PHY 4105: Quantum Information Theory
Lecture 13

Anil Shaji
School of Physics, IISER Thiruvananthapuram
(Dated: September 17, 2013)

Brief Recap

The composite system made of two subsystems A and B with respective Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ has an associated Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ of dimension $d_A d_B$ where d_A and d_B are the dimensions of A and B. We have a basis for $\mathcal{H}_{AB}$ given by

$$|e_j\rangle \otimes |f_k\rangle = |e_j\rangle|f_k\rangle = |e_j, f_k\rangle = |j,k\rangle = |jk\rangle.$$

The expansion of an arbitrary vector in $\mathcal{H}_{AB}$ looks like

$$|\Psi\rangle = \sum_{jk} |e_j, f_k\rangle\langle e_j f_k|\Psi\rangle = \sum_{jk} c_{jk}|e_j, f_k\rangle.$$

The basic operators on the tensor product space $\mathcal{H}_{AB}$ are outer products of the form

$$(|\psi\rangle \otimes |\phi\rangle)(\langle\chi| \otimes \langle\xi|) = |\psi\rangle\langle\chi| \otimes |\phi\rangle\langle\xi|.$$

An arbitrary operator O acting on tensor product space can be expanded as

$$O = \sum_{jklm} O_{jk,lm}|e_j, f_k\rangle\langle e_l, f_m|.$$

The partial trace of an operator O with respect to system B is an operator on A:

$$\mathrm{tr}_B(O) = \sum_k \langle f_k|O|f_k\rangle = \sum_{jl} O_{jk,lk}|e_j\rangle\langle e_l|.$$

If the composite system has a state ρ_{AB} then a measurement in the basis $|e_j\rangle$ on system A yields result j with probability

$$p_j = \sum_k p_{jk} = \sum_k \langle e_j, f_k|\rho_{AB}|e_j, f_k\rangle.$$

$$p_j = \sum_k \langle e_j, f_k|\rho_{AB}|e_j, f_k\rangle = \langle e_j|\Big(\sum_k \langle f_k|\rho_{AB}|f_k\rangle\Big)|e_j\rangle = \langle e_j|\,\mathrm{tr}_B(\rho_{AB})|e_j\rangle = \langle e_j|\rho_A|e_j\rangle = \mathrm{tr}(P_{e_j}\rho_A),$$

where we have defined

$$\rho_A = \mathrm{tr}_B(\rho_{AB}).$$

Based on what we have learned so far, we can reformulate the axioms of quantum mechanics as

1. Quantum states: density operators ρ
2. Observables $A = A^\dagger = \sum_j \lambda_j |e_j\rangle \bar{e_j} = \sum_j \lambda_j P_j$,
$$p(e_j) = \langle e_j|P_j|e_j\rangle = \mathrm{tr}(\rho P_j).$$
3. Post measurement state:
$$\frac{P_j \rho P_j}{\mathrm{tr}(\rho P_j)} = |e_j\rangle\langle e_j|.$$
4. Dynamics:
$$i\hbar \frac{d\rho}{dt} = [H, \rho], \qquad \Leftrightarrow \qquad \rho(t) = e^{-iHt/\hbar} \rho(0) e^{iHt/\hbar}.$$
5. Hilbert space for multiple quantum systems is a tensor product.

Gleason's theorem: For $D \geq 3$, if a function f from one dimensional projectors to [0, 1] satisfies $\sum_j f(P_j) = 1$, whenever $\sum_j P_j = \mathbb{1}$ then there exists a density operator ρ such that $f(P) = \mathrm{tr}(\rho P)$.

Gleason's theorem represents an approach to the axiomatization of quantum mechanics. It seeks to obtain the state space from the Hilbert space structure of quantum measurements. It seeks to ask and possibly address questions like why do we have specifically a Hilbert space and especially why do we have non-contextual probabilities?

Two qubits

Let us now look in detail at the state space of two qubits and see what new and interesting phenomena emerge over and above those we saw with respect to a single qubit. For two qubits we have the standard orthonormal basis given by

$$\left.\begin{array}{ccc} |00\rangle & = & |0\rangle \otimes |0\rangle \\ |01\rangle & = & |0\rangle \otimes |1\rangle \\ |10\rangle & = & |1\rangle \otimes |0\rangle \\ |11\rangle & = & |1\rangle \otimes |1\rangle \end{array}\right\} \quad |x\rangle = |x_1\rangle \otimes |x_2\rangle.$$

An alternate and useful basis is given by the "Bell orthonormal" basis,

$$\begin{aligned} |\Phi^\pm\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle \pm |11\rangle\big) = \begin{array}{c} |\beta_{00}\rangle \\ |\beta_{10}\rangle \end{array} \\ |\Psi^\pm\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle \pm |10\rangle\big) = \begin{array}{c} |\beta_{01}\rangle \\ |\beta_{11}\rangle \end{array} \end{aligned}$$

The naming of the basis states is with respect to the eigenvalues of two out of the three commuting operators, $Z \otimes Z$, $X \otimes X$ and $Y \otimes Y$. In other words, we have

$$\begin{aligned} Z \otimes Z|\Phi^\pm\rangle &= |\Phi^\pm\rangle \\ Z \otimes Z|\Psi^\pm\rangle &= -|\Psi^\pm\rangle \\ X \otimes X|\Phi^\pm\rangle &= \pm|\Phi^\pm\rangle \\ X \otimes X|\Psi^\pm\rangle &= \pm|\Psi^\pm\rangle \end{aligned}$$

So the Φ and Ψ label the "parity" of the state (parity bits) and the $\pm$ labels the "phase" of the two qubit state. We can use the combined notation,

$$|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}\big(|0b\rangle + (-1)^a|0\bar{b}\rangle\big), \qquad \bar{b} = 1 + b.$$

Here the subscript a labels the phase of the state and is called the phase bit and the subscript b is the parity bit. For all the Bell-basis states, the marginal density operators are

$$\rho_A = \rho_B = \mathbb{1}/2.$$

A. Superdense coding

The states $|\beta_{ab}\rangle$ are connected to each other through local operations on one of the two qubits. This allows two parties, hereafter called Alice and Bob, to send two bits worth of information from one party to the other by sending only a single qubit across provided they share previously pairs of qubits in the $|\beta_{00}\rangle$ state. This protocol is called superdense coding. The Bell basis state shared between the two previously is treated as a resource that is eaten up each time when the protocol implemented. The transformation between $|\beta_{00}\rangle$ and the other three Bell basis states is

$$\begin{aligned} Z \otimes \mathbb{1}|\beta_{00}\rangle &= |\beta_{10}\rangle &= \mathbb{1} \otimes Z|\beta_{00}\rangle \\ X \otimes \mathbb{1}|\beta_{00}\rangle &= |\beta_{01}\rangle &= \mathbb{1} \otimes X|\beta_{00}\rangle \\ ZX \otimes \mathbb{1}|\beta_{00}\rangle &= |\beta_{11}\rangle &= \mathbb{1} \otimes XZ|\beta_{00}\rangle, \end{aligned}$$

with $ZX = iY$.

The protocol proceeds as follows: Alice and Bob each have one qubit of an entangled pair in state $|\beta_{00}\rangle$. Alice can encode two bits on the joint state using $\mathbb{1}$, Z, X and ZX on her qubit. Alice sends her qubit to Bob, who reads out the qubit pair in the Bell basis.

B. Pauli representation of Bell basis states

We have seen that any operator can be expanded in the Pauli basis as

$$\rho = \frac{1}{4}\sum_{\alpha\beta} \rho_{\alpha\beta}\sigma_\alpha \otimes \sigma_\beta, \quad \text{with} \quad \rho_{\alpha\beta} = \operatorname{tr}(\rho\sigma_\alpha \otimes \sigma_\beta), \quad \rho_{00} = 1.$$

We can do an expansion of this sort for the Bell basis states,

$$|\Phi^+\rangle\langle\Phi^+| = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11| + |00\rangle\langle 11| + |11\rangle\langle 00|).$$

Using

$$\begin{aligned} |00\rangle\langle 00| &= \frac{1}{2}(\mathbb{1} + Z) \otimes \frac{1}{2}(\mathbb{1} + Z) \\ |11\rangle\langle 11| &= \frac{1}{2}(\mathbb{1} - Z) \otimes \frac{1}{2}(\mathbb{1} - Z) \\ |00\rangle\langle 1| &= \frac{1}{2}(X + iY) \otimes \frac{1}{2}(X + iY) \\ |11\rangle\langle 00| &= \frac{1}{2}(X - iY) \otimes \frac{1}{2}(X - iY), \end{aligned}$$

we get

$$|\Phi^+\rangle\langle\Phi^+| = |\beta_{00}\rangle\langle\beta_{00}| = \frac{1}{4}\big(\mathbb{1}\otimes\mathbb{1} + Z\otimes Z + X\otimes X - Y\otimes Y\big).$$

Similarly we have

$$\begin{aligned}
|\Phi^-\rangle\langle\Phi^-| &= |\beta_{10}\rangle\langle\beta_{10}| &= \frac{1}{4}\big(\mathbb{1}\otimes\mathbb{1} + Z\otimes Z - X\otimes X + Y\otimes Y\big) \\
|\Psi^+\rangle\langle\Psi^+| &= |\beta_{01}\rangle\langle\beta_{01}| &= \frac{1}{4}\big(\mathbb{1}\otimes\mathbb{1} - Z\otimes Z + X\otimes X + Y\otimes Y\big) \\
|\Psi^-\rangle\langle\Psi^-| &= |\beta_{11}\rangle\langle\beta_{11}| &= \frac{1}{4}\big(\mathbb{1}\otimes\mathbb{1} - Z\otimes Z - X\otimes X - Y\otimes Y\big)
\end{aligned}$$

The last state is rotationally invariant. This is because

$$u\otimes u(\sigma_j\otimes\sigma_j)u\otimes u = \sigma_k R_{kj}\otimes\sigma_l R_{lj} = \sigma_k\otimes\sigma_l(RR^T)_{kl} = \sigma_k\otimes\sigma_k.$$

It is rather useful to note that the Z operator represents a 180 degree rotation about the $z-$axis and X represents a 180 degree rotation around the $x-$axis and so on. In other words

$$ZXZ = -X, \quad ZYZ = -Y, \quad ZZZ = Z, \qquad XXX = X, \quad XYX = -Y, \quad XZX = -Z.$$