An Introduction to Quantum Information

Assumed background:

Undergraduate real space quantum Mechanics

1. Hilbert space basics — Dirac notation
2. Schrödinger time evolution
3. Hermitian and unitary operators.

Outline:

1. Motivations
2. Qubits and quantum logic gates
3. Density operators
4. Entanglement
5. ~~The simplest quantum algorithm: Deutch-Jozsa algorithm~~
6. ~~Generalized measurements~~
7. Quantum key distribution (QKD)
8. CHSH inequality – Bell's theorem
9. The rotating frame
10. NMR

References:

1. Schumacher and Westmoreland – Quantum Processes, Systems, and Information
2. Michael Nielsen & Isaac Chuang – Quantum Computation and Quantum Information.

1. Motivations:

1. Size of transistors shrinking ~ 7 nm (7×10^{-9}m). Comparable to size of atoms ~ 0.2 nm (2×10^{-10}m) for a silicone atom. Quantum and thermal effects will limit the efficiency of next generation of transistors. To keep up with Moore's law we may need to go quantum.

2. Information Security: Many of our current cryptographic protocols safe-guard information against brute-force attacks by being based on NP-hard problems. Quantum algorithms exist that can crack such protocols in polynomial time. Also quantum cryptographic protocols offer better security against hacking. This is covered in QKD.

3. Simulations of quantum systems: Classical computers are not very efficient in simulating quantum systems. The dim of the Hilbert space of N two-level systems is 2^N. For $N = 100$ such systems [common in many-body physics] the dim of the Hilbert space ~ $2^{100} \approx 10^{30}$. Quantum processors would fare much better at simulating such a large state space.

4. Quantum Church-Turing hypothesis:

(Classical) strong Church-Turing Thesis: A probabilistic Turing machine can efficiently simulate any model of classical computation.

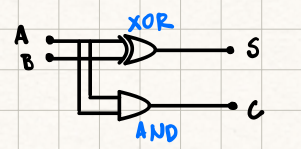
Quantum strong Church-Turing Thesis: A quantum Turing machine can efficiently simulate any realistic model of computation.

5. Quantum algorithms

2. Qubits and quantum logic gates

Information in classical computers are encoded in strings of bits. Each bit can be represented by a binary digit — 0 or 1. Complicated computer circuits are made out of simpler logic gates such as NOT, AND, OR, NAND, XOR, NOR etc. NAND and NOR gates can be used to make any other gate and so the set of NAND & NOR is an example of a universal gates.

An example of a digital circuit:

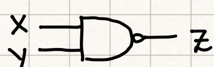


A half-adder circuit

A	B	C	S
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

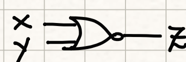
An important observation about classical gates: They are irreversible. Not 1-1:

NAND:



X	Y	$Z = \overline{X \cdot Y}$
0	0	1
0	1	1
1	0	1
1	1	0

NOR



X	Y	$Z = \overline{X \oplus Y}$
0	0	1
0	1	0
1	0	0
1	1	0

Quantum bits (qubits) are two-level quantum systems. The two orthonormal basis states representing 0 & 1 are written as $|0\rangle$ & $|1\rangle$. Physical realization of a qubit:

a) Spin degree of freedom of a quantum particle

b) Two energy levels of a quantum state

c) Interferometer — photon / neutron travelling along an arm.

The set $\{|0\rangle, |1\rangle\}$ is called the computational basis. In contrast to a classical computer qubits have the following features:

1. A qubit can be in an arbitrary superposition of $|0\rangle$ & $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{with} \quad |\alpha|^2 + |\beta|^2 = 1.$$

2. Two or more qubits can be in an entangled state. E.g. The state

$$\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \quad \text{can not be written as} \quad |\psi\rangle|\phi\rangle.$$

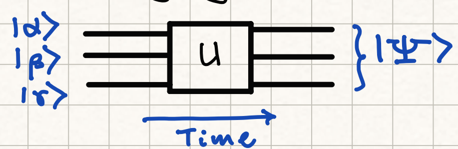
Much of the power of quantum computers arise from these two features.

Often we shall represent $|0\rangle$ & $|1\rangle$ in the computational basis:

$$|0\rangle \text{``=''} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle \text{``=''} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad [\text{The matrix elements are } \langle a|b\rangle]$$

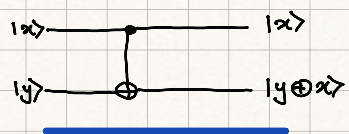
We shall henceforth drop the quotation marks.

Quantum logic gates are unitary operators that act on qubits:



Examples of logic gates:

1. CNOT



CNOT defined in terms of the computational basis

CNOT

$$|x\rangle|y\rangle \longrightarrow |x\rangle|y\oplus x\rangle$$

Control bit, data bit

Explicitly
$$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$$
$$|1\rangle|1\rangle \longrightarrow |1\rangle|0\rangle$$

The CNOT is a linear operator and it acts on an arbitrary two qubit input by linearity:

$|\Psi\rangle = \alpha\, |0\rangle|0\rangle + \beta|0\rangle|1\rangle + \gamma|1\rangle|0\rangle + \delta\, |1\rangle|1\rangle$ then CNOT acting on it will give

$|\Psi'\rangle = \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + \gamma|1\rangle|1\rangle + \delta\,|1\rangle|0\rangle.$

Verify that in the computational basis CNOT is given by

$$U_+ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Other useful gates include

Control-Phase Gate:

$$|x\rangle|y\rangle \longrightarrow e^{ixy\phi}\,|x\rangle|y\rangle \qquad \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{i\phi} \end{pmatrix}$$

Of course single qubit gates are also necessary:

Single qubit phase gate:

$$U_\phi^1 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}. \quad U_\phi |x\rangle = e^{i\phi x} |x\rangle \qquad |x\rangle \;—\boxed{U_\phi}—\; e^{ix\phi} |x\rangle$$

Hadamard Gate:

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} : \quad \begin{aligned} U_H |0\rangle &= \tfrac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |+\rangle \\ U_H |1\rangle &= \tfrac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |-\rangle . \end{aligned}$$

Since $U_H^2 = \mathbb{1}$, the Hadamard is its own inverse. The four gates $\{ U_+, U_\phi^{(2)}, U_\phi^{(1)} \; \& \; U_H \}$ form a universal set of quantum logic gates.

Exercise: If we use $\{|+\rangle, |-\rangle\}$ as our basis then show that in the CNOT gate given above the second qubit acts as the control qubit:

$$\begin{aligned} |+\rangle|+\rangle &\rightarrow |+\rangle|+\rangle \\ |-\rangle|+\rangle &\rightarrow |-\rangle|+\rangle \\ |+\rangle|-\rangle &\rightarrow |-\rangle|-\rangle \\ |-\rangle|-\rangle &\rightarrow |+\rangle|-\rangle \end{aligned}$$

An important set of gates are the Pauli gates:

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

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

Exercise: Show that

$$R_x(\theta) = e^{-i\theta X/2} = (\cos \tfrac{\theta}{2}) \cdot \mathbb{1} - i (\sin \theta/2) X$$

$$R_y(\theta) = e^{-iY/2} = (\cos \tfrac{\theta}{2}) \cdot \mathbb{1} - i (\sin \theta/2) Y$$

$$R_z(\theta) = e^{-iZ/2} = (\cos \tfrac{\theta}{2}) \cdot \mathbb{1} - i (\sin \theta/2) Z$$

3. Density Operators:

Consider a quantum system with A as an observable. If $\{|\alpha\rangle\}$ are the set of orthonormal eigenvectors: $A|\alpha\rangle = \alpha|\alpha\rangle$, $\langle\alpha|\alpha'\rangle = \delta_{\alpha\alpha'}$

Then any measurement of A will yield one of its eigenvalues. According to the spectral decomposition theorem: $A = \sum_\alpha \alpha |\alpha\rangle\langle\alpha|$

If a system was in the state $|\psi\rangle$ when the measurement was made the probability obtaining α is: $P_\psi(\alpha) = |\langle\alpha|\psi\rangle|^2$

The expectation value of A for the state $|\psi\rangle$ is:

$$\langle A\rangle = \sum_\alpha \alpha P_\psi(\alpha)$$

$$= \sum_\alpha \alpha \langle\alpha|\psi\rangle\langle\psi|\alpha\rangle$$

$$= \sum_\alpha \langle\alpha|\psi\rangle\langle\psi|\alpha|\alpha\rangle$$

$$= \sum_\alpha \langle\alpha|\psi\rangle\langle\psi|A|\alpha\rangle$$

$$\langle A\rangle = \mathrm{Tr}(|\psi\rangle\langle\psi|A)$$

Now suppose we weren't sure of what the state of the system was and it was given by a probability distribution: $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\} \rightsquigarrow$ completely arb. set of normalized states of the system with the probability distribution $\{p_1, p_2, \dots, p_n\}$

[These ps have nothing to do with $P_\psi(\alpha)$ above.]

Then the expectation value of A is:

$$\langle A\rangle = \sum_{i=1}^{n} p_i \langle\psi_i|A|\psi_i\rangle$$

$$= \sum_{i=1}^{n} p_i \,\mathrm{Tr}(|\psi_i\rangle\langle\psi_i|A)$$

$$= \mathrm{Tr}\Big(\sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i|A\Big)$$

$$= \mathrm{Tr}(\rho A)$$

where $\rho \equiv \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i|$ is the density matrix of the system whose 'state' is given by probability distribution of states given above. If only one $p=1$ and there is only one state in ρ, i.e. $\rho = |\psi\rangle\langle\psi|$, in some basis, then we say it's a pure state. Otherwise we say the state is mixed.

Properties of density operators:

1. ρ is a positive operator. All eigenvalues are positive semi-definite.
2. $\mathrm{Tr}\,\rho = 1$.
3. If $\rho^2 = \rho$ then ρ is pure. $\Rightarrow$ $\mathrm{Tr}(\rho^2) = 1$. [converse true only in dim > 3]

Examples:

1. $\rho = |0\rangle\langle 0| \Rightarrow \rho = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

2. $\rho = |+\rangle\langle +| = \frac{1}{2}\{|0\rangle + |1\rangle\}\{\langle 0| + \langle 1|\} = \frac{1}{2}\{|0\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|\}$
$$\Rightarrow \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

3. $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

1 & 2 are pure states while 3 is mixed.

In d-dimensions the density operator:
$$\pi_d = \frac{1}{d}\mathbb{I}_d$$
is known as the maximally mixed state.

Density matrix of a quantal system in an enviornment at temperature T:
$$\rho_\beta = \frac{1}{Z}\sum_n e^{-H\beta}|n\rangle\langle n| \quad , \quad \beta = \frac{1}{k_B T}$$
where $|n\rangle$ are the eigenstates of the Hamiltonian operator and $Z = \mathrm{Tr}\, e^{-H\beta}$.

Some will recognize ρ_β as the quantum canonical ensemble.

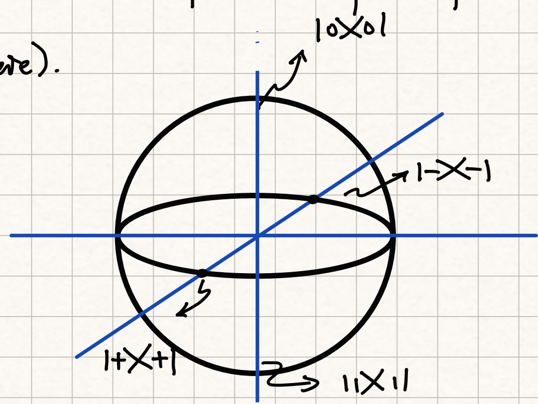
<u>Ex:</u> Suppose you are given a collection of states which are a) either many copies of the state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ or b) many copies of the state $|0\rangle$ or $|1\rangle$ drawn at

random using a fair coin. Is there a way distinguish between the two scenarios? If so devise an experiment to distinguish the two cases.

Ex: Show that the general state of a qubit can be written as:

$$|\theta,\varphi\rangle = \cos\frac{\theta}{2}\cdot|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle \,,\quad 0\leq\theta\leq\pi,\ 0\leq\varphi<2\pi$$

and so a pure qubit can be represented by the points on the surface of a unit sphere (Bloch sphere).



We shall now show that the interior of the Bloch sphere represent all the mixed states of a qubit.

Let $\rho \rightarrow$ general state of a qubit. Since $\rho^{\dagger}=\rho \Rightarrow \rho = \begin{pmatrix} a & c \\ c^{*} & b \end{pmatrix}$ with $a,b\in\mathbb{R}$

But $\mathrm{Tr}\,\rho = 1 \Rightarrow a+b=1$. Thus we can parametrize ρ by three real numbers.

Now $\mathrm{Tr}\,\rho=1 \Rightarrow \rho = \frac{1}{2}(\mathbb{I} + a_x X + a_y Y + a_z Y)$ and $\mathrm{Tr}\,\rho^2 \leq 1 \Rightarrow$

$\bar{a} = a_x\hat{x} + a_y\hat{y} + a_z\hat{z}$ must have $|\bar{a}|^2 \leq 1$.

$\vec{a}$ is the called a Bloch vector and when $|\vec{a}|<1$ it represents a mixed state.

$\vec{a}=0$ is represented by the centre of the Bloch ball and it is known as the maximally mixed state:

Note: $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$.

For any mixed state $\exists$ an infinite number of decomposition in terms of other mixed states. This is known as the ambiguity of mixtures.

Von Neumann Entropy

A measure of the ambiguity of mixture is the von Neuman entropy:

$$S_{vN} = -\mathrm{Tr}(\rho \log \rho) \quad \text{[Base 2 when working with qubits]}$$

where for $\rho_{ii} = 0$ we define $\rho_{ii} \log \rho_{ii} = 0$. For pure states $S = 0$. For a maximally mixed state $\Pi_d = \frac{1}{d} \mathbb{1}_d$ we get $S = -\mathrm{Tr}\left(\frac{1}{d} \mathbb{1}_d \log \Pi_d\right) = \mathrm{Tr}\left(\frac{1}{d} \log d\right)$ $= \log d$. And so $0 \leq S \leq \log d$.

Von Neumann entropy is part of an infinite tower of entropies known as Renyi entropies

$$S_\alpha = \frac{1}{1-\alpha} \log \mathrm{Tr}\, \rho^\alpha \quad , \alpha \geq 0.$$

As $\alpha \to 1$ $S_\alpha \to S_{vN}$ using L'Hopital's rule and $\frac{d}{d\alpha} \rho^\alpha = \frac{d}{d\alpha} e^{\alpha \log \rho} = (\log \rho)\, \rho^\alpha$.

Von Neumann entropy is a useful measure of bi-partite entanglement which we turn to next.

Entanglement

If we have two quantum systems A & B the combined system is described a tensor product Hilbert space: $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

If $\{|\psi_i^A\rangle\}$ and $\{|\phi_m^B\rangle\}$ are orthonormal bases on $\mathcal{H}_A$ and $\mathcal{H}_B$, then the product states $|\psi_i^A, \phi_m^B\rangle = |\psi_i^A\rangle \otimes |\phi_m^B\rangle$ form an orthonormal basis on $\mathcal{H}_{AB}$.

These are examples of product states but $\exists$ states on $\mathcal{H}_{AB}$ of the form:

$|\Psi_{AB}\rangle = c_1 |\psi_1^A, \phi_1^B\rangle + c_2 |\psi_2^A, \phi_2^B\rangle + \cdots$ which may not be written in the product form. Such states are called entangled states.

Example: For two qubits the following states are examples of entangled states:

$$|\Phi_\pm\rangle = \frac{1}{\sqrt{2}}\left(|0,0\rangle \pm |1,1\rangle\right)$$

$$|\Psi_\pm\rangle = \frac{1}{\sqrt{2}}\left(|0,1\rangle \pm |1,0\rangle\right)$$

These states are known as the Bell states and they are maximally entangled.

Before we discuss about entanglement and how to quantify it let us give bit more background on tensor product.

The tensor product $\otimes : \mathcal{H}_A \times \mathcal{H}_B \rightarrow \mathcal{H}_{AB}$ has the following properties:

1. If $|a\rangle \in \mathcal{H}_A$ & $|b\rangle \in \mathcal{H}_B$ then $|a,b\rangle = |a\rangle \otimes |b\rangle \in \mathcal{H}_{AB}$
2. Bilinearity: $|a\rangle \otimes (\beta_1 |b_1\rangle + \beta_2 |b_2\rangle) = \beta_1 (|a\rangle \otimes |\beta_1\rangle) + \beta_2 (|a\rangle \otimes |\beta_2\rangle)$
3. Any vector $|\psi\rangle \in \mathcal{H}_{AB}$ can be expressed as linear superposition of $|a_l\rangle \otimes |b_m\rangle$ where $\{|a_l\rangle\}$ and $\{|b_m\rangle\}$ are orthonormal bases of $\mathcal{H}_A$ & $\mathcal{H}_B$ respectively.
4. The inner-product on $\mathcal{H}_{AB}$ is given by: $\langle \psi_A, \phi_B | \psi'_A, \phi'_B \rangle = \langle \psi_A | \psi'_A \rangle \langle \phi_B | \phi'_B \rangle$

Discussion on Tensor Product Structure:

By demanding that $\mathcal{H}_{AB}$ is also a Hilbert Space we introduce an enormous amount of structure into the tensor product. Here we enumerate some of these:

1. $|a\rangle \otimes (\beta |b\rangle) = \beta (|a\rangle \otimes |b\rangle) = (\beta |a\rangle) \otimes |b\rangle$ {Using bi-linearity}
2. Suppose $|a_1\rangle$ & $|a_2\rangle \in \mathcal{H}_A$ s.t. $\langle a_1 | a_2 \rangle = 0$. Now consider $|a_1, b_1\rangle$ & $|a_2, b_2\rangle \in \mathcal{H}_{AB}$. $\langle a_1, b_1 | a_2, b_2 \rangle = \langle a_1 | a_2 \rangle \langle b_1 | b_2 \rangle = 0$ regardless of the value of $\langle b_1 | b_2 \rangle$
3. Let $\{|a_i\rangle\}$ be an orthonormal basis for $\mathcal{H}_A$ and $\{|b_m\rangle\}$ an orthonormal basis for $\mathcal{H}_B$. Then $\{|a_i, b_m\rangle\}$ form an orthonormal basis for $\mathcal{H}_{AB}$: $\langle a_i, b_m | a_j, b_n \rangle = \delta_{ij} \delta_{mn}$
   This basis called the product basis for $\mathcal{H}_{AB}$.
4. If the dimensions of $\mathcal{H}_A$ & $\mathcal{H}_B$ are d_A & d_B, respectively then the dimension of $\mathcal{H}_{AB}$ is $d_A d_B$.
5. Extending linear maps on $\mathcal{H}_A$ & $\mathcal{H}_B$ onto $\mathcal{H}_{AB}$: If A (B) is a linear operator $A : \mathcal{H}_A \longrightarrow \mathcal{H}_A$ ($B : \mathcal{H}_B \rightarrow \mathcal{H}_B$) then we can extend its action by defining

$$A(|a\rangle \otimes |b\rangle) = (A|a\rangle) \otimes |b\rangle \qquad [\, B(|a\rangle \otimes |b\rangle) = |a\rangle \otimes (B|b\rangle)$$

6. The product operator $A \otimes B$ is defined by:

$$(A\otimes B)(|a\rangle \otimes |b\rangle) = A|a\rangle \otimes B|b\rangle$$

$$|a_1, b_1\rangle\langle a_1, b_1| = |a_1\rangle\langle a_1| \otimes |b_1\rangle\langle b_1|$$

Example 1: Constructing the Bell states from product states: Consider:

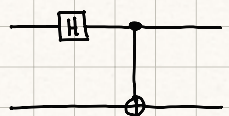
Hadamard: $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. $H|0\rangle = |+\rangle$ & $H|1\rangle = |-\rangle$

CNOT: $U_+|a,b\rangle = |a, a\oplus b\rangle$ $\quad U_+ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Now consider the Circuit:



So in the first step $(H \otimes \mathbb{1})|a,b\rangle = \frac{1}{\sqrt{2}}((-1)^a|a\rangle + |\bar{a}\rangle)|b\rangle$, where $\bar{a} = \text{NOT}(a)$.

$$= \frac{1}{\sqrt{2}}[(-)^a|ab\rangle + |\bar{a}b\rangle]$$

Now if we apply the CNOT gate:

$$|\psi\rangle = U_+ \frac{1}{\sqrt{2}}[(-)^a|ab\rangle + |\bar{a}b\rangle] = \frac{1}{\sqrt{2}}[(-)^a |a, a\oplus b\rangle + |\bar{a}, \bar{a}\oplus b\rangle]$$

$\|a\ b\rangle$	$\|\psi\rangle$
0 0	$\frac{1}{\sqrt{2}}[\|0,0\rangle + \|1,1\rangle] \equiv \|\beta_{00}\rangle$
0 1	$\frac{1}{\sqrt{2}}[\|01\rangle + \|10\rangle] \equiv \|\beta_{01}\rangle$
1 0	$\frac{1}{\sqrt{2}}[-\|11\rangle + \|00\rangle \equiv \|\beta_{10}\rangle$
1 1	$\frac{1}{\sqrt{2}}[-\|10\rangle + \|01\rangle] \equiv \|\beta_{11}\rangle$

Example 2: Let us consider two qubits whose Hamiltonian is given by

$$\mathbb{H} = \lambda Z \otimes Z \qquad Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

The product states $|a,b\rangle$ are eigenstates of $\mathbb{H}$ and so under time evolution they just change by a phase factor: $e^{-\frac{i}{\hbar}\lambda Z\otimes Z t}|0,0\rangle = e^{-\frac{i}{\hbar}\lambda t}|0,0\rangle$

↳ $U(t)$ ~ time evolution operator

But if we consider the action of the time evolution operator on $|+,+\rangle$, which is not an eigenstate, then

$$e^{-\frac{i}{\hbar}\lambda Z\otimes Z t}|+,+\rangle = e^{-\frac{i}{\hbar}\lambda t Z\otimes Z}\frac{1}{2}\{|0,0\rangle + |0,1\rangle + |1,0\rangle + |1,1\rangle\}$$

$$|\Psi(t)\rangle = \frac{1}{2}\{e^{-\frac{i}{\hbar}\lambda t}|00\rangle + e^{+\frac{i}{\hbar}\lambda t}|01\rangle + e^{i\lambda t/\hbar}|10\rangle + e^{-i\lambda t/\hbar}|11\rangle\}$$

At $t = \frac{\pi\hbar}{4\lambda}$: $|\Psi(\frac{\pi\hbar}{4\lambda})\rangle = \frac{1}{2}e^{-i\pi/4}\{|0,+\rangle + |1-\rangle\}$ ⇝ entangled

$$= \frac{1}{2}e^{-i\pi/4}\{\tfrac{1}{\sqrt{2}}|+\rangle|+\rangle + \tfrac{1}{\sqrt{2}}|-\rangle|+\rangle + \tfrac{1}{\sqrt{2}}|+\rangle|-\rangle - \tfrac{1}{\sqrt{2}}|-\rangle|-\rangle\}$$

~ Entangled

At $t = \frac{\pi\hbar}{2\lambda}$ $|\Psi(\frac{\pi\hbar}{2\lambda})\rangle = e^{-i\pi/2}|+\rangle|-\rangle$ ⇝ Not entangled

$$|+,+\rangle + |-+\rangle + |++\rangle - |-+\rangle$$

<u>Alice & Bob</u>

Let us consider an entangled state $|\Psi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \in \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$

Suppose after the creation of such a state the qubit belonging $\mathcal{H}_A$ comes into Alice's possession, while the qubit from B goes to Bob.

If Alice measures in the $\{|0\rangle, |1\rangle\}$ basis then Bob's qubit collapes into either $|0\rangle$ or $|1\rangle$ state conditional upon the outcome of Alice's measurement.

This brings us to the idea of conditional states.

The No communication Theorem:

Suppose Alice & Bob share an entangled state:

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\{|01\rangle - |10\rangle\}$$

If Alice makes a measurement then it influences the result of Bob's measurement. But entanglement can not be used to send information by Alice to Bob in a way that violates the principle of special relativity.

Furthermore Alice's choice of measurement does not influence the probability of Bob's measurement outcomes.

Let us make those ideas more concrete. Let $|\Psi\rangle$ be an entangled state shared by Alice & Bob:

$$|\Psi^{(AB)}\rangle = \sum_{a,b} \Psi_{ab}|a\rangle \otimes |b\rangle = \sum_a |a\rangle \otimes \Big(\sum_b \Psi_{ab}|b\rangle\Big) = \sum |a\rangle \otimes |\Psi_a^{(B)}\rangle$$

where $\{|a\rangle\}$ & $\{|b\rangle\}$ are orthonormal bases for $\mathcal{H}_A$ & $\mathcal{H}_B$. $\{|\Psi_a^{(B)}\rangle\}$ are states that belong to $\mathcal{H}_B$. Note that $|\Psi_a^{(B)}\rangle = \langle a|\Psi^{(AB)}\rangle$.

Now suppose Alice and Bob decide to make projective measurements in the $\{|a\rangle\}$ and $\{|b\rangle\}$ bases. Then we can compute the joint probability $p(a,b)$ by:

$$\begin{aligned} p(a,b) &= |\langle a,b|\Psi\rangle|^2 \\ &= |\langle a,b| \sum_{a'} |a', \Psi_{a'}^{(B)}\rangle|^2 \\ &= |\sum_{a} \delta_{aa'} \langle b|\Psi_{a'}^{(B)}\rangle|^2 \end{aligned}$$

$$\boxed{p(a,b) = |\langle b|\Psi_a^{(B)}\rangle|^2}$$

Similarly we can write:

$$p(a,b) = |\langle a|\Psi_b^{(A)}\rangle|^2$$

Now let us compute the probability for Bob to get $|b\rangle$ as a result of his measurement:

$$p(b) = \sum_a p(a,b) = \sum_a |\langle a|\Psi_b^{(A)}\rangle|^2$$

$$= \sum_a \langle \Psi_b^{(A)} | a \rangle \langle a | \Psi_b^{(A)} \rangle$$

$$= \langle \Psi_b^{(A)} | \Psi_b^{(A)} \rangle$$

Thus we see that $p(b)$ is independent of the choice of measurement by Alice.

Since $p(b)$ involves $|\Psi_b^{(A)}\rangle \in \mathcal{H}_A$ if we make a change of basis in $\mathcal{H}_A$ then $|\Psi_b^{(A)}\rangle \to |\Psi_b^{(A)'}\rangle = U|\Psi_b^{(A)}\rangle$. This may seem to give a different probability distribution $p'(b) = \langle \Psi_b^{(A)'} | \Psi_b^{(A)'} \rangle$ but since $|\Psi_b^{(A)'}\rangle = U|\Psi_b^{(A)}\rangle$ we get

$$p'(b) = \langle \Psi_b^{(A)} | U^\dagger U | \Psi_b^{(A)} \rangle = \langle \Psi_b^{(A)} | \Psi_b^{(A)} \rangle = p(b).$$

Thus we see that $p(b)$ is independent of the choice of basis for $\mathcal{H}_A$.

This is the content of the no-communication Theorem:

Two parties who share a quantum state cannot communicate by:

i) either a choice of local measurement

ii) or by making a local unitary transformation.

Conditional states:

Although Alices choice of measurement or choice of states do not influence Bob's probabilities $p(b)$, the result of Alice's measurement does influence Bob's measurement out comes.

This is most easily seen if we take the singlet state and Alice measures in the $\{|0\rangle, |1\rangle\}$ basis. Then $p(b=0|a=0) = 0$ $p(b=1|a=0) = 1$.

According to Baye's Theorem:

$$p(b|a) = \frac{p(a,b)}{p(a)}$$

$$= \frac{|\langle b | \Psi_a^{(B)} \rangle|^2}{p(a)}$$

This probability is identical to that obtained by Bob having the conditional state:

$$|\hat{\Psi}_a^{(B)}\rangle = \frac{|\Psi_a^{(B)}\rangle}{\sqrt{p(a)}}$$

Density Operator for a subsystem:

Now consider a subsystem B of a compositive system AB. The states of B are given by the conditional states:

$$|\hat{\Psi}_a^{(B)}\rangle = \frac{|\Psi_a^{(B)}\rangle}{\sqrt{p(a)}} = \frac{\langle a|\Psi^{(AB)}\rangle}{\sqrt{p(a)}}$$

If we now compute the density operator for system B:

$$\rho^{(B)} = \sum_a p(a)|\hat{\Psi}_a^{(B)}\rangle\langle\hat{\Psi}_a^{(B)}|$$

$$= \sum_a \langle a|\Psi^{(AB)}\rangle\langle\Psi^{(AB)}|a\rangle$$

$$= \sum_a \langle a|\rho^{(AB)}|a\rangle$$

Thus we see that $\rho^{(B)}$, the density operator for the subsystem B is given by tracing over the subsystem A.

Partial Trace:

Tracing over a system involves the mathematical operation of partial tracing which is defined using product states:

If $Q^{AB} = |\alpha^{(A)}, \phi^{(B)}\rangle\langle\beta^{(A)}, \psi^{(B)}|$

Then $Q^A = Tr_B\, Q^{AB} = \langle\phi^{(B)}|\psi^{(B)}\rangle\; |\alpha^{(A)}\rangle\langle\beta^{(A)}|$

$$= \sum_b \langle\phi^{(B)}|b\rangle\langle b|\psi^{(B)}\rangle\; |\alpha^{(A)}\rangle\langle\beta^{(A)}|$$

$$= \sum_b \langle b|\beta^{(A)}, \psi^{(B)}\rangle\langle\alpha^{(A)}, \phi^{(B)}|b\rangle$$

$$= \sum \langle b|Q^{AB}|b\rangle$$

Expectation Values of Operations of A Subsystem:

Suppose $\mathcal{O}_A$ is an operator / Observable of the subsystem A. If we compute $\langle \mathcal{O}_A \rangle$ then we first extend $\mathcal{O}_A$ to the system AB by $\mathcal{O}_A \to \mathcal{O}_A \otimes \mathbb{1}_B$.

Then if the system in the joint state $|\Psi^{(AB)}\rangle$ then

$$\langle \mathcal{O}_A \rangle = \langle \Psi^{(AB)} | \mathcal{O}_A \otimes \mathbb{1}_B | \Psi^{(AB)} \rangle$$

$$= \sum_b \langle \Psi^{(AB)} | \mathcal{O}_A \otimes |b\rangle\langle b| \, |\Psi^{(AB)} \rangle$$

$$= \sum_b \underbrace{\langle \Psi^{(AB)} | b \rangle}_{\in \mathcal{H}_A^*} \mathcal{O}_A \underbrace{\langle b | \Psi^{(AB)} \rangle}_{\in \mathcal{H}_A}$$

$$= \mathrm{Tr}_A \underbrace{\sum_b \langle b | \Psi^{(AB)} \rangle \langle \Psi^{(AB)} | b \rangle}_{\rho^{(A)}} \mathcal{O}_A = \mathrm{Tr}_A \, \rho^{(A)} \mathcal{O}_A$$

The Two Interpretations of Density Operators:

Interpretation 1: Density operator for a system describes our lack of knowledge about how the state was prepared. This is the statistical ensemble picture.

Interpretation 2: If systems A & B share an entangled state but the two systems cannot communicate then $\rho^{(A)} = \mathrm{Tr}_B \, \rho^{(AB)}$

describes the state of the subsystem A.

The two interpretations are related: If Bob makes a measurement on B but cannot communicate the result of his measurement to Alice then we see that Interpretation 2 $\longrightarrow$ Interpretation 1.

Schmidt Decomposition:

Suppose we have a density matrix ρ_P defined on a system P. We can then diagonalize ρ_P in some orthonormal basis $\{|k^P\rangle\}$:

$$\rho_P = \sum_k \lambda_k |k^P\rangle\langle k^P|$$

where $\lambda_k \geq 0$ with $\sum_{k=1}^{\dim \mathcal{H}_P} \lambda_k = 1$. This is just the spectral decomposition of ρ_P. Now suppose that there exists an auxiliary system Q such that the combined system PQ admits an entangled state $|\Psi^{PQ}\rangle \in \mathcal{H}_P \otimes \mathcal{H}_Q$ st that with $\rho_{PQ} = |\Psi^{PQ}\rangle\langle\Psi^{PQ}|$ we have:

$$\rho_P = \mathrm{Tr}_Q \, \rho_{PQ}$$

For a generic basis $\{|\phi^Q\rangle\}$ of Q we can write:

$$|\Psi^{PQ}\rangle = \sum_{\phi,k} c_{\phi k} |k^P\rangle|\phi^Q\rangle$$

$$= \sum_k |k^P\rangle \sum_\phi c_{\phi k} |\phi^Q\rangle$$

$$\boxed{|\Psi^{PQ}\rangle = \sum_k |k^P\rangle|\Psi_k^Q\rangle}$$

where $|\Psi_k^Q\rangle \equiv \sum_\phi c_{\phi k} |\phi^Q\rangle$.

So now $\rho_P = \mathrm{Tr}_Q |\Psi^{PQ}\rangle\langle\Psi^{PQ}|$

$$= \sum_{kk'} |k^P\rangle\langle k'^P| \langle\Psi_k^Q|\Psi_{k'}^Q\rangle$$

Comparing this with $\rho_P = \sum_k \lambda_k |k\rangle\langle k|$ we see that $\langle\Psi_k^Q|\Psi_{k'}^Q\rangle = \lambda_k \delta_{kk'}$

We can then introduce the orthonormal set: $|\Psi_k^Q\rangle = \sqrt{\lambda_k}\,|k^Q\rangle$

Then we write $|\Psi^{PQ}\rangle$ as:

$$\boxed{|\Psi^{PQ}\rangle = \sum_k \sqrt{\lambda_k}\,|k^P\rangle|k^Q\rangle}$$

Schmidt Decomposition

$\sqrt{\lambda_k} \rightarrow$ Schmidt coefficients.

Comments:

1. If $\dim \mathcal{H}^P = \dim \mathcal{H}^Q = d$, then the expansion of an entangled state in a generic product basis $\{|\phi^P, \chi^Q\rangle\}$ would have d^2 terms in general. The Schmidt decomposition has at most only d terms with real coefficients $\sqrt{\lambda_k}$. These coefficients are known as the Schmidt coefficients. The Schmidt decomposition is specific to the entangled state we have chosen.

2. For an entangled state at least two Schmidt coefficients must be non-zero.

3. If the dimensions of the two Hilbert spaces are unequal then the number of terms in the decomposition will be determined by the dimension of the smaller dimensional Hilbert space.

4. The Schmidt basis is a special basis (when the two dimensions are the same). $\{|k^P\rangle\}$ & $\{|k^Q\rangle\}$ are eigenbases for ρ_P & ρ_Q, respectively.

5. $|\psi^{PQ}\rangle$ is known as the purification of ρ_P. For a given mixed state ρ_P one can always find an auxiliary quantum system Q such that there exists a pure state $|\psi^{PQ}\rangle \in \mathcal{H}_P \otimes \mathcal{H}_Q$ s.t. $\rho_P = \mathrm{Tr}_Q |\psi^{PQ}\rangle\langle\psi^{PQ}|$.

Example: For a pair of qubits, find the Schmidt decomposition for the state

$$|\Upsilon\rangle = \frac{1}{\sqrt{2}}\left(|0,0\rangle + |1,+\rangle\right)$$

Entanglement Entropy:

If we take the partial trace of a subsystem of an entangled state we find that the remaining subsystem is described by a mixed state. One can then compute the von Neumann entropy of the remaining density operator and it will be non-zero only if the original state was an entangled state. This is called entanglement entropy:

$$\rho_A = \mathrm{Tr}_B\, \rho_{AB}$$

$$S_{EE} = -\mathrm{Tr}\left(\rho_A \log \rho_A\right).$$

Ex: Compute the entanglement entropy of the state $|\Phi_-^\alpha\rangle = \dfrac{\alpha|01\rangle - (1-\alpha)|10\rangle}{N_\alpha}$ for $\alpha \in [0,1]$ and $N_\alpha \to \alpha$-dependent normalization constant. Show that it vanishes for $\alpha = 0$ & 1 and is maximized for $\alpha = 0.5$. What is $|\Phi_-^{\frac{1}{2}}\rangle$?