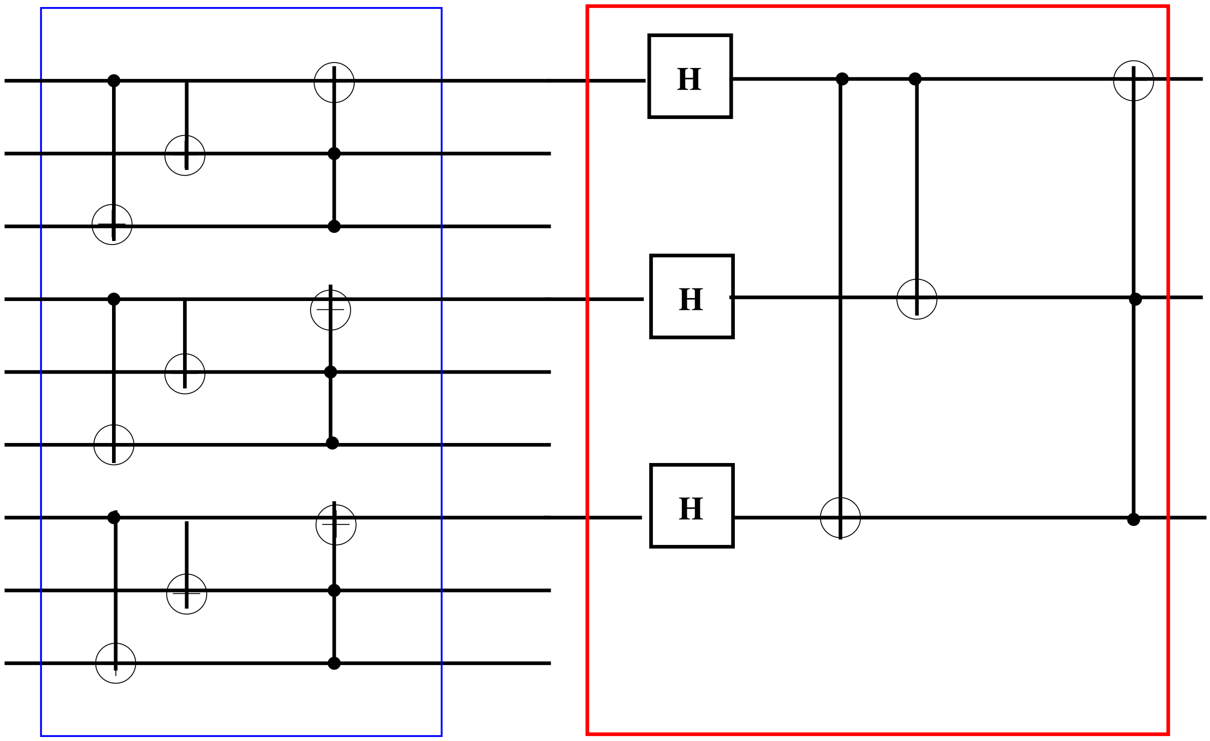

Figure 6: Shor's Decoding Circuit

the second and the third as the controls. Identical operations for the group (4,5,6) and (7,8,9). The result of the action (a) is to give

$$\frac{a}{2\sqrt{2}}\left[(\mid 111\rangle - \mid 011\rangle) \otimes (\mid 000\rangle + \mid 100\rangle) \otimes (\mid 000\rangle + \mid 100\rangle)\right] +$$

$$\frac{b}{2\sqrt{2}}\left[(\mid 111\rangle + \mid 011\rangle) \otimes (\mid 000\rangle - \mid 100\rangle) \otimes (\mid 000\rangle - \mid 100\rangle)\right]$$

The application of CCNOT gate in step (b) will then give the following

$$\frac{a}{2\sqrt{2}}\left[(\mid 011\rangle - \mid 111\rangle) \otimes (\mid 000\rangle + \mid 100\rangle) \otimes (\mid 000\rangle + \mid 100\rangle)\right] +$$

$$\frac{b}{2\sqrt{2}}\left[(\mid 011\rangle + \mid 111\rangle) \otimes (\mid 000\rangle - \mid 100\rangle) \otimes (\mid 000\rangle - \mid 100\rangle)\right]$$

This is the output from the left half of the circuit shown in the figure. It may be seen that in each case, we can factorize the states and write it as

$$\frac{a}{2\sqrt{2}}\left[(\mid 0\rangle - \mid 1\rangle) \mid 11\rangle \otimes (\mid 0\rangle + \mid 1\rangle) \mid 00\rangle \otimes (\mid 0\rangle + \mid 1\rangle) \mid 00\rangle\right] +$$

$$\frac{b}{2\sqrt{2}}\left[(\mid 0\rangle + \mid 1\rangle) \mid 11\rangle \otimes (\mid 0\rangle - \mid 1\rangle \mid 00\rangle) \otimes (\mid 0\rangle - \mid 1\rangle) \mid 00\rangle\right]$$

We ignore now the second set of ancilla that we had introduced and concentrate only on the first, the fourth and the seventh qubits. On these we apply Hadamard gates, which yields $a \mid 1\rangle_1 \mid 0\rangle_4 \mid 0\rangle_7 + b \mid 0\rangle_1 \mid 1\rangle_4 \mid 1\rangle_7$, where the subscripts are to remind us about the qubit numbers. We now apply a CNOT gates each on qubits 4 and 7 with qubit 1 as the control. This would give $a \mid 1\rangle_1 \mid 1\rangle_4 \mid 1\rangle_7 + b \mid 0\rangle_1 \mid 1\rangle_4 \mid 1\rangle_7$. The final act is to apply a CCNOT on the first qubit with the 4th and 7th as control, yielding $a \mid 0\rangle_1 \mid 1\rangle_4 \mid 1\rangle_7 + b \mid 1\rangle_1 \mid 1\rangle_4 \mid 1\rangle_7 = (a \mid 0\rangle + b \mid 1\rangle) \otimes \mid 11\rangle$.

Though for illustration purpose we had selected error to occur in qubit 1, the principle enunciated here is equally applicable for any of the qubits. Let us summarize what we have learnt. We had encoded the qubit $\mid 0\rangle$ as $(\mid 000\rangle + \mid 111\rangle)^{\otimes 3}$ and the qubit $\mid 1\rangle$ as $(\mid 000\rangle - \mid 111\rangle)^{\otimes 3}$. Suppose a bit flip has occurred. We need to find out in which qubit the error has occurred. The way to do is to check parity. When we compare parity of 1 and 2, we get either a $+1$ or a -1. This is trivially done by measuring $\sigma_{z1} \otimes \sigma_{z2}$. Since we have assumed that there is only one error, we know for a fact that an error has occurred in one of the qubits if the parity is -1, either in qubit 1 or in qubit 2. We now repeat the procedure for bits 2 and 3 to determine which is the qubit where it actually occurred. If both result in $+1, +1$ which implies there is no error. If one of the checks is positive while the other is negative, one can easily conclude which qubit the error was there. The following example illustrates the protocol. Recall that in our notation $\mid +\rangle = \frac{1}{\sqrt{2}}(\mid 000\rangle + \mid 111\rangle$. If all the 9 qubits are error free, we would have $a \mid +++\rangle + b \mid ---\rangle = a \mid 0\rangle_L + b \mid 1\rangle_L$. Because of superposition principle, we can consider error in each of the basis vector separately. Suppose a bit flip has occurred in the fifth qubit. We then would have received $\mid +\rangle \frac{1}{\sqrt{2}}(\mid 010\rangle + \mid 101\rangle) \mid +\rangle$. We will now check group-wise checking parity of the first and the second qubit first, i.e. find out $x_1 \oplus x_2$ which is 0 and then 2 and 3 for which $x_2 \oplus x_3$ also is zero. Thus there is no error in the first group. In the second group, we find $x_4 \oplus x_5 = 1$, showing that there is a fault in the 4th or the 5th qubit. We now find $x_5 \oplus x_6$ which also gives one, showing that there is a

fault in the fifth or the sixth qubit. Combining these two result and considering that we have a maximum of one error, we already have found the error to be in the fifth qubit. The error, once detected can be corrected by application of a X-gate.
The phase flip occurring in any of the qubits within a given block alters the sign of the entire block and the correction is done the same way irrespective of where the phase flip actually is. Thus we need to compare the phase of the first 6 qubits (i.e. of the first two blocks) which can be done by applying $\sigma_{x1}\sigma_{x2}\sigma_{x3}\sigma_{x4}\sigma_{x5}\sigma_{x6}$ which will find out if the error has occurred in the first two blocks by flipping each of the six qubits and then comparing the sign of the second and the third block, which may be done by applying $\sigma_{x4}\sigma_{x5}\sigma_{x6}\sigma_{x7}\sigma_{x8}\sigma_{x9}$. This way Shor code can detect both phase flip errors and bit flip errors.