Quantum Information

GURUPRASAD KAR

Physics and Applied Mathematics Unit
Indian Statistical Institute
203 B.T. Road, Kolkata- 700108

1 Introduction

Some Basics of quantum mechanics

Starting from the begining of the 20th century some new things were appearing specially from the experiments involving quantum nature of light, spectrum analysis of different elements, interference phenomena for micro particles which were counterintuitive to the common sense shaped by classical ideas for years. To explain these new phenomena and to interpret the world of physics, the physicists were forced to adopt a new kind of mathematical formalism and rules in the arena of physics. Quantum mechanics is actually this set of mathematical rules which reproduces the physical theories.

System: In quantum mechanics, every system is associated with a Hilbert space H. For example, a Harmonic Oscillator is associated with the Hilbert space $L^2(-\infty, \infty)$, spin-$\frac{1}{2}$ particle with two dimensional complex Hilbert space, etc.

State: Quantum states are associated with positive trace class operators(with trace 1) on that Hilbert space. If ρ is a state, then $\rho \geq 0$ and $Tr[\rho] = 1$. ρ is called a pure state if $\rho^2 = \rho$. In this case ρ is a one dimensional projection operator i. e. $\rho = |\psi\rangle\langle\psi|$ for some vector $|\psi\rangle$. In the case of pure states, states are usually identified with the vector $|\psi\rangle$. For $\rho^2 \neq \rho$, the state is in general, called a mixed state. The set of states is convex.

State for qubits:

Any quantum system associated with two dimensional complex Hilbert space is referred as qubit. In general, as we have discussed earlier the state of a system in quantum mechanics is represented by positive normalized trace class operator. This is popularly known as density matrix. Now for a qubit (two level system), any operator can be written in terms of the basis operators (linear operaors acting on a Hilbert space form a Vector space) given by $I, \sigma_x, \sigma_y, \sigma_z$ where σ's are popularly known as Pauli matrices. The density matrix (ρ, say) in particular are represented by

$$\rho = \frac{1}{2}[I + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z]$$

where $a_i (i = x, y, z)$'s are real and $\Sigma|a_i|^2 \leq 1$.

In short this can also be written as

$$\rho = \frac{1}{2}[I + a.\sigma]$$

where a is a vector with components a_i and the notation $r.\sigma$ means $\Sigma r_i \sigma_i$.

So there is a one to one correspondence between single qubit states and points in the Poincare sphere. For $\Sigma |a_i|^2 = 1$, the state become pure which is represented by points on the surface of the Poincare sphere.

Observable: Observable (measurable quantities like position momentum, spin) are associated with self adjoint operators on the Hilbert space.

Consider a linear self adjoint operator A. Being self adjoint, $A = A^\dagger$. Then the eigen values $\{a_i\}$ of A are real. The set of eigen vectors $\{|\psi_i\rangle, A|\psi_i\rangle = a_i|\psi_i\rangle\}$ from an orthonormal basis for the Hilbert space. The operator A can be expressed as (also called spectral representation) $A = \Sigma a_i P_i$, P_i being projection operator. For non-degenerate eigenvalue a_r, the corresponding projection operator P_r is one dimensional and is given by $P_r = |\psi_r\rangle\langle\psi_r|$, and for degenerate eigen values the subspace corresponding to projection operator will have dimension equal to the degree of degeneracy.

Measurement Rule:

1. Measurement result is always one of the eigen value.

2. **Born Rule:** If a state is prepared in a state ρ (with $Tr\rho = 1$) and measurement of an observable A with spectral representation $A = \Sigma a_i P_i$, is performed on the system, then the probability that the measurement result is a_i is given by $Tr[\rho P_i]$. In the case when the state is pure like $\rho = |\psi\rangle\langle\psi|$, the corresponding probability becomes $\langle\psi|P_i|\psi\rangle$.
One should note that if the considered observable is B instead of A, having spectral representation $B = \Sigma b_i P_i$ (which involves same set of projection operators as A and $a_i \neq b_i$), then also the probability of the result b_i for B measurement on the state ρ is given by $Tr[\rho P_i]$. So the probability does not depend on the eigenvalues. Rather it depends on the projection operators present in the

spectral representation. So measurement represents partition of Identity matrix in terms of projection operator. Different measurements in quantum mechanics mean partition of Indentity in terms of different set of projectors. When all the P_i's are one dimensional projection operator i.e. $P_i = |\psi_i\rangle\langle\psi_i|$ for all i, we can characterize the measurement by referring only the basis vectors on which the projectors are defined.

3. **Collapse postulate:** If after the measurement the result is a_i, then the final state will be

$$\rho_i = \frac{P_i \rho P_i}{Tr[P_i \rho]}$$

Unitary dynamics: The future development of a state is given by the unitary dynamics where the unitary operator U ($UU^\dagger = U^\dagger U = I$)is determined by the Hamiltonian acting on the system.The dynamical equation is given by

$$\rho(t) = U(t, t_0)\rho(t_0)U(t, t_0)^\dagger$$

For pure state $\rho(t_0) = |\psi(t_0)\rangle\langle\psi(t_0)|$, the dynamics can also be expressed in terms of the state vector $|\psi(t)\rangle = U(t, t_0)|\psi(t_0)\rangle$

Description of Joint system:

1. Consider two system S_1 and S_2 associated with the Hilbert space H_1 and H_2 respectively. The joint system $S_1 + S_2$ is described by the Tensor product Hilbert space $H_1 \otimes H_2$.
2. Consider a density operator $\rho_{12}$for joint system $S_1 + S_2$. Now if some observable A (say) is measured on system S_1 alone, the expectation value is obtained by

$$\langle A \rangle_{S_1} = Tr[A \otimes I \rho_{12}] = Tr_{S_1}[A \rho_1]$$

where ρ_1 is called marginal density matrix for system S_1 and is given by

$$\rho_1 = Tr_{S_2}[\rho_{12}]$$

.

The state of a two qubits system can be written in a operator basis having 16 members ($I \otimes I$, $I \otimes \sigma_i$, $\sigma_i \otimes I$, $\sigma_i \otimes \sigma_j$, $i, j = x, y, z$). Explicitly a state of a two qubit system can be written as

$$\rho_{12} = \frac{1}{4}[I_1 \otimes I_2 + I_1 \otimes (r.\sigma)_2 + (s.\sigma)_1 \otimes I_2 + \Sigma t_{ij}(\sigma_i)_1 \otimes (\sigma_j)_2]$$

where r and s represents two vectors characterizing the marginal state of each qubit. One can easily calculate the marginal density matrix for particles 1 and 2 as $\rho_1 = Tr_2[\rho_{12}] = \frac{1}{2}[I + s.\sigma]$ and $\rho_2 = Tr_1[\rho_{12}] = \frac{1}{2}[I + r.\sigma]$

General quantum operation: In general there is no quantum mechanical operation by which one can violate the principle of causality. In quantum mechanics, the dynamics of a closed system is described by Unitary transformations which is expressed by Schrodinger equation. Then in a natural way the dynamics of an open system should be described by Unitary interaction on the system of interest and its environment which together again form a closed system. Now if we are interested in the dynamics of the system only, we will have to ignore the environment after the Unitary interaction which mathematically means performing partial trace over the environment to obtain the reduced state of the system alone.

$$T(\rho_{sys}) = Tr_{env}[U(\rho_{sys} \otimes \rho_{env})U^{\dagger}]$$

From the above , it clearly follows that T is a physical operation. But surprisingly all possible (trace preserving) physical operations

on the system can be obtained in the above way. Mathematically these are characterized by linear completely positive (CP) maps. A map T is said to be completely positive if T maps (by acting on one system A)every density matrix (which is by definition, positive operator) defined on a joint system A and B to another valid density matrix, whatever be the dimension of Hilbert space corresponding to system B. According to Kraus representation theorem any trace preserving CP map *i.e* general quantum mechanical operation can also be expressed in a very useful form;

$$T(\rho) = \sum_k A_k \rho A_k^\dagger$$

where A_k is some set of operator with $\sum_k A_k^\dagger A_k = I$ (Unit operator).

2 Existence of non-orthogonal states

Nonorthogonality has important physical consequences.

Consider the set of states $\{|\psi_z\rangle, |\psi_{-z}\rangle\}$

If a particle is prepared in one of these states, can one determine the state?

The answer is obviously yes as measurement of σ_z will answer it.

But if the set is
$\{|\psi_z\rangle, |\psi_x\rangle\}$
Then the answer is not so obvious.

In this case measurement of σ_z will determine the state

probabilistically.

If the result is up, one can not tell.

If the result is down, then the state must have been $|\psi_x\rangle\}$

The question is whether there is some good measurement which would answer deterministically has to be answered.

We shall answer the question from a more powerful theorem in quantum mechanics.

Suppose $|\Psi\rangle$ and $|\Phi\rangle$ are two nonorthogonal states i.e. $\langle\Psi|\Phi\rangle \neq 0$.

Let there is a machine along with a blank state which can clone these two states.

So there must be a unitary operator U (This must be the most

general physical operation on the system and blank state as there is no restriction on the dimension of Hilbert space associated with the machine system) such that

$$U|\Psi\rangle \otimes |0\rangle \otimes |M\rangle = |\Psi\rangle \otimes |\Psi\rangle \otimes |M_1\rangle$$

$$U|\Phi\rangle \otimes |0\rangle \otimes |M\rangle = |\Phi\rangle \otimes |\Phi\rangle \otimes |M_2\rangle$$

where $|0\rangle$ and $|M\rangle$, $|M_1\rangle$, $|M_2\rangle$ are blank state, initial machine state and final machine states corresponding to cloning of two different states respectively.

Takeing scaler product of both side

$$\langle\Psi|\Phi\rangle = \langle\Psi|\Phi\rangle^2\langle M_1|M_2\rangle$$

Now this can be true only when $\langle\Psi|\Phi\rangle = 1$ or 0 .

So two different states can be cloned only when they are orthogonal.

From this result it also follows that two nonorthogonal states can not distinguished with certainty. This can simply be proved in the following way. On the contrary, we assume that two nonorthogonal states can be discriminated with certainty. Then even if the states are destroyed in the process of knowing it, one can prepare as many copies of the state as he wants because now he knows the state. But this would imply exact cloning of nonorthogonal states. A contradiction.

b. Non unique decomposition of mixed state

Every density matrix, in general, can be written as convex combination of pure states. Being positive operator, the spectral representation of the density operator will be one such example. But interestingly, a density matrix can be written as convex combination of pure states in infinitely many ways.

Example

1. In two dimensional Hilbert space the state $\frac{1}{2}I$ (I being the Identity operator on two dimensional Hilbert space) can be written as

$$\frac{1}{2}I = \frac{1}{2}|\psi_z\rangle\langle\psi_z| + \frac{1}{2}|\psi_{-z}\rangle\langle\psi_{-z}| = \frac{1}{2}|\psi_x\rangle\langle\psi_x| + \frac{1}{2}|\psi_{-x}\rangle\langle\psi_{-x}|$$

where the orthogonal set $\{|\psi_z\rangle, |\psi_{-z}\rangle\}$ and $\{|\psi_x\rangle, |\psi_{-x}\rangle\}$ are eigen vector of Pauli matrix σ_z and σ_x respectively.

2.

$$\rho = p|\psi_z\rangle\langle\psi_z| + (1-p)|\psi_{-z}\rangle\langle\psi_{-z}|$$

with $p \neq \frac{1}{2}$.

Then this density matrix can be expressed as convex combination of two non-orthogonal states
$|R\rangle$ and $|L\rangle$;

$$\rho = \frac{1}{2}|R\rangle\langle R| + \frac{1}{2}|L\rangle\langle L|$$

where

$$|R\rangle = \sqrt{p}|\psi_z\rangle + \sqrt{1-p}|\psi_{-z}\rangle$$

$$|L\rangle = \sqrt{p}|\psi_z\rangle - \sqrt{1-p}|\psi_{-z}\rangle.$$

3. Consider any normalized qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$, Then the density matrix $\frac{1}{2}I$ can be expressed as

$$\frac{1}{2}I = \frac{1}{4}[|\psi\rangle\langle\psi| + \sigma_x|\psi\rangle\langle\psi|\sigma_x + \sigma_y|\psi\rangle\langle\psi|\sigma_y + \sigma_z|\psi\rangle\langle\psi|\sigma_z]$$

This is an outstanding result and will be very useful in quantum teleportation.

c. Existence of entangled states:

Let ρ_{AB} is a state for the joint system A and B. Then ρ_{AB} is a entangled state if it can not be written as

$$\rho_{AB} = \Sigma\omega_i {\varrho_A}^i \otimes {\varrho_B}^i$$

for any choice of $\{{\varrho_A}^i\}$ and $\{{\varrho_B}^i\}$ for subsystems A and B respectively. For special case of a pure state, the state is entangled if the vector can not be written as product vector. For example one can check that the vector

$$|\Theta_{sing}\rangle_{AB} = \frac{1}{\sqrt{2}}[|\Psi\rangle_A \otimes |\bar{\Psi}\rangle_B - |\bar{\Psi}\rangle_A \otimes |\Psi\rangle_B]$$

$|\bar{\Psi}\rangle$, $|\Psi\rangle$ being orthogonal, can not be written as a product vector

$$|\phi\rangle_A \otimes |\theta\rangle_B$$

for any $|\phi\rangle$ and $|\theta\rangle$ for system A and B respectively.

3 Shmidt Decomposition theorem

Consider two systems

A and B associated with Hilbert space H_A of dimension d_A and H_B of dimension d_B respectively.

Consider orthogonal basis $\{|\alpha_i\rangle\}_{i=1}^{d_A}$ for H_A and $\{|\beta_j\rangle\}_{j=1}^{d_B}$ for H_B.

Then $\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$ form a orthogonal basis for the Hilbert space $H_A \otimes H_B$.
Then any vector $|\psi\rangle_{AB}$ in $H_A \otimes H_B$ can be expressed as

$$|\psi\rangle_{AB} = \sum_{i,j} C_{ij} |\alpha_i\rangle \otimes |\beta_j\rangle$$

But Schimdt decomposition theorem says that any pure state $|\psi\rangle_{AB}$ of the composite system can be expressed as

$$|\psi\rangle_{AB} = \sum_{i=1}^{r} \sqrt{\lambda_i} |a_i\rangle \otimes |b_i\rangle$$

where $\{|a_i\rangle\}$ and $\{b_i\rangle\}$ are orthonormal basis for system A and B respectively and $r \leq Min\{d_A, d_B\}$.

The proof goes as follows.

Let the marginal density matrix of the system A is ρ_A
where

$$\rho_A = Tr_B[|\psi\rangle_{AB}\langle\psi|]$$

ρ_A being a self adjoint operator will have a spectral representation of the form

$$\rho_A = \sum_{k=1}^{m} \lambda_k |a_k\rangle\langle a_k|$$

Write $|\psi\rangle_{AB}$ using basis$\{|a_k\rangle\}$ as

$$|\psi\rangle_{AB} = \sum_k |a_k\rangle_A \otimes |\phi_k\rangle_B$$

where in general $\{|\phi_k\rangle_B\}$ are neither orthogonal nor normalized.

Again calculate ρ_A from this expression which will be

$$\rho_A = \sum_{kl} \langle \phi_l | \phi_k \rangle |a_k\rangle\langle a_l|$$

Comparing with early expression of ρ_A we get

$$\langle \phi_l | \phi_k \rangle = \lambda_k \delta_{kl}$$

So if we rewrite $|\phi_k\rangle$ as

$$|\phi_k\rangle = \sqrt{\lambda_k}|b_k\rangle$$

we get the result of the theorem.

4 GHJW theorem

Objectively real internal properties of an isolated individual system should not change when something is done to another non-interacting system.

Consider the singlet state of two qubits which can be written in the following two representations

$$|\Theta_{sing}\rangle_{AB} = \frac{1}{\sqrt{2}}[|\psi_z\rangle_A \otimes |\psi_{-z}\rangle_B - |\psi_{-z}\rangle_A \otimes |\psi_z\rangle_B]$$

$$|\Theta_{sing}\rangle_{AB} = \frac{1}{\sqrt{2}}[|\psi_x\rangle_A \otimes |\psi_{-x}\rangle_B - |\psi_{-x}\rangle_A \otimes |\psi_x\rangle_B]$$

Now if one measures σ_z on qubit A, qubit A will collapse either on $|\psi_z\rangle_A$ or on $|\psi_{-z}\rangle_A$, both with probability $\frac{1}{2}$. So due to (anti) correlation, the qubit B will also collapse on $|\psi_{-z}\rangle_B$ or $|\psi_z\rangle_B$ with

equal probability.
So the density matrix in the z- representation of qubit B can be prepared by acting on system A.
But due to the symmetry, acting on qubit A i.e. measuring σ_x on qubit A, same density matrix in the x-representation can also be prepared.

Now if one assumes that there is an objective difference between these two representations violating the assertion, then that difference can be used to send some information (encoded in the direction of spin measurement on qubit A) instantaneously as qubits A and B can be put light years away preparing in singlet state.

If one thinks that the above result holds due to degeneracy of the density matrix $\frac{1}{2}I$ and may not hold for other representations like in example 2., then one can see the following two expansions of the same entangled state;

$$|\Psi\rangle = \sqrt{p}|\psi_z\rangle \otimes |\psi_z\rangle + \sqrt{1-p}|\psi_{-z}\rangle \otimes |\psi_{-z}\rangle$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}[|R\rangle \otimes |\psi_x\rangle - |L\rangle \otimes |\psi_{-x}\rangle]$$

So measurement of spin in the z-direction and x-direction on second qubit will prepare the first and second representation respectively.

Actually every mixed density matrix has infinitely many representation and there is a theorem due to GHJW which tells that every representation of a density matrix can be produced for a system by acting on different non-interacting system (whose associated Hilbert space has infinite dimension) by a single suitable choice of an entangled state of the joint system.

Proof of GHJW theorem :

Consider a spectral representation of density matrix ρ_A *i.e*

$$\rho_A = \sum_i p_i |\eta_i\rangle\langle\eta_i|, \qquad \sum p_i = 1$$

Where $\{|\eta_i\rangle's\}$ are orthogonal to each other. ρ_A can be realized as ensemble in which each pure state $|\eta_i\rangle\langle\eta_i|$ occurs with probability p_i. If ρ_A is not degenerate then it's spectral representation is also unique. Now Bob can remotely prepare this ensemble in the following way:

Let Alice and Bob are sharing a bipartite pure entangled state

$$|\phi_1\rangle_{AB} = \sum_i \sqrt{p_i}|\eta_i\rangle_A \otimes |\alpha_i\rangle_B$$

where the vector $|\alpha_i\rangle_B \in H_B$ are mutually orthogonal and normalized. Now a measurement $|\alpha_i\rangle_B$ basis in system B will prepare the density matrix $\rho_A == \sum_i p_i|\eta_i\rangle\langle\eta_i|$ for the system A. $|\phi_1\rangle_{AB}$ is called purification of ρ_A.
Consider any other probabilistic mixture of the same density matrix

$$\rho_A = \sum_\mu q_\mu |\psi_\mu\rangle\langle\psi_\mu|, \qquad \sum q_\mu = 1$$

Where $\{|\psi_\mu\rangle's\}$ are not orthogonal in general. Then one can have the corresponding purification for this ensemble

$$|\phi_2\rangle_{AB} = \sum \sqrt{q_\mu}|\psi_\mu\rangle_A \otimes |\beta_\mu\rangle_B$$

where again$\{|\beta_\mu\rangle'_B s\}$ are orthonormal vector in H_B.

Again by performing orthogonal measurement in $|\beta_\mu\rangle_B$ basis in B system , above ensemble can be prepared for system A.
But the Schmidt decomposition of $|\phi_2\rangle_{AB}$ must have the form

$$|\phi_2\rangle_{AB} = \sum \sqrt{p_i}|\eta_i\rangle_A \otimes |\xi_i\rangle_B$$

where the vector $|\xi_i\rangle_B \in H_B$ are mutually orthogonal and normalized, as it has to reproduce the correct reduced density matrix for A. Let us now define a Unitary operator U such that $U|\alpha_i\rangle = |\xi_i\rangle$, then

$$|\phi_1\rangle_{AB} = I \otimes U|\phi_2\rangle_{AB}$$

Thus we have seen that starting from a single purification ($|\phi_1\rangle_{AB}$, say) Bob can prepare any representation leading to the same density matrix for Alice by the proper choice of Unitary operator and measurement basis.

Introduction: We now scan some of the applications of the quantum laws in new area of quantum information. But again one should be careful about in what sense quantum laws enters into information theory. Long before the birth of quantum information, quantum physics had been used to understand better, and thus improve existing technology. For example, the development of smaller and faster Silicon or other semiconductor devices benefits from the understanding of the quantum behaviour of electrons in such metals.

Here we enter into information theory in a different way. Instead of improved versions of what we already have, consider devices which actually process information and perform logical operations according to the laws of quantum mechanics. Such devices, which would be part of new quantum information technology will be fundamentally different from their classical counterparts.

5 Quantum cryptography

The most simple but very powerful application of quantum laws in information processing is the area of cryptography.
The aim of cryptography is secret information exchange between two parties, so that any attempt of eavesdropping message or breaking the code would be unsuccessful.
Schematically things can be put in the following way.
Let P be the message $E_K(P) = C$ (cryptotext)
where the encrypton operation E_K produce the cryptotext using the key K, only known to sender and receiver.
C is sent to Bob.
$D_K(C) = P$
where D_K is the decrypton operation reproducing the original message.
In this scenario if K remains secret, message remains safe.

Example:

The message (P): 0 1 1 0 1

The key (K): 1 1 0 0 1

Alice encrypts the message by ($C_i = P_i + K_i \bmod 2$):

$0\ 1\ 1\ 0\ 1 \bigoplus 1\ 1\ 0\ 0\ 1 = 1\ 0\ 1\ 0\ 0$ (cryptotext, C)

Bob decrypts the message by addition modulo 2:

$1\ 0\ 1\ 0\ 0 \bigoplus 1\ 1\ 0\ 0\ 1$

$= 0\ 1\ 1\ 0\ 1$ (message, P)

Now if the sender and receiver meet and agreed on a key before going apart, they can safely send message later using that key. Now the question remains how to generate the secret key when Alice and Bob are far away?

In principle, any private classical channel can be monitored passively, without the sender and receiver knowing that the eavesdropping has taken place. For example, a key carried by a trusted courier might have been read en route by a surreptitious high-resolution X-ray scan or other sophisticated imaging technique without the courier's knowledge. Since all information, including a cryptographic key, is encoded in measurable physical properties of some object or signal, classical theory leaves open the possibility of passive eavesdropping, because it allows eavesdropper in principle to measure physical properties without disturbing them.

But this fundamental problem in cryptography can be solved by using quantum system and quantum laws. In the process of generating the secret key if the information about the key are encoded in states of a quantum system then that message can not be cloned or deciphered as unknown quantum state can neither be cloned nor determined. If a eavesdropper try some measurements on the quantum system he will irreversibly change the state and will be caught when the sender and receiver compare their result.

Secure quantum key generation protocol :

Let us study the simplest secret key generation protocol provided by Bennett et.al. in 1984. Let Alice and Bob are two distant parties who have been provided the facility of public communication as well as transportation of physical system like a spin-1/2 system or a polarized photon. Now we describe the steps to be taken by them to generate the key as well as detect the eavesdropper if any.

Step-1 Alice picks up a spin-1/2 particle prepared in one of the sates $|\Psi_z\rangle$, $|\Psi_{-z}\rangle$, $|\Psi_x\rangle$ and $|\Psi_{-x}\rangle$ where first two are eigen states of σ_z representing spin measurement in the z-diection and the last two are eigen states of spin observable $\sigma_x$for x-direction, and send them to Bob one by one.

Step-2 Bob randomly choses spin measurement either in the z-direction or in the x-direction.

Step-3 Bob records his bases and the result of spin measurement.

Step-4 Bob announces his bases publicly
but not the result of his measurement

Step-5 Alice tells Bob in which cases Bob choses the correct basis. They discard the results when their bases are different and keep the rest.

Let their assignment of bit value (0, 1) is like this;
$(|\Psi_{\rangle},|\Psi_x\rangle) \mapsto 0$
$(|\Psi_{-z}\rangle,|\Psi_{-x}\rangle) \mapsto 1$
Then they have generated the key.

Alice	$\|\Psi_z\rangle$	$\|\Psi_{-z}\rangle$	$\|\Psi_x\rangle$	$\|\Psi_z\rangle$	$\|\Psi_{-x}\rangle$	$\|\Psi_x\rangle$	$\|\Psi_{-z}\rangle$
Bob's basis	X	Z	X	X	Z	X	Z
Bob's result	$\|\Psi_x\rangle$	$\|\Psi_{-z}\rangle$	$\|\Psi_x\rangle$	$\|\Psi_{-x}\rangle$	$\|\Psi_z\rangle$	$\|\Psi_x\rangle$	$\|\Psi_{-z}\rangle$
Alice's message	$\times$	$\surd$	$\surd$	$\times$	$\times$	$\surd$	$\surd$
Raw key		1	0			1	0

From the table one can see how the key is generated where Alice sends 7 qubits one by one and Bob performs spin measurement randomly in one of the bases.

Now let us consider what happens when some eavesdropper try to intervene to get the information about the key. One should note that the four states that Alice sends are linearly depended set and hence Eve can not either clone them or discriminate among them even probabilistically. Still if Eve intervenes by performing spin measurement in one of the bases (X or Z) he can be caught if Alice and Bobcompares some of their result. This is due the disturbance introduced by the measurement which is in no away unavoidable. Let us consider the example;

$\|\Psi_z\rangle$	$\rightarrow$	X	$\rightarrow$	$\|\Psi_x\rangle$	$\rightarrow$	Z	$\rightarrow$	$\|\Psi_{-z}\rangle$
Alice		*Eve's basis*		*Eve's result*		*Bob's basis*		*Bob's result*

where Alice sends the particle in the state $|\Psi_z\rangle$, Eve intervenes be making measurement in the X-basis and the state collapses to $|\Psi_x\rangle$ (which has a 50 percent probability). After getting the particle let Bob measures it in the correct basis i.e. in the Z- basis. Then again there is a 50 percent probability that the state collapses to $|\Psi_{-z}\rangle$ which is orthogonal to what Alice sends. So in such cases error will be introduced by Eve's intervention. So it is obvious that If Alice and Bob compare some of their results when they have chosen the same basis, they would easily learn whether someone is monitoring the channel.

EPR protocol:

In EPR key generation protocol Alice and Bob share a singlet state of two qubit, each holding one qubit. We can write the singlet state as

$$|\Theta_{sing}\rangle = \frac{1}{\sqrt{2}}[|\Psi_z\rangle_A \otimes |\Psi_{-z}\rangle_B - |\Psi_{-z}\rangle_A \otimes |\Psi_z\rangle_B]$$

But the singlet state can also be written as

$$|\Theta_{sing}\rangle = \frac{1}{\sqrt{2}}[|\Psi_x\rangle_A \otimes |\Psi_{-x}\rangle_B - |\Psi_{-x}\rangle_A \otimes |\Psi_x\rangle_B]$$

In this protocol in the first step Alice and Bob perform spin measurement either in the Z-basis or in the X-basis randomly. In the second step, they compare their chosen basis and discard the cases when basis are not same.

Then they keep the rest of the result and assign the bit in the following way;

For Alice

$(|\Psi_z\rangle, |\Psi_x\rangle) \mapsto 0$

$(|\Psi_{-z}\rangle, |\Psi_{-x}\rangle) \mapsto 1$

For Bob

$(|\Psi_z\rangle, |\Psi_x\rangle) \mapsto 1$

$(|\Psi_{-z}\rangle, |\Psi_{-x}\rangle) \mapsto 0$

As their results are anticorrelated, they will generate the same key.

One can easily check that the singlet state is a eigen state of both $\sigma_z \bigotimes \sigma_z$ and $\sigma_x \otimes \sigma_x$ with eigen value -1. So the result of spin measurement in the same direction on both will remain strictly (anti)correlated.

Now if any eavesdropper intercepts one or both the particles and performs some measurement it will break the EPR correlation and collapse it to a product state.

Now there is a theorem (Horodecki, PLA, 210,(1996)227) which tells that if there are more than one pair of axes along which spin measurements of two qubits are either correlated or anti-correlated, then possible states of two qubits are $U_1 \otimes U_2$ isomorphic to the singlet state. So there can not be any pure product state for which the results of spin measurements along both z direction and x direction can be anti-correlated. From this result it is obvious that if Alice and Bob compare some of their preserved results (when they measure along same directions) publicly they be able to know whether there is some eavesdropper acting on the channel.

Alternative proof of security in both the protocol

Let in the BB-84 protocol, Eve gets hold of the qubit and makes it interact with an auxiliary quantum system, to be measured afterwards with the aim of knowing the secret key and then send the original qubit to Bob. Let $|a\rangle$ be the state of the auxiliary system and U be the unitary operation which leaves just two non-orthogonal states $|\Psi_z\rangle$ and $|\Psi_x\rangle$ undisturbed so that his intervention remains undetected. Then

$$U|\Psi_z\rangle \otimes |a\rangle = |\Psi_z\rangle \otimes |a_z\rangle$$

$$U|\Psi_x\rangle \otimes |a\rangle = |\Psi_x\rangle \otimes |a_x\rangle$$

If the two states $|a_z\rangle$ and $|a_x\rangle$ are different, the auxiliary system has extracted some information about the state keeping the original states undisturbed and thus Eve will remain undetected.

Now if we take the scaler product of both sides, we get

$$\langle \Psi_z | \Psi_x \rangle = \langle \Psi_z | \Psi_x \rangle \langle a_z | a_x \rangle$$

Since $\langle \Psi_z | \Psi_x \rangle \neq 0$,

$$\langle a_z | a_x \rangle = 1$$

.

So Eve's state has to remain same to escape detection.

The only attack that avoids detection is one that yields no information. *This shows another fundamental point (more powerful than no-cloning theorem) that without disturbing the system no information about the states can be obtained if the states are non-orthogonal*.

Now we consider the case of EPR protocol. We assume the extreme case of intervention by Eve where he supplies the EPR pair to Alice and Bob who will generate the secret key. So Eve can cause one or both the particles to interact coherently with an auxiliary system, to be measured afterwards. The most general entangled state that Eve can prepare is of the form

$$|\Phi\rangle_{ABE} = |\Psi_z\rangle_A \otimes |\Psi_z\rangle_B \otimes |A\rangle_E + |\Psi_{-z}\rangle_A \otimes |\Psi_{-z}\rangle_B \otimes |B\rangle_E$$

$$+|\Psi_z\rangle_A \otimes |\Psi_{-z}\rangle_B |C\rangle_E + |\Psi_{-z}\rangle_A \otimes |\Psi_z\rangle_B \otimes |D\rangle_E$$

If $|A\rangle_E$, $|B\rangle_E$, $|C\rangle_E$ and $|D\rangle_E$ are orthogonal then Eve can know completely the result of measurement in the Z-basis done by Alice and Bob.

But if Eve's tampering is to escape detection, the state $|\Phi\rangle_{ABE}$ must be eigen state of $\sigma_z \bigotimes \sigma_z \bigotimes I$ with eigen value -1. To meet this constraint $|\Phi\rangle_{ABE}$ has to be of the form

$$|\Phi\rangle_{ABE} = |\Psi_z\rangle_A \otimes |\Psi_{-z}\rangle_B \otimes |A\rangle_E + |\Psi_{-z}\rangle_A \otimes |\Psi_z\rangle_B \otimes |D\rangle_E$$

but again $|\Phi\rangle_{ABE}$ has to be eigen state of $\sigma_x \bigotimes \sigma_x \bigotimes I$ with eigen value -1. This further restriction forces Eve to prepare the state in the form

$$|\Phi\rangle_{ABE} = [|\Psi_z\rangle_A \otimes |\Psi_{-z}\rangle_B \otimes -|\Psi_{-z}\rangle_A \otimes |\Psi_z\rangle_B] \otimes |K\rangle_E$$

$$= |\Theta_{sing}\rangle_{AB} \otimes |K\rangle_E$$

So Eve's system becomes completely uncorrelated if he has to evade detection. *It also shows that if two qubits are maximally correlated (a pure entangled state where the subsystem's states are $\frac{1}{2}I$,I being an unit operator) , then they can in no way be correlated (either quantum mechanically or classically) with a third system.*

6 Quantum dense coding

We have seen that for a single qubit, only two orthogonal states can be distinguished. If one is supplied a state from a set of three states of a qubit, the state can not be determined even probabilistically as they are linearly dependent. So with a qubit we can encode only one bit (either 0 or 1) of information to be used later. Although there are infinite possible states for a qubit we can not use them for coding more information. So Alice can transfer one bit of information to Bob by physically transferring a qubit to Bob.
So in this respect two level classical system and two level quantum system are no different. Similarly two classical bits of information can be sent using two qubits or two two-level classical system. let us consider a cricket match to be played between India and Pakistan. Alice is supposed to watch the match and allowed to send two level classical system (for example ball either coloured red

or blue)or quantum system for communicating the result of the match to Bob. The encoding may be done as follows;
India won $\rightarrow$ RR
India lost $\rightarrow$ BB
Match drawn $\rightarrow$ RB
Match abandoned $\rightarrow$ BR

Similarly encoding may be done by quantum system replacing red ball by qubit in state $|\Psi_z\rangle$ and blue ball by qubit in state $|\Psi_{-z}\rangle$. Now let us consider a situation where Alice will be allowed to send only one ball or one qubit after the match ends. So she can send one system earlier to Bob. Then is it possible to communicate the result of the match by using classical or quantum system in this situation? The result seems to be NO. But this is not true for quantum system.

Surprisingly in the case of quantum system, if Alice prepares a two qubit entangled state and send one qubit earlier even before deciding which message to be sent, Alice can still send two bits. This process is known as dense coding.
Let Alice and Bob share a maximally entangled state (one of the four Bell states)

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}[|\Psi_z\rangle_A \otimes |\Psi_z\rangle_B \otimes +|\Psi_{-z}\rangle_A \otimes |\Psi_{-z}\rangle_B]$$

It is a nice result of quantum mechanics that all the four Bell states are connected by a unitary operation on one side. For example if Alice apply the unitary operation σ_z on her qubit the Bell state $|\Phi^+\rangle_{AB}$ changes to $|\Phi_-\rangle_{AB}$. Mathematically we can write

$$|\Phi_-\rangle_{AB} = \sigma_z \otimes I|\Phi^+\rangle_{AB}$$

$$|\Psi_+\rangle_{AB} = \sigma_x \otimes I|\Phi^+\rangle_{AB}$$

$$|\Psi_-\rangle_{AB} = \sigma_z\sigma_x \otimes I|\Phi^+\rangle_{AB}$$

Let us now describe the protocol; Alice encodes her two bits of information in her operation on the qubit in the following way;

India won $\rightarrow I$,
India lost $\rightarrow \sigma_z$,
Mathch drawn $\rightarrow \sigma_x$,
Match abandoned $\rightarrow \sigma_z\sigma_x$.

Alice encode her bit applying the proper operation on her qubit and then send the qubit to Bob.

So finally Bob gets two qubits and he performs a measurement in the Bell basis. After getting the result he decodes the information according to the following correspondence;

India won $\rightarrow |\Phi_+\rangle_{AB}$,
India lost $\rightarrow |\Phi_-\rangle_{AB}$,
Mathch drawn $\rightarrow |\Psi_+\rangle_{AB}$,
Match abandoned $\rightarrow |\Psi_-\rangle_{AB}$

So in this way two bits of information will be transferred by physically sending one qubit which again reveals the power of quantum correlation.

7 Quantum teleportation

To understand the teleportation process we start with the following ensemble representation of the density matrix $\frac{1}{2}I$;

$$\frac{1}{2}I = \frac{1}{4}[|\psi\rangle\langle\psi| + \sigma_x|\psi\rangle\langle\psi|\sigma_x + \sigma_y|\psi\rangle\langle\psi|\sigma_y + \sigma_z|\psi\rangle\langle\psi|\sigma_z]$$

Now GHJW theorem tell that this ensemble (for any $|\psi\rangle$) can be prepared by Alice on Bob's side by sharing appropriate pure entangled state. Now the density matrix on Bob's side being $\frac{1}{2}I$, the pure entangled state must be maximally entangled one. We describe two protocols for preparing this ensemble representation.
1) Alice and Bob share a singlet state. Alice tosses an unbiased coin and if the result is head she makes a measurement in the orthogonal basis $\{|\psi\rangle, \sigma_y|\psi\rangle\}$ and for tail she does the same in orthogonal basis $\{\sigma_x|\psi\rangle, \sigma_z|\psi\rangle\}$. In this way, the required ensemble is prepared.

2) Let Alice and Bob share the maximally entangled state given by

$$|\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}}[|\Psi_z\rangle_2 \otimes |\Psi_z\rangle_3 \otimes +|\Psi_{-z}\rangle_2 \otimes |\Psi_{-z}\rangle_3]$$

where Alice is holding the particle 2 and Bob is holding the particle 3.

Alice prepare another qubit in the state $|\psi\rangle$ which can be expressed in the basis $\{|\Psi_z\rangle_1, |\Psi_{-z}\rangle_1\}$ as

$$|\psi\rangle_1 = a|\Psi_z\rangle_1 + b|\Psi_{-z}\rangle_1$$

Now the state of all the three qubits can be written as

$$|\Upsilon\rangle_{123} = (a|\Psi_z\rangle_1 + b|\Psi_{-z}\rangle_1) \otimes |\Phi^+\rangle_{23}$$

If the joint states of the two particles on the Alice's side are written in the Bell basis, given by

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}[|\Psi_z\rangle_1 \otimes |\Psi_z\rangle_2 + |\Psi_{-z}\rangle_1 \otimes |\Psi_{-z}\rangle_2]$$

$$|\Phi^-\rangle_{12} = \frac{1}{\sqrt{2}}[|\Psi_z\rangle_1 \otimes |\Psi_z\rangle_2 - |\Psi_{-z}\rangle_1 \otimes |\Psi_{-z}\rangle_2]$$

$$|\Psi^+\rangle_{12} = \frac{1}{\sqrt{2}}[|\Psi_z\rangle_1 \otimes |\Psi_{-z}\rangle_2 + |\Psi_{-z}\rangle_1 \otimes |\Psi_z\rangle_2]$$

$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}[|\Psi_z\rangle_1 \otimes |\Psi_{-z}\rangle_2 - |\Psi_{-z}\rangle_1 \otimes |\Psi_z\rangle_2]$$

Then the state $|\Upsilon\rangle_{123}$ of the three qubits can be written as

$$
\begin{aligned}
&|\Upsilon\rangle_{123} \\
&= \frac{1}{2}[|\Phi^+\rangle_{12} \otimes (a|\Psi_z\rangle_3 + b|\Psi_{-z}\rangle_3)(= |\psi\rangle) \\
&+\frac{1}{2}|\Phi^-\rangle_{12} \otimes (a|\Psi_z\rangle_3 - b|\Psi_{-z}\rangle_3)(= \sigma_z|\psi\rangle) \\
&+\frac{1}{2}|\Psi^+\rangle_{12} \otimes (a|\Psi_{-z}\rangle_3 + b|\Psi_z\rangle_3)(= \sigma_x|\psi\rangle \\
&+\frac{1}{2}|\Psi^-\rangle_{12} \otimes (a|\Psi_{-z}\rangle_3 - b|\Psi_z\rangle_3)(= \sigma_y|\psi\rangle)
\end{aligned}
$$

Now one can easily see that if Alice makes a measurement in the Bell basis on qubits 1 and 2, she will be preparing the required ensemble for the density matrix $\frac{1}{2}I$ on Bob's side.
But one should note that in the first protocol, Alice has to learn the state $|\psi\rangle$ for performing the measurement, but in the second one as her measurement basis is independent of $|\psi\rangle$, she can

produce the ensemble even without knowing $|\psi\rangle$ if only a qubit is supplied in the state $|\psi\rangle$ to her. This is the essential thing which makes teleportation scheme possible.
Now The teleportation protocol can be described in the following way;

1) Upon receiving the qubit in the unknown state Alice performs projective measurements on her two qubits in the Bell basis. this means that she will obtain one of the four Bell states randomly and with equal probability.

2) After getting the result Alice will inform it to Bob.

3) Bob will perform some unitary operation on his qubit depending on the result of Alice and gets the state to be teleported.

The correspondence is like this;
If Alice gets $|\Phi^+\rangle_{12}$ Bob does nothing. If Alice gets $|\Phi^-\rangle_{12}$, Bob applies the unitary operation σ_z on his qubit, if Alice gets $|\Psi^+\rangle_{12}$, Bob applies σ_x and if Alice gets $|\Psi_-\rangle_{12}$, Bob first apply σ_x and then apply σ_z. One can easily see that this unitary transformation does not any way depend on the unknown parameter a and b, So this is an universal protocol to teleport any unknown state of a qubit.
The important features of quantum teleportation to be noted are
(i) Two classical bits of information are required to inform Alice's measurement result to Bob.
(ii) After the teleportation the entangled channel i.e. the maximal quantum correlation between Alice and Bob are totally destroyed.
(iii) On the Alice's side the state of the two particles is one of the maximally entangled state and hence no remnant
of information about the teleported state remains on the Alice's side.

Is entangled channel necessary for quantum teleportation?

Let us assume that there is a classically correlated state between Alice and Bob by which quantum state can be teleported by using local operations and classical communications. Let the classically correlated state is given by

$$\Omega_{12} = \Sigma\lambda_i(\gamma_i)_1 \otimes (\pi_i)_2$$

where Alice holds the particle 1 and Bob holds the particle 2, and $(\gamma_i)_1$ and $(\pi_i)_2$ are density matrices for particles of 1 and 2 respectively. As assumed, if this state is used as channel any quantum state can be teleported by using some local protocol. Now interestingly there exists a three-particles state for which particle 1 has same classical correlation with particle 3 as it had with particle 2. Such state can easily be constructed as

$$\Gamma_{123} = \Sigma\lambda_i(\gamma_i)_1 \otimes (\pi_i)_2 \otimes (\pi_i)_3$$

If one consider only the state of 1 and 2 by tracing out 3 we get Ω_{12} and by tracing out 2 we get Ω_{13}. So the party who is holding the particle 3 can follw the teleportation protocol like Bob and there is nothing to debar him to get the teleported state like Bob. But then a single quantum state would appear in two places which means cloning of an unknown quantum state has been possible. This is a contradiction.

Why two classical bit is necessary in quantum teleportation

In quantum teleportation we have seen that Alice the sender makes a projective measurement in the bell basis and has to classically inform Bob which one of the four Bell states she has got. This needs two classical bits of information. Now the question is whether there can be other teleportation protocol which will need less no. of classical bits. We show that this is impossible.
Let Alice and Bob share two maximally entangled state $|\Phi^+\rangle_{12}$ and

$|\Phi^+\rangle_{34}$ where Alice holds the particle 1 and 3 and Bob holds the particle 2 and 4. Now they decide to use the state $|\Phi^+\rangle_{12}$ for quantum dense coding. For that Alice has to send the particle 1 to Bob physically. But now as they share another maximally entangled state $|\Phi_+\rangle_{34}$ they can use it for teleporting the state of 1 by using teleportation protocol, where Alice first performed the operation on the particle 1 corresponding to the classical bit she wants to communicate and then teleport the state to Bob. So finally Bob gets the desired maximally entangled state (encoding the Alice's clasical bit) between particle 2 and 4 both of which are on his side. Bob can easily know the Bell state and get the desired classical bit. In this whole process one sees that in the absence of physical transfer of qubit, Alice can send two classical bits by spending (during teleportation)two classical bits.

Now we assume that there exists a teleportation protocol which can teleport any quantum state exactly using c bits which is less that

two bits of classical information. Using that protocol Alice can send two bits of information by spending only c(< 2) bits of classical information without physically transferring any particles. This implies signalling. To be more explicit, let in the teleportation protocol, Bob guesses the classical bit instead of hearing from Alice and performs his necessary action fixed by the teleportation protocol. Then Bob will be correct with probability $\frac{1}{2^c}$ which is obviously greater than $\frac{1}{4}$ as $c < 2$. But for four mutually exclusive random information with equal probability, guessing can give correct result with probability $\frac{1}{4}$. But teleportation of quantum state with classical bits less than two makes this probability greater which implies signalling. Hence quantum teleportation can not be performed with classical information less than two bits.

8 Remote state preparation

In quantum teleportation as we have seen any unknown state of a qubit can be teleported but this process necessarily needs two bits of classical information. Now we pose a different question. If the state is known to Alice, does it help to reduce the number of bits for preparing the state at Bob's end. The question in general, remains unsolved though there is some asymptotic result which we refrain from discussing now. Here we shall show that if the state to be prepared at Bob's end, is from a great circle of the Poincare sphere, then the state can be remotely prepared using only one bit of information. Let Alice and Bob share a singlet state where Alice holds the particle 1 and Bob holds particle 2.

$$|\Theta_{sing}\rangle_{12} = \frac{1}{\sqrt{2}}[|\Psi_z\rangle_1 \otimes |\Psi_{-z}\rangle_2 - |\Psi_{-z}\rangle_1 \otimes |\Psi_z\rangle_2]$$

Let the state known to Alice that Alice has to remotely prepare is $|\psi\rangle = a|\Psi_z\rangle + b|\Psi_{-z}\rangle$. Due to symmetry of the singlet state, it can be written in any basis with same form. We can express the singlet state in the basis $(|\psi\rangle, |\bar{\psi}\rangle)$ where $|\bar{\psi}\rangle (= a^*|\Psi_{-z}\rangle - b^*|\Psi_z\rangle)$ is orthogonal to $|\psi\rangle$.

$$|\Theta_{sing}\rangle_{12} = \frac{1}{\sqrt{2}}[|\psi\rangle_1 \otimes |\bar{\psi}\rangle_2 - |\bar{\psi}\rangle_1 \otimes |\psi\rangle_2]$$

Now let us come to the protocol.
Alice performs measurement in the basis $(|\psi\rangle, |\bar{\psi}\rangle)$. If her qubit collapses on the state $|\bar{\psi}\rangle$, then Bob's qubit collapses on the state $|\psi\rangle$ that was suppose to be prepared. So the programme has been successful. But if Alice's qubit collapses on the the state $|\psi\rangle$, then Bob's qubit collapses on $|\bar{\psi}\rangle$. So after knowing the result of Alice Bob has to apply a unitary operation such that

$$a^*|\Psi_{-z}\rangle - b^*|\Psi_z\rangle \quad \xrightarrow{\mathbf{U}} \quad a|\Psi_z\rangle + b|\Psi_{-z}\rangle$$

But at this point there is a no-go theorem which states that there is no universal unitary operator which can flip every state. So in general remote state preparation is impossible using only one classical bit. But if one restricts the set of states to be remotely prepared, to the set $|\psi\rangle = a|\Psi_z\rangle + b|\Psi_{-z}\rangle$ for a, b real, then if Bob applies σ_x first and then σ_z, the state is successfully prepared at Bob's end as

$$\sigma_z\sigma_x(a|\Psi_{-z}\rangle - b|\Psi_z\rangle) = a|\Psi_z\rangle + b|\Psi_{-z}\rangle = |\psi\rangle$$

Though, in general Alice can not prepare an arbitrary state half of the times, she can make Bob generate the correct statistics for any state. Let Alice has the pure state $\rho = |\psi\rangle\langle\psi| = \frac{1}{2}[I + a.\sigma]$ with $|a| = 1$ and B is an (polarization) observable in the direction of the vectorb. Now for measurement of a spin observable $b.\sigma$ in the state

ρ the probability of spin-up $(+)$ and spin-down $(-)$ are given by

$$P_{\pm}(\rho) = \frac{1}{2}[1 \pm b.a]$$

Interestingly the corresponding probabilities for the pure state orthogonal to ρ are given by

$$P_{\pm}(\overline{\rho}) = \frac{1}{2}[1 \mp b.a]$$

Then the remote statistics generation protocol will be like this. If Alice gets $|\psi\rangle$ then after Alice's phone call Bob performs the measurement of $b.\sigma$ (say) and records his result. When Alice gets $|\overline{\psi}\rangle$, then after Alice's phone call Bob performs his measurement but inverts her result as

$$+1 \rightarrow -1$$

$$-1 \rightarrow +1$$

By this transformation

$$P_{\pm}(\overline{\rho}) = \frac{1}{2}[1 \mp b.a] \rightarrow \frac{1}{2}[1 \pm b.a] = P_{\pm}(\rho)$$

Finally what we saw is that though a quantum state can not be remotely prepared, one can remotely generate the measurement statistics for any given state by using one classical bit only.

9 Quantum correlation reduces communication

The pseudo-telepathy games described above shows the power of quantum correlation (entanglement) in the world of communication. Now we shall see how quantum entanglement can be used to reduce the communication needed to compute (in classical world) a function whose input data is distributed among remote parties.

Consider the following three-party scenario. Alice, Bob and Charlie receive n- strings x, y and z respectively, where

$$x = (x_1 x_2 \dots x_n), \quad x_i \in \{0, 1\}$$

Similarly for y and z. There is a constraint on the inputs x, y and

z given by

$$x_i + y_i + z_i = 1$$

for all i where the $+$ is addition modulo 2. The goal is for Alice to determine the value of the following function

$$f(x, y, z) = x_1 \cdot y_1 \cdot z_1 + \ldots + x_n \cdot y_n \cdot z_n$$

For $n \geq 3$, in classical world, more than two bits of communication are necessary to compute this function.

A three-bit classical protocol

Now we shall see that three bits of communication are also sufficient. We shall check this for the simplest case $n = 3$.
The idea behind the protocol is to count the total number of zeros among all the 9 bits input (3 bits each). Now for each $i \in \{1, 2, 3\}$, if $x_i \cdot y_i \cdot z_i = 1$ then none of x_i, y_i, z_i is zero and if $x_i \cdot y_i \cdot z_i = 0$,

then two among x_i, y_i, z_i are zero (remember $x_1 + y_i + z_i = 1$). Let the number of zeros in Alice's input, Bob's input and Charlie's input are r_A, r_B and r_C respectively. Obviously the total no. of zeros among all their input is even and let us denote it by $2k$. Then one can easily see that in the sum

$$x_1 \cdot y_1 \cdot z_1 + \ldots + x_n \cdot y_n \cdot z_n$$

, k no. of terms are zero and hence

$$f(x, y, z) = (n - k) mod 2$$

So the problem of computing the function reduces to computing k. k can be computed if Bob and Charlie communicate r_B and r_C whose possible values can be $0, 1, 2, 3$. To communicate this no. Bob and Charlie have to communicate two bits of information $(00, 01, 10, 11)$. But $r_A + r_B + r_C$ being even, if Alice knows one of r_B and r_C, she can find the parity of the other. So it will be

sufficient if one of them just send the higher order bit (0 for $\{00, 01\}$ and 1 for $\{10, 11\}$) of their two bit-number.

Two-bit quantum protocol:

Let Alice Bob and Charlie share n copies of the following entangled state

$$|\psi>^{i}_{ABC}= \frac{1}{2}[|001> +|010> +|100> -|111>]$$

where $i = 1, 2..n$. So each party will have n qubits in their lab. The protocol is as follows.

$*$ If Alice i-th bit is 1 i.e. $x_i = 1$, she measures on the qubit belonging to the ith entangled state in the $\{|0>, |1>\}$ basis and notes down the outputs s^i_A (0 if collapses on $|0>$ and 1 if collapses on $|1\rangle$).

$*$ If i-th bit is 0, she first applies the Haddamard gate on the

respective qubit

$$H|0>=\frac{1}{\sqrt{2}}(|0>+|1>), H|1>=\frac{1}{\sqrt{2}}(|0>-|1>)$$

and then follows the same procedure described above.
Bob and Charlie follow similar procedure.
The Alice, Bob and Charlie calculates $S_A(=\sum S_A^i)$, $S_B=(\sum S_B^i)$, and $S_C(=\sum S_C^i)$ respectively. Bob and Charlie send S_B and S_C using one cbit respectively to Alice. Alice outputs $S_A+S_B+S_C$ as value of the function.

How this protocol works

We shall see that for all $i \in \{1, ..., n\}$,

$$S_A^i + S_B^i + S_C^i = x_i \cdot y_i \cdot z_i$$

Due to the constraint on the input the allowed values of $x_i y_i z_i$ are

$\{001, 010, 100.111\}$

$*$ First we consider the case when $x_i y_i z_i = 111$. In this case all of them will measure on their respective qubits in the $\{|0>, |1>\}$ basis. Obviously all possible results $\{S_A^i S_B^i S_C^i\}$ will satisfy

$$S_A^i + S_B^i + S_C^i = 1 = x_i \cdot y_i \cdot z_i$$

$*$ Next we consider the case $x_i y_i z_i = 001$. Following the protocol, Alice and Bob first apply Haddamard operation on their respective qubit. So the final state will become

$$H \otimes H \otimes I \ \frac{1}{2}[|001> + |010> + |100> - |111>]$$

$$= \frac{1}{2}[|011> + |101> + |000> - |110>]$$

Obviously again all possible measurement result $\{S_A^i S_B^i S_C^i\}$ will satisfy

$$S_A^i + S_B^i + S_C^i = 0 = x_i \cdot y_i \cdot z_i$$

Due to the symmetry of the entangled state things will work similarly for cases where $x_i y_i z_i = 010, 100$.

Now one can compute

$$S_A + S_B + S_C = \sum_{i=1}^{n} S_A^i + \sum_{i=1}^{n} S_B^i + \sum_{i=1}^{n} S_C^i$$

$$= \sum_{i=1}^{n} (S_A^i S_B^i S_C^i)$$

$$= \sum_{i=1}^{n} x_i \cdot y_i \cdot z_i = f(x, y, z)$$