Lecture 1

16 JUN 2014

Overview of lectures

AG-66

Monday 3-4pm Tues. 10am & 2:30pm

Wed. ~~Thu.~~ - Fri. 10am - 11am & 3-4pm

all others

AG-80

ask about background

how many info. theory?

how many QM?

how many QIT?

nearly every year @ TIFR there is a QIT course taught by Naresh Sharma or Pranab Sen or both

Schedule

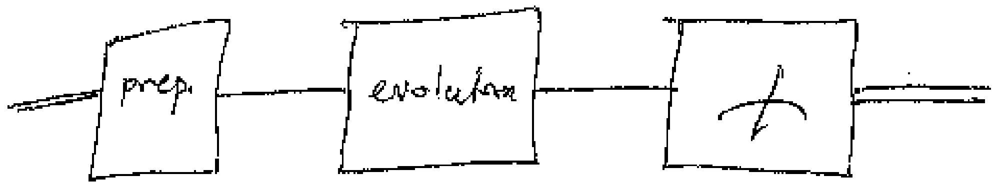
Basics:

1. Intro to QM
2. no-cloning theorem, CHSH game
3. teleportation & dense coding
4. mixed states & channels
5. proof of Choi-Kraus theorem for channels
6. distance measures

Advanced topics:

7. ~~[illegible]~~ classical communication
8. conditional mutual information (Renyi)
9. Strong converse bounds for quantum communication

Any quantum information processing protocol will have the form



steps include

1) preparation of a quantum state
2) evolution according to some process
3) measurement or ~~read~~ out

We need to understand each of these steps in order to describe QIP ~~protocols~~,

there is a mathematical formalism that subsumes ~~[illegible]~~ classical info. processing

We begin by assuming that each step is perfect + then we later show how to bring noise into the picture.

Main goal of quantum information theory is to understand the fundamental limits of communication w/ quantum resources. Examples are communicating over a noisy channel or compressing quantum data.

General questions of practical interest:

Fix a small parameter $\varepsilon > 0$. What is the largest number of messages that a sender can communicate to a receiver ~~such that~~ using a channel such that the error probability is no larger than ε? What if allowed to use the channel n independent times where n is large?

Similar kind of question for data compression

Now give the postulates of quantum mechanics
(We will revise these later when we bring noise into the picture.)

I. Quantum states are described mathematically as a "ray" in Hilbert space.
For the duration of these lectures, we will focus on finite-dimensional spaces for simplicity, so that states are just unit vectors.
We write

$|\psi\rangle$ to mean $\begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{bmatrix}$ where

$\alpha_i \in \mathbb{C}$ & $\| |\psi\rangle \|_2^2 = 1$, i.e.,

$$\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$$

A qubit is described by $\begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$

quote of Schumacher on the invention of the term qubit

~~A~~ Classical states can be encoded into quantum systems as <u>orthogonal</u> states

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

If they are orthogonal, they are perfectly distinguishable by a measurement (in principle)

However, in QM, we can have superpositions of classical states

$\alpha_0 |0\rangle + \alpha_1 |1\rangle$ as long as
"here" "there"

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

- can put anything in a ket!

a global phase is irrelevant, i.e., no measurement can distinguish the states

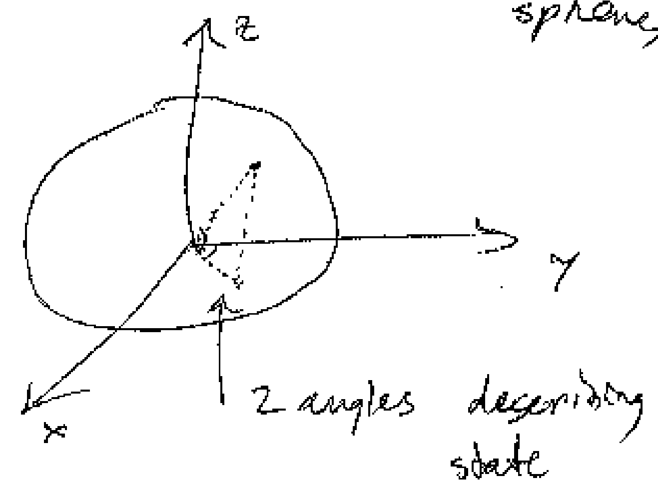
$$r_0 e^{i\phi_0} |0\rangle + r_1 e^{i\phi_1} |1\rangle \quad \text{from}$$

$$\cancel{e^{i\phi_0}} \left(r_0 |0\rangle + r_1 e^{i(\phi_1 - \phi_0)} |1\rangle \right)$$

So the condition $|r_0|^2 + |r_1|^2 = 1$

leaves two parameters to describe the state.

can think of a pure state as being on the surface of a sphere (Bloch sphere)



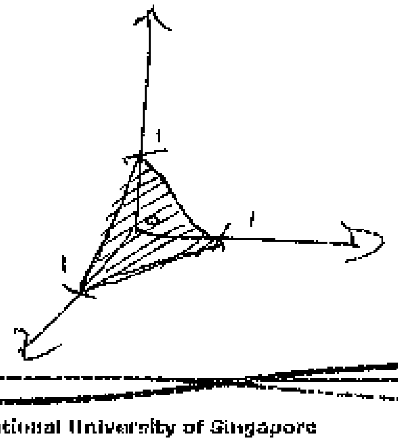
Contrast this description w/ probability distributions, relatively modern tool indispensable in the analysis of classical information processing:

we can describe them as

$$\vec{p} \equiv \begin{bmatrix} p_0 \\ \vdots \\ p_{d-1} \end{bmatrix} \quad \text{such that} \quad p_i \geq 0 \ \forall i$$

$$\quad \& \quad \sum_{i=0}^{d-1} p_i = 1$$

these conditions impose that probability distributions live on the simplex:



deterministic "pure" states are on the vertices ~~boundary~~ of the simplex

can take "superpositions" of prob. dist's
(call them mixtures) as ~~any~~

$\lambda_p \vec{p} + \lambda_q \vec{q}$

as long as $\lambda_p \geq 0$, $\lambda_q \geq 0$ & $\lambda_p + \lambda_q = 1$
space of prob. dist's is convex

II. Evolutions of quantum states in closed system are
described mathematically as unitary
operators. I.e., $U^\dagger U = I$

Why? Seems sensible that an evolution
should take one state to another. So,
if you "buy into" I, then this
one is a natural consequence given
that unitaries are the only matrices
that preserve the l_2 norm
(exercise in linear algebra to prove this).

So we take this as a postulate.

Contrast this w/ probability theory.
There, the evolutions take probability dists
to prob. dist, & the only ones that do so

(8)

are stochastic matrices

(matrices w/ nonnegative entries such that ~~the columns~~ each column sums to one.) matrices that take "pure" classical states to "pure" classical states are ~~the~~ permutation matrices.

This is a big difference between the classical & quantum theories of information:

- In QM, we can go from pure states to pure states by continuous unitary transformations
- In CM, the transformations from pure states to pure states are not continuous in this sense.

III. States of composite quantum systems are described as a ray in a tensor product Hilbert space.

This is again almost a natural consequence of I.

Consider that we describe the state of deterministic classical bits w/ Cartesian product

$(z_0, z_1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$

We can write this as
$(0,0), \ldots, (1,1)$ or

$00, \ldots, 11$ so we can embed this

as $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

But again, from 1st postulate, we know that superpositions of these states are possible so that

$$\sum_{i,j \in \{0,1\}} \alpha_{ij} |ij\rangle$$

as long as $\sum_{i,j \in \{0,1\}} |\alpha_{ij}|^2 = 1$

To desribe these states mathematically, we use the Kronecker tensor product, defined as

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \otimes \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \\ b_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{bmatrix}$$

So this means that a general state

$$\sum_{i,j \in \{0,1\}} \alpha_{ij} |ij\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \quad \text{since}$$

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \ldots, |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

this allows for entangled states which are those that cannot be written as a product $|\psi\rangle \otimes |\phi\rangle$ for any $|\psi\rangle, |\phi\rangle$

Entanglement is very particular to quantum theory & we will show how it is possible to do things w/ entangled states that are impossible to do classically.

~~Continue~~ We should also note that the tensor product can be used to describe joint probability distributions as well. I.e., we can have two RVs (Z_0, Z_1) w/ joint distribution $P_{Z_0,Z_1}(z_0,z_1)$ so that the probability vector is

$$\begin{bmatrix} P_{Z_0,Z_1}(0,0) \\ P_{Z_0Z_1}(0,1) \\ P_{Z_0Z_1}(1,0) \\ P_{Z_0Z_1}(1,1) \end{bmatrix}$$

So this is a mixture of deterministic states $|0\rangle\otimes|0\rangle$, $|0\rangle\otimes|1\rangle$, ... $|1\rangle\otimes|1\rangle$

It might seem from this comparison that entangled states are no different from joint probability distributions, but in fact they are <u>very different</u>

we return to this point later.

IV. (stated in a minimal way) Immediate repetition of a measurement gives the same outcome. Most controversial aspect of Q.M. This is how we "read out" information from a quantum system.

The implication of this postulate is that measurement is described by a set of projection matrices $\{\Pi_i\}_{i=0}^{d-1}$ such that $\sum_i \Pi_i = I$.

This captures the probabilistic aspect of QM or the "jumpiness" part

When a measurement $\{\Pi_i\}$ is performed on a quantum system in the state $|\psi\rangle$,

The probability of getting outcome i

is $\langle\psi|\Pi_i|\psi\rangle = \| \Pi_i |\psi\rangle \|_2^2$

called the "Born rule"

+ the post-measurement state is

$$|\psi\rangle \rightarrow \frac{\Pi_i|\psi\rangle}{\|\Pi_i|\psi\rangle\|_2}$$

so the state is projected and renormalized so that it is a legitimate q. state.

mention how global phase is then physically irrelevant

If we have two qubits + perform a measurement on one of them, we describe the overall measurement as $\{\Pi_i \otimes I\}$

We can also have joint measurements that act collectively, + this is one reason

... optical chann