These exercises show that measurement of the single qubit of system A in $|\Psi\rangle = (|0_A 0_B\rangle + |1_A 1_B\rangle)/\sqrt{2}$ gives the same probability distribution of outcomes as the probabilistic mixture of $|0_A\rangle$ and $|1_A\rangle$ with probability 0.5.
Therefore, no observable on the system A can distinguish $|\Psi\rangle$ and the probabilistic mixture of $|0_A\rangle$ and $|1_A\rangle$ with probability 0.5.

2009-7-2

securacy of superdense coding

In superdense coding, the sender sends

$$\begin{aligned} & (U \otimes I)(|0_A 0_B\rangle + |1_A 1_B\rangle)/\sqrt{2} \\ = \; & (U|0_A\rangle \otimes |0_B\rangle + U|1_A\rangle \otimes |1_B\rangle)/\sqrt{2} \end{aligned}$$

for some 2×2 unitary matrix U.
Its corresponding density operator is

$$\frac{1}{2}(U|0_A\rangle\langle 0_A|U^* \otimes |0_B\rangle\langle 0_B| + U|1_A\rangle\langle 1_A|U^* \otimes |1_B\rangle\langle 1_B| + U|0_A\rangle\langle 1_A|U^* \otimes |0_B\rangle\langle 1_B| + U|1_A\rangle\langle 0_A|U^* \otimes |1_B\rangle\langle 0_B| \quad (1)$$

Observe that $\mathrm{Tr}[|0_B\rangle\langle 1_B|] = \mathrm{Tr}[|1_B\rangle\langle 0_B|] = 0$ and $\mathrm{Tr}[|0_B\rangle\langle 0_B|] = \mathrm{Tr}[|1_B\rangle\langle 1_B|] = 1$.
Thus, the partial trace of (1) over B is

$$\begin{aligned} & \frac{1}{2}(U|0_A\rangle\langle 0_A|U^* + U|1_A\rangle\langle 1_A|U^*) \\ = \; & \frac{1}{2}(U(|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|)U^*) \\ = \; & UIU^*/2 \\ = \; & I/2 \end{aligned}$$

Whichever information the sender sends, the transmitted state is the same!! Moreover, it cannot be distinguished with sending $|0\rangle$ and $|1\rangle$ with equal probability.

2009-7-3

Properties of density operators

What kind of a matrix ρ can be a density matrix?

1. $\rho = \rho^*$ (Hermitian matrix).
2. All eigenvalules of ρ is nonnegative.
3. $\mathrm{Tr}\rho = 1$.

The state represented by a state vector is called pure state. The above three conditions gurantees that ρ can be represented as a probabilistic mixture of pure states.
Let the spectral decomposition of ρ be

$$\rho = \sum_{i=1}^{n} \lambda_i |\varphi_i\rangle\langle\varphi_i|.$$

By the second condition, $\lambda_i \geq 0$ for all i, and by the third condition $\lambda_1 + \cdots + \lambda_n = 1$.
ρ can be seen as the state of the system whose state is $|\varphi_i\rangle$ with probability λ_i.

2009-7-4

State after measurement

Let M be an observable with spectral decomposition

$$M = \sum_{i=1}^{n} iP_i.$$

After getting the outcome i, the state becomes

$$\frac{P_i \rho P_i}{\mathrm{Tr}[P_i \rho P_i]} = \frac{P_i \rho P_i}{\mathrm{Tr}[\rho P_i]}. \tag{2}$$

This is consistent with the definition of state change of pure states (Exercise 2).

Locality

It is believed that the effect of physical action does not propagate faster than light. No physical phenomenon violating the above conjecture has been found.
The axioms of quantum theory negates the above conjecture, if we think the density operator or the state vector represents "physical reality."

Suppose that we measure Z of the first qubit of $(|00\rangle + |11\rangle)/\sqrt{2}$. After measurement, the state is $|00\rangle$ or $|11\rangle$ depending on the measurement outcome.
If the first qubit and the second qubit is spacially far apart, then the above state change implies that the effect of measurement propagete faster than light.
Do you think that the state vector represents "physical reality"? If you disagree that the state vector represents "physical reality", (I disagree), do you see how the research on quantum information processing has the significance and importance?

2009-7-6

No cloning theorem

Quantum information cannot be copied. Suppose that there is a unitary operator U such that for an arbitrary state $|\varphi\rangle$ and a fixed state $|\psi\rangle$

$$U(|\varphi\rangle \otimes |\psi\rangle) = |\varphi\rangle \otimes |\varphi\rangle. \tag{3}$$

Then U is not linear (Exercise. Hint: consider what happens if we try to copy $|\varphi_1\rangle + |\varphi_2\rangle$).
Therefore, there is no unitary operator copying quantum information.

Classical error correction is done by adding redundant information by copying original information. Because of the no cloning theorem, error correction for quantum information had been thought to be impossible.

The quantum error correction is a useful tool for understanding the security of quantum cryptography. (But I will not teach it.)

Exercise

Submit your answer to the box in front of Room 311, S3 building, by 17:00 Thursday, if you don't finish by 12:10.

1. Prove Eq. (2).

2. When ρ is a pure state $|\varphi\rangle\langle\varphi|$, is the state after measurement defined by Eq. (2) the same as $P_i|\varphi\rangle/\||P_i|\varphi\rangle\|$? P_i is the same as Eq. (2). Do not answer "One is a vector while another is a matrix. Thus, they are different." I am asking whether or not they corresponds to the same physical state.

3. Let $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Suppose that we measure Z of the first qubit and Z of the second qubit ($\neq$ measurement of $Z \otimes Z$). There are four possible measuremnet outcomes $(\pm 1, \pm 1)$. Compute the probability of getting each outcome. This exercise shows that $|\Phi\rangle$ can be used for sharing a secret random bit.

4. Compute eigenvalues, eigenvectors, and spectral decomposition of

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

5. Repeat Exercise 3 with Z replaced with Y. This exercise shows that the measurement outcomes for

$|\Phi\rangle$ do not always coincide. (hint: Let $|a\rangle$, $|b\rangle$ be the eigenvectors of Y with $\||a\rangle\| = \||b\rangle\| = 1$. Prove $|00\rangle + |11\rangle = |ab\rangle + |ba\rangle$, which can decrease the difficulty of computation.)
6. Explain why Eq. (3) is not linear.
7. If your answers to the previous exercises were evaluated as incorrect, please indicate whether or not you agree to that evaluation. Write which part in today's lecture was difficult for your understanding.

I will explain the quantum factoring algorithm in the following steps:

1. the quantum Forier transform,
2. phase estimation of an eigenvalue of a unitary operator,
3. finding the order of an integer modulo another integer.

If you want other topics, please write them in your answer.