FUNDAMENTALS OF QUANTUM COMPUTING

Page No: 2

Date:

21/02/20 Friday.

For 2nd ~~Sessional~~

Quantum Key Distribution (QKD) (BB84) (Bennett & Brassard 1984)

Assumptions

1) Alice & Bob share public authenticated classical channel
2) Alice can publicly send qubits to Bob.

The Basic BB84 protocol

1) For i=1 to n
   - Alice randomly chooses a qubit $|0\rangle$ or $|1\rangle$ and randomly chooses basis H or X & sends it to Bob. (over quantum channel)

2) Bob receives a random sequence of qubits.

3) For each qubit, Bob randomly applies basis H or X & measure the qubit in chosen basis.

4) Bob announces (over the classical channel) which basis he used for each measurement.

5) Alice tell Bob which measurements were made in the correct basis.

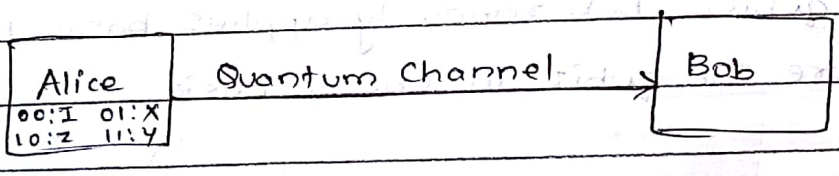
6) The qubits which were measured in the wrong basis are rejected, while rest form a shared key.

Example: $n=6$

	1	2	3	4	5	6
	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|\psi\rangle$
Alice	X	H	X	X	H	H
	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$ (public)
	H	H	X	H	X	H (Public)
Bob	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$
Alice	✓	✓				✓ (public)

Shared key : $|0\rangle$ $|1\rangle$ $|1\rangle$

Superdense Coding



Communication from Alice to Bob

- In Superdense coding, Alice wants to transmit Bob 2 classical bits by sending one qubit over the quantum channel. Suppose Alice & Bob initially share a pair of qubits in the entangled state,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alice initially in possession of 1st qubit, while bob has possession of the 2nd qubit.

Alice: Alice wants to send bob a binary number $x \in \{00, 01, 10, 11\}$. Depending on the number, Alice performs the transformation $\{I, X, Z, iy\}$ on her qubit of the entangled state $|\psi\rangle$.

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

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Page No :
Date :

The resulting new state is,

x	transformation	New State
0=00	$\|\psi_0\rangle = (I \otimes I) . \|\psi\rangle$	$\|\psi_0\rangle = \frac{1}{\sqrt{2}} (\|00\rangle + \|11\rangle)$
1=01	$\|\psi_1\rangle = (X \otimes I) . \|\psi\rangle$	$\|\psi_1\rangle = \frac{1}{\sqrt{2}} (\|10\rangle + \|01\rangle)$
2=10	$\|\psi_2\rangle = (Z \otimes I) . \|\psi\rangle$	$\|\psi_2\rangle = \frac{1}{\sqrt{2}} (\|00\rangle - \|11\rangle)$
3=11	$\|\psi_3\rangle = (iy \otimes I) \|\psi\rangle$	$\|\psi_3\rangle = \frac{1}{\sqrt{2}} (-\|10\rangle + \|01\rangle)$

Alice then sends her qubit to Bob.

Bob: To decode the information Bob applies a CNOT to 2 qubits of the entangled pair. and then applies the Hadamard transformation H to the first qubit

Received State	Output of CNOT
$\|\psi_0\rangle$	$1/\sqrt{2} (\|00\rangle + \|10\rangle) =$
$\|\psi_1\rangle$	$1/\sqrt{2} (\|11\rangle + \|01\rangle) =$
$\|\psi_2\rangle$	$1/\sqrt{2} (\|00\rangle - \|10\rangle) =$
$\|\psi_3\rangle$	$1/\sqrt{2} (-\|11\rangle + \|01\rangle) =$

$= 1/\sqrt{2} (|0\rangle + |1\rangle) \otimes |00\rangle$

$= 1/\sqrt{2} (|1\rangle + |0\rangle) \otimes |11\rangle$

$= 1/\sqrt{2} (|0\rangle - |1\rangle) \otimes |10\rangle$

$= 1/\sqrt{2} (-|1\rangle + |0\rangle) \otimes |11\rangle$

Output of H.

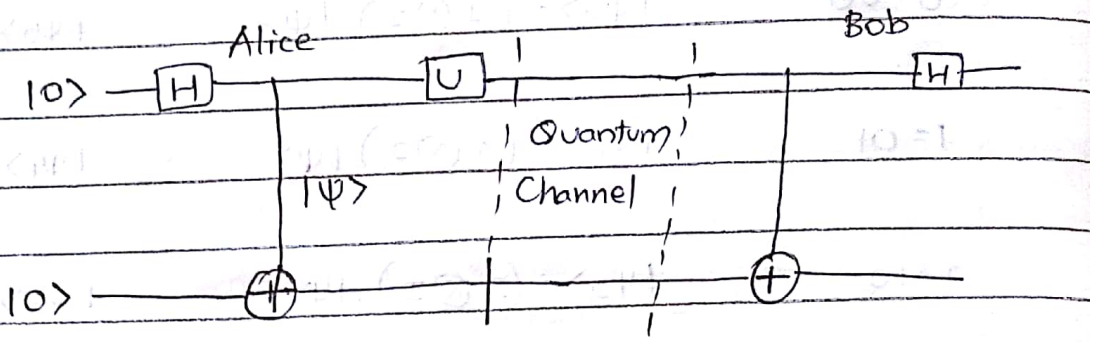
$|00\rangle$

$|01\rangle$

$|10\rangle$

$|11\rangle$

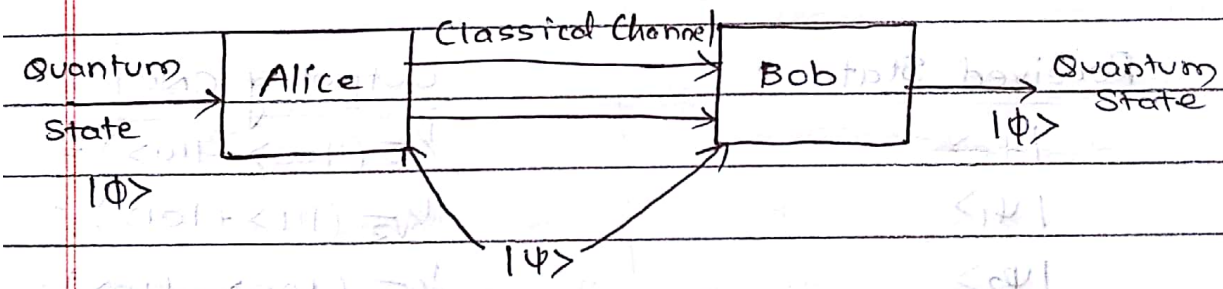
Quantum Circuit Implementation of Superdense Coding



$U = \{I \text{ or } X \text{ or } Z \text{ or } iy\}$

The number x is either 00 or 01 if the measurement of 1st qubit results in $|0\rangle$, while it either $|10\rangle$ or $|11\rangle$ if it is $|1\rangle$.

Quantum Teleportation



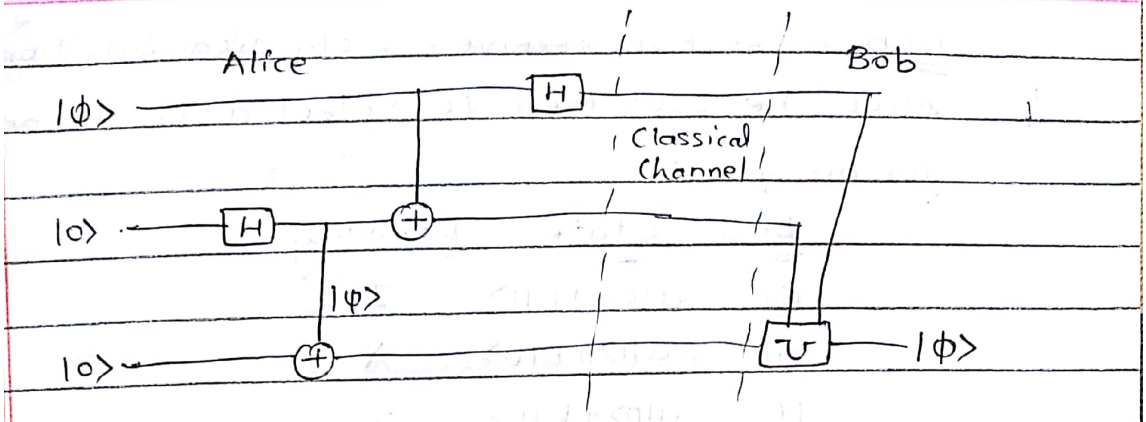
Quantum teleportation is the opposite of superdense coding in that it uses 2 classical bits to transmit single qubit quantum state $|\phi\rangle = a|0\rangle + b|1\rangle$

Alice: Alice has a qubit $|\phi\rangle = a|0\rangle + b|1\rangle$, wants to send to Bob using 2 classical bits

Assume that Alice & Bob share one qubit of an entangled state.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alice Bob Alice Bob



U: I or X or Z or iY

Quantum Circuit Implementation Quantum teleportation

The composite system comprising of $|\phi\rangle$ & $|\psi\rangle$ is,

$$|\phi\rangle \otimes |\psi\rangle = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)$$

(A A B)

Alice controls the 1st 2 qubits & Bob controls 3rd qubit.

Alice applies CNOT to $|\psi_0\rangle$

$$|\psi_1\rangle = (\text{CNOT} \otimes I)\,|\psi_0\rangle$$

$$= (\text{CNOT} \otimes I)\left(\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)\right)$$

$$= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle)$$

Alice now applies H gate to her qubit

$$|\psi_2\rangle = (H \otimes I \otimes I)\cdot|\psi_1\rangle$$

$$= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle)$$

$$= \frac{1}{2}\left(a(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + b(|010\rangle - |110\rangle + |001\rangle - |101\rangle)\right)$$

$$= \frac{1}{2}\left(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)\right)$$

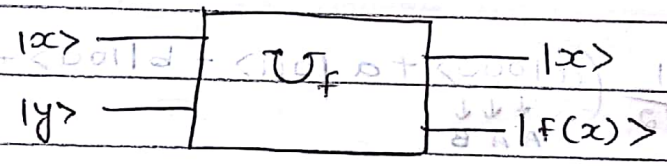
Bob: When bob receives 2 classical bits from Alice, he uses them to select a transformation for his qubit.

Bits	State	Decoding
00	$a\|0\rangle + b\|1\rangle$	I
01	$a\|1\rangle + b\|0\rangle$	X
10	$a\|0\rangle + b\|1\rangle$	Z
11	$a\|1\rangle - b\|0\rangle$	iy

Quantum Parallelism

Given an input x, a typical quantum computer computes $f(x)$ in such a way as,

$$U_f : |x\rangle |0\rangle \longrightarrow |x\rangle |f(x)\rangle$$



Suppose U_f acts on the input which is a superposition of many states, then output is also superposition of all the results

$$U_f : \sum_x |x\rangle |0\rangle \rightarrow \sum_x |x\rangle |f(x)\rangle$$

when the input is a superposition of n states, U_f computes n values $f(x_k)$, $1 \le k \le n$ simultaneously. this feature is called quantum parallelism

Date :

$|0\rangle^n \xrightarrow{H^n}$

$|00\cdots0\rangle \xrightarrow{H^n}$

$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|0\rangle \otimes |0\rangle \xrightarrow{H^2} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$

$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

$|0\rangle \otimes |0\rangle \otimes |0\rangle \cdots |0\rangle \xrightarrow{H^n}$

n qubit

$\frac{1}{\sqrt{2^n}}(|00000\cdots0\rangle + |0\cdots1\rangle + \cdots + |1111\cdots1\rangle)$

$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$

Simple Quantum Algorithms

1) Deutsch Algorithm

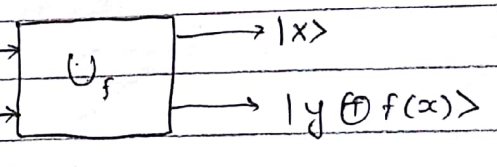
Let, $f: \{0,1\} \to \{0,1\}$ be a binary func. Note that there are four possible values of f, namely

$f_1: 0 \to 0, 1 \to 0$, $f_2: 0 \to 1, 1 \to 1$

$f_3: 0 \to 0, 1 \to 1$, $f_4: 0 \to 1, 1 \to 0$

The first two cases, f_1 & f_2 are called constant, while the rest f_3 & f_4 are balanced.

Oracle : Oracle is basically a black box computation of a function.



Black Box

$U_f : |x, y\rangle \longrightarrow |x, y \oplus f(x)\rangle$

If we set $y=0$, output is $f(x)$

If we set $y=1$, output is $f(\bar{x})$

- This is nothing but CNOT-gate with control bit $f(x)$, the target bit, y is flipped if and only if $f(x)=1$, otherwise no change.

-

Deutsch Algorithm:

Input : one qubit $|0\rangle$ or $|1\rangle$

Output : func^n is constant or balanced

(i). Constant : $f(0) = f(1) = \begin{cases} 0 \\ 1 \end{cases}$

(ii). Balanced: $f(0) \neq f(1)$

i.e., $f(0)=0$, $f(1)=1$

or $f(0)=1$, $f(1)=0$

Let, $|0\rangle$ and $|1\rangle$ correspond to classical bits 0 and 1 respectively & consider the state

$$|\psi_0\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right)$$

Apply Oracle U_f to $|\psi_0\rangle$

$$|\psi_1\rangle = U_f \cdot |\psi_0\rangle$$

$$= \frac{1}{2}\left(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle\right)$$

$$= \frac{1}{2}\left(|0, f(0)\rangle - |0, f(\bar{0})\rangle \oplus |1, f(1)\rangle - |1, f(\bar{1})\rangle\right)$$

Apply Hadamard gate on the first qubit.

$$|\psi_2\rangle = (H \otimes I)(|\psi_1\rangle)$$

$$= \frac{1}{2\sqrt{2}}\left[(|0\rangle + |1\rangle)(|f(0)\rangle - |f(\bar{0})\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |f(\bar{1})\rangle)\right]$$

If f is constant, for which $f(0) = f(1)$ then

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle(|f(0)\rangle - |f(\bar{0})\rangle)$$

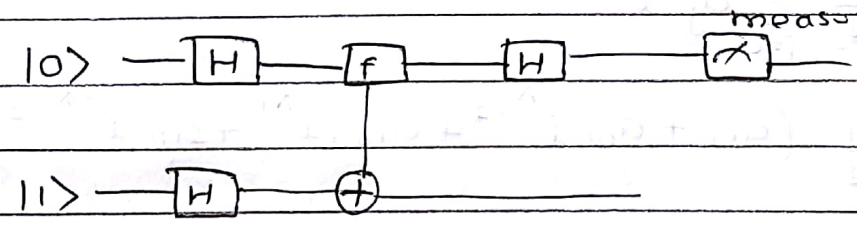
- function is constant if measurement of first qubit is $|0\rangle$.

If f is balanced, for which $|f(\bar{0})\rangle = |f(1)\rangle$

$$|\psi_2\rangle = \frac{1}{2\sqrt{2}}\left[(|0\rangle + |1\rangle)(|f(0)\rangle - |f(1)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |f(0)\rangle)\right]$$

$$= \frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |f(\bar{0})\rangle)$$

⇒ function is balanced if measurement of first qubit is $|1\rangle$



$$\frac{1}{2\sqrt{2}}\left[(|0\rangle + |1\rangle)(|f(0)\rangle - f(1)\rangle) + (|0\rangle - |1\rangle)(|f(1) - f(0)\rangle)\right]$$

$$|0\rangle.f|0\rangle - |0\rangle.f(1) + |1\rangle.f(0) - |1\rangle.f(1) + 0(f(1) - |0\rangle f(0) - |1\rangle.f(1) + |1\rangle.f(\bar{0})\rangle$$

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

$$= 1/\sqrt{2}\,|1\rangle.(|f(0)\rangle - |f(1)\rangle)$$

The Quantum Fourier Transform (QFT)

Definition: Given a general qubit state

$$|\psi\rangle = \sum_{j=0}^{N-1} a_j |j\rangle = \begin{pmatrix} a_0 \\ \vdots \\ a_{N-1} \end{pmatrix}$$

we define QFT of this state as,

$$F.|\psi\rangle = \sum_{k=0}^{N-1} b_k |k\rangle$$

where $b_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j . e^{2\pi i jk}$, $i = \sqrt{-1}$

Example of a QFT for 2 qubit

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

which has $N = 4$

we have,

$$b_0 = \frac{1}{2} \sum_{j=0}^{3} a_j = \frac{1}{2} (a_{00} + a_{01} + a_{10} + a_{11})$$

$$b_1 = \frac{1}{2} \sum_{j=0}^{3} a_j . e^{2\pi i j/4}$$

$$b_1 = \frac{1}{2} (a_{00} + a_{01} e^{\pi i/2} + a_{10} . e^{\pi i} + a_{11} . e^{3\pi i/2})$$

$$b_2 = \frac{1}{2} \sum_{j=0}^{3} a_j e^{\pi i j} = \frac{1}{2} (a_{00} + a_{01} e^{i\pi} + a_{10} e^{2\pi i} + a_{11} . e^{3\pi i})$$

$$b_3 = \frac{1}{2} \sum_{j=0}^{3} a_j . e^{\frac{3\pi i j}{2}} = \frac{1}{2} (a_{00} + a_{01} . e^{3i\pi/2} + a_{10} e^{3i\pi} + a_{11} . e^{4i\pi/2})$$

$e^{3i\pi}$

$\omega = e^{\pi i/2}$

$\omega^2 = e^{\pi i} = e^{3\pi i}$

Page No :

Date :

writing $\omega = e^{\pi i/2}$ & nothing that $\omega^4 = e^{2\pi i} = 1$

$(e^{i\theta} = \cos\theta + i\sin\theta)$

$\Rightarrow e^{2\pi i} = \cos(2\pi) + i.\sin(2\pi) = 1 + i0 = 1$

$e^{i\pi/2} = i = e^{9i\pi/2}$

we can write the 2 qu-bit QFT in matrix form

$$F = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & 1 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega \end{pmatrix}$$

$FF^+ = I$

$\Rightarrow$ F is Unitary

$$F = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$ //

1) Find QFT for N=4 of the function

$|f\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

$$F.|f\rangle = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$4\times4 \qquad 4\times1$

$$= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}_{4\times1}$$

2). Find QFT for $M=4$ of the function $|g\rangle = |00\rangle$

$$F.|g\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

3). Find QFT for $M=4$ of the function $|h\rangle = |01\rangle$

$$F.|h\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} & \\ & \\ & \\ & \end{pmatrix} =$$

The Inversal QFT

We have the matrix for 2 qubit QFT,

$$F = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Since F is unitary, then $F^{+}F = I \quad (F^{+} = (\bar{F})^{T})$

$$\Rightarrow F^{-1} = F^{+}$$

$$F^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Page No :
Date :

Quantum Error Correcting Code

Suppose we transmit a series of 0's & 1's through a noisy classical channel. Each bit is assumed to flip independently with a prob p.

How does classical error correction works?

The simplest example of classical error correction code is a repetition code.

We replace the bit we wish to protect by 3 copies of the bit

$$0 \rightarrow (000)$$
$$1 \rightarrow (111)$$

For example, when 000 is sent through this channel.

It will be received as 000 with probability $(1-p)^3$.

It will be received as 100, 010 or 001 with prob $3p(1-p)^2$.

It will be received as 011, 101 or 110 with prob $3p^2(1-p)$.

It will be received as 111 with prob p^3.

Note that the summation of all prob is 1 at it should.

By taking the majority vote, we correctly reproduce the desired result 0 with prob,

$$P_0 = (1-p)^3 + 3p(1-p)^2$$
$$= (1-p)^2(1+2p)$$

The prob of fail is,

$$P_1 = 3p^2(1-p) + p^3 = (3-2p)p^2.$$

Bit-Flip QECC

Suppose Alice wants to send a qubit, $|\psi\rangle = a.|0\rangle + b.|1\rangle$ to bob through a noisy quantum channel.

Let, p be the prob with which a qubit is flipped ($|0\rangle \leftrightarrow |1\rangle$) and we assume there are no other types of errors in the channel.

$$|\psi\rangle \rightarrow |\psi'\rangle = X.|\psi\rangle = a.|1\rangle + b.|0\rangle.$$