Problem 1 Please describe the EPR paradox introduced by Einstein, Podolsky, Rosen at 1935 , and explain the contradiction between quantum theory and local realism theory.

Solution: According to the EPR paper, a local realism theory should satisfy the following two conditions:

- Realism: if, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists a physical reality corresponding to this physical quantity. And every element of physical reality must have a counter part in the physical theory.
- Locality: The measurement performed by spatially separated parties should not have any causal correlation.

EPR paradox states that, in quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality.

Original EPR paradox: Supposing that a source (at $x = x_0$) created two particles A and B which moving opposite directions with the same momentum, the wave function is then

$$\Psi(x_1, x_2) = \int \varphi_p^A(x_1)\varphi_{-p}^B(x_2)dp = \int e^{i\frac{px_1}{\hbar}} e^{i\frac{-p(x_2-x_0)}{\hbar}} dp, \tag{1}$$

where $\varphi_p^A(x_1), \varphi_{-p}^B(x_2)$ are eigenstate of momentum operators P^A, P^B of system A and B with respective eigenvalues p and $-p$.

We can rewrite the state with coordinate eigenstates, suppose that the eigenstates corresponding to X^A (with eigenvalue x) and X^B (with eigenvalue $x_0 - x$) are respectively

$$\psi_x^A(x_1) = \delta(x_1 - x), \quad \psi_{x_0-x}^B(x_2) = \delta(x_2 - (x_0 - x)) = \int e^{i\frac{p(x-x_2+x_0)}{\hbar}} dp, \tag{2}$$

it's easily checked that

$$\Psi(x_1, x_2) = \int \psi_x^A(x_1)\psi_{x_0-x}^B(x_2)dp. \tag{3}$$

Now A and B are space-like separated, suppose that we choose to measure momentum for A and obtain the eigenvalue p, then particle B must have be in the momentum eigenstate with eigenvalue $-p$ after the measument; similarly if we choose to measure position for A and obtain the value x, then particle B must be in the coordination eigenstate with eigenvalue $x_0 - x$. Notice that in this process, only A is measured and B is spatially separated with A, thus B is by no way disturbed, thus the momentum $-p$ and position $x_0 - x$ must be elements of reality, this implies that the eigenstates of momentum operator and position operation must have a simultaneous reality, but these two operators are non-commuting, then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality.

Bohm's version of EPR paradox: Suppose that spatially separated Alice and Bob pre-share a singlet state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle),$$

notice that fact that for singlet state, Alice and Bob choose to measure spin in any directions $\vec{v} \cdot \vec{\sigma}$, their outcomes are anti-correlated.

Now suppose that Alice choose to measure σ_z and obtain the outcome z, then Bob's state must be in $|-z\rangle$; and when Alice choose to measure σ_x and obtain the outcome x, then Bob's state must be in $|-x\rangle$. Since in this process, Alice in no way disturbing the system of Bob, the σ_z eigenstates $|-z\rangle$ and σ_x eigenstates $|-x\rangle$ for Bob must have simultaneous reality, but σ_z and σ_x are non-commuting, then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. ■

Problem 2 (1) Prove the CHSH inequality

$$\left|E\left(A_1B_1\right)+E\left(A_1B_2\right)+E\left(A_2B_1\right)-E\left(A_2B_2\right)\right|\leq 2$$

in which $E\left(A_iB_j\right)$ is the expectation value of the correlation experiment A_i, B_j.

(2) Give the maximum violation allowed by quantum mechanics, and the correspond- ing quantum state and measurement operator.

Solution:

(1) Notice local hidden variable theory assume that when Alice and Bob perform measurements A and B the joint probability for their measurement is controlled by a hidden variable ξ with probability $p(\xi)$, and there is no correlations between them, more precisely

$$p(a,b)=p(a,b|A,B)=\sum_{\xi}p(\xi)p(a|A,\xi)p(b|B,\xi). \tag{4}$$

The form of expression is a result of locality of realism assumptions.

We now prove Bell inequality using this assumption. From four correlators

$$E(A_1,B_1)=\langle A_1\otimes B_1\rangle=\sum_{a_1=\pm1}\sum_{b_1=\pm1}a_1b_1p(a_1,b_1) \tag{5}$$

$$E(A_1,B_2)=\langle A_1\otimes B_2\rangle=\sum_{a_1=\pm1}\sum_{b_2=\pm1}a_1b_2p(a_1,b_2) \tag{6}$$

$$E(A_2,B_1)=\langle A_2\otimes B_1\rangle=\sum_{a_2=\pm1}\sum_{b_1=\pm1}a_2b_1p(a_2,b_1) \tag{7}$$

$$E(A_2,B_2)=\langle A_2\otimes B_2\rangle=\sum_{a_2=\pm1}\sum_{b_2=\pm1}a_2b_2p(a_2,b_2) \tag{8}$$

we have

$$\begin{aligned}&E\left(A_1,B_1\right)+E\left(A_1,B_2\right)+E\left(A_2,B_1\right)-E\left(A_2,B_2\right)\\=&\sum_{a_1=\pm1}\sum_{b_1=\pm1}a_1b_1p(a_1,b_1)+\sum_{a_1=\pm1}\sum_{b_2=\pm1}a_1b_2p(a_1,b_2)\\&+\sum_{a_2=\pm1}\sum_{b_1=\pm1}a_2b_1p(a_2,b_1)-\sum_{a_2=\pm1}\sum_{b_2=\pm1}a_2b_2p(a_2,b_2)\end{aligned} \tag{9}$$

Then using the local hidden variable model assumption (4), we have

$$\begin{aligned}&\sum_{a_1=\pm1}\sum_{b_1=\pm1}a_1b_1\sum_{\xi}p(a_1|\xi)p(b_1|\xi)p(\xi)\\&+\sum_{a_1=\pm1}\sum_{b_2=\pm1}a_1b_2\sum_{\xi}p(a_1|\xi)p(b_2|\xi)p(\xi)\\&+\sum_{a_2=\pm1}\sum_{b_1=\pm1}a_2b_1\sum_{\xi}p(a_2|\xi)p(b_1|\xi)p(\xi)\\&-\sum_{a_2=\pm1}\sum_{b_2=\pm1}a_2b_2\sum_{\xi}p(a_2|\xi)p(b_2|\xi)p(\xi)\end{aligned} \tag{10}$$

After simplification we obtain

$$\begin{aligned}&\sum_{\xi}p(\xi)\{\sum_{a_1=\pm1}a_1p(a_1|\xi)[\sum_{b_1=\pm1}b_1p(b_1|\xi)+\sum_{b_2=\pm1}b_2p(b_2|\xi)]\\&+\sum_{a_2=\pm1}a_2p(a_2|\xi)[\sum_{b_1=\pm1}b_1p(b_1|\xi)-\sum_{b_2=\pm1}b_2p(b_2|\xi)]\}\end{aligned} \tag{11}$$

Problem 2 continued on next page...

Let $x_1 = \sum_{a_1=\pm1} a_1 p(a_1|\xi)$, $x_2 = \sum_{a_2=\pm1} a_2 p(a_2|\xi)$,$y_1 = \sum_{b_1=\pm1} b_1 p(b_1|\xi)$,and $y_2 = \sum_{b_2=\pm1} b_2 p(b_2|\xi)$ and notice that $|x_1|, |x_2|, |y_1|, |y_2| \leq 1$, then we have

$$\begin{aligned}
&|\langle A_1 \otimes B_1\rangle + \langle A_1 \otimes B_2\rangle + \langle A_2 \otimes B_1\rangle - \langle A_2 \otimes B_2\rangle| \\
=&|\sum_{\xi} p(\xi)\{\sum_{a_1=\pm1} a_1 p(a_1|\xi)[\sum_{b_1=\pm1} b_1 p(b_1|\xi) + \sum_{b_2=\pm1} b_2 p(b_2|\xi)] \\
&+ \sum_{a_2=\pm1} a_2 p(a_2|\xi)[\sum_{b_1=\pm1} b_1 p(b_1|\xi) - \sum_{b_2=\pm1} b_2 p(b_2|\xi)]\}| \\
\leq&\sum_{\xi} p(\xi)|x_1(y_1+y_2) + x_2(y_1-y_2)| \\
\leq&\sum_{\xi} p(\xi)(|x_1||y_1+y_2| + |x_2||y_1-y_2|) \\
\leq&\sum_{\xi} p(\xi)(|y_1+y_2| + |y_1-y_2|)
\end{aligned}$$

Since $-1 \leq y_1, y_2 \leq 1$, we see that $|y_1+y_2| + |y_1-y_2| \leq 2$ this implies that

$$\left|E(A_1B_1) + E(A_1B_2) + E(A_2B_1) - E(A_2B_2)\right| \leq 2. \tag{12}$$

We thus complete the proof.

(2) The maximum quantum violation is $2\sqrt{2}$.

We can choose the state as singlet state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{13}$$

thus for any operators $A = \vec{a}\cdot\vec{\sigma}$ and $B = \vec{b}\cdot\vec{\sigma}$ we have

$$\left\langle \psi^- |A \otimes B| \psi^- \right\rangle = -\vec{a}\cdot\vec{b} = -\cos\theta \tag{14}$$

where θ is the angle between $\vec{a}$ and $\vec{b}$.

We can choose

$$A_1 = \sigma_z, \quad A_2 = \sigma_x \tag{15}$$

$$B_1 = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z), \quad B_2 = \frac{1}{\sqrt{2}}(-\sigma_x + \sigma_z) \tag{16}$$

this implies that

$$\begin{aligned}
&\left\langle \psi^- |A_1 \otimes B_1| \psi^- \right\rangle = \left\langle \psi^- |A_1 \otimes B_2| \psi^- \right\rangle = \left\langle \psi^- |A_2 \otimes B_1| \psi^- \right\rangle = -1/\sqrt{2} \\
&\left\langle \psi^- |A_2 \otimes B_2| \psi^- \right\rangle = 1/\sqrt{2}
\end{aligned} \tag{17}$$

Thus $|\langle\psi^-|C|\psi^-\rangle| = 4/\sqrt{2} = 2\sqrt{2}$. The upper bound is reachable, we complete our proof. ■

Problem 3 (Tsirelson's inequality) Suppose $Q = \vec{q}\cdot\vec{\sigma}, R = \vec{r}\cdot\vec{\sigma}, S = \vec{s}\cdot\vec{\sigma}, T = \vec{t}\cdot\vec{\sigma}$, where $\vec{q}, \vec{r}$, $\vec{s}$ and $\vec{t}$ are real unit vectors in three dimensions and $\vec{\sigma} = \left(\sigma_x, \sigma_y, \sigma_z\right)$. Show that

$$(Q\otimes S + R\otimes S + R\otimes T - Q\otimes T)^2 = 4I + [Q,R]\otimes[S,T]$$

Use this result to prove that

$$\langle Q\otimes S\rangle + \langle R\otimes S\rangle + \langle R\otimes T\rangle - \langle Q\otimes T\rangle \leq 2\sqrt{2}$$

Problem 3 continued on next page...

Solution: For convenience, we first denote $A_1 = R$, $A_2 = Q$ $B_1 = S$ and $B_2 = T$.
To prove the Tsirelson's bound, first notice that A_i,B_j are all spin operators, thus

$$A_1^2 = A_2^2 = B_1^2 = B_2^2 = I, \quad [A_i, B_j] = 0 \ \ \forall i, j = 1, 2. \tag{18}$$

From the expression

$$C = A_1 \otimes B_1 + A_1 \otimes B_2 + A_2 \otimes B_1 - A_2 \otimes B_2 \tag{19}$$

we have

$$\begin{aligned} C^2 =& 4I \otimes I - A_1A_2 \otimes B_1B_2 + A_2A_1 \otimes B_1B_2 + A_1A_2 \otimes B_2B_1 - A_2A_1 \otimes B_2B_1 \\ =& 4I \otimes I - [A_1, A_2] \otimes [B_1, B_2] \end{aligned} \tag{20}$$

We can then use the definition of sup-norm for an operator

$$\|T\|_{\sup} = \sup_{|\psi\rangle} \left(\frac{\||T|\psi\rangle\|}{\||\psi\rangle\|} \right) = \sup_{|\psi\rangle, \||\psi\rangle\|=1} \left(\||T|\psi\rangle\| \right) \tag{21}$$

For Hermitian operator, we know that $\|T\|_{\sup}$ is the maximum value of the absolute value of their eigenvalues, thus

$$\|A_1\|_{\sup} = \|A_2\|_{\sup} = \|B_1\|_{\sup} = \|B_2\|_{\sup} = 1. \tag{22}$$

Notice that

$$\begin{aligned} &\|TS\|_{\sup} \leq \|T\|_{\sup} \cdot \|S\|_{\sup} \\ &\|T + S\|_{\sup} \leq \|T\|_{\sup} + \|S\|_{\sup} \\ &|\langle\psi|T|\psi\rangle| \leq \|T\|_{\sup}, \text{for all states} \psi \end{aligned} \tag{23}$$

thus

$$\|A_1A_2 \otimes B_1B_2\|_{\sup} \leq \|A_1\|_{\sup} \|A_2\|_{\sup} \|B_1\|_{\sup} \|B_2\|_{\sup} \tag{24}$$

With these preparation, from expression (20) we have

$$\begin{aligned} \left\|C^2\right\|_{\sup} \leq& 4\|I \otimes I\|_{\sup} + \|A_1A_2 \otimes B_1B_2\|_{\sup} + \|A_2A_1 \otimes B_1B_2\|_{\sup} \\ &+ \|A_1A_2 \otimes B_2B_1\|_{\sup} \|A_2A_1 \otimes B_2B_1\|_{\sup} \\ \leq& 4 + 4\|A_1\|_{\sup} \cdot \|A_2\|_{\sup} \cdot \|B_1\|_{\sup} \cdot \|B_2\|_{\sup} = 8 \end{aligned} \tag{25}$$

Since C is Hermitian, we have $\left\|C^2\right\|_{\sup} = \|C\|_{\sup}^2$. From expression (25) we obtain $\|C\|_{\sup}^2 \leq 8$, this implies that

$$\|C\|_{\sup} \leq 2\sqrt{2}. \tag{26}$$

Using the properties of sup-norm, we see that for arbitrary quantum state we have

$$|\langle C\rangle| \leq \|C\|_{\sup} \leq 2\sqrt{2} \tag{27}$$

This implies

$$\left|E(A_1B_1) + E(A_1B_2) + E(A_2B_1) - E(A_2B_2)\right| \overset{LHV}{\leq} 2 \overset{Q}{\leq} 2\sqrt{2}. \tag{28}$$

From problem 3 we see that the quantum upper bound is reachable. We thus obtain the result we want. ■

Problem 4 Consider the CHSH game in which the referee chooses questions $r, s \in \{0,1\}$ uniformly, and Alice and Bob must each answer a single bit: a for Alice, b for Bob, in which $a, b \in \{0,1\}$. They win if $a \oplus b = r \wedge s$ and lose otherwise.

(1) Prove that the maximum probability of winning with a classical strategy is $\frac{3}{4}$.

(2) Suppose Alice and Bob share a maximum quantum entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, please derive the maximum probability of winning and give the corresponding quantum strategy.

Solution:

(1) Suppose that Alice and Bob are given bits r, s with for values $= 0,0; 0,1; 1,0; 1,1$ with probability $1/4$ respectively. Suppose there is classical black box (can be regarded as some kind of classical appratus) for Alice and Bob, which can generate output a, b for input r, s with probability $p(ab|rs)$. In a classical world for where local realism holds, we known from Bell-CHSH inequality that

$$\begin{aligned}&[p(00|00) + p(11|00) - p(01|00) - p(10|00)] + [p(00|01) + p(11|01) - p(01|01) - p(10|01)] \\ &+[p(00|10) + p(11|10) - p(01|10) - p(10|10)] + [-p(00|11) - p(11|11) + p(01|11) + p(10|11)] \leq 2.\end{aligned} \tag{29}$$

Using the fact that $p(00|rs) + p(11|rs) + p(01|rs) + p(10|rs) = 1$ for $r, s = 0, 1$. We obtain that

$$2\{[p(00|00) + p(11|00)] + [p(00|01) + p(11|01)] + [p(00|10) + p(11|10)] + [p(01|11) + p(10|11)]\} - 4 \leq 2, \tag{30}$$

which implies that

$$[p(00|00) + p(11|00)] + [p(00|01) + p(11|01)] + [p(00|10) + p(11|10)] + [p(01|11) + p(10|11)] \leq 3. \tag{31}$$

Notice that the left hand sider of the above equation is nothing but the unnormalized probability for the $a \oplus b = x \wedge y$ condition to hold. Since each kind of input is of probability $1/4$, we thus have

$$\begin{aligned}p_{succ} =&\frac{1}{4}[p(00|00) + p(11|00)] + \frac{1}{4}[p(00|01) + p(11|01)] \\ &+ \frac{1}{4}[p(00|10) + p(11|10)] + \frac{1}{4}[p(01|11) + p(10|11)] \quad \leq \frac{3}{4}.\end{aligned} \tag{32}$$

Thus the maximum classical success probability is $3/4$.

(2) The maximum success probability that quantum strategies can reach is $\frac{2+\sqrt{2}}{4} \simeq \frac{3.414}{4}$ which is greater than $3/4$.

Suppose Alice and Bob share the states

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle = |11\rangle), \tag{33}$$

Notice that for unit vectors $\vec{a}, \vec{b}$ in xz-plane, we have

$$\langle\psi|(\vec{a} \cdot \vec{\sigma}) \otimes (\vec{b} \cdot \vec{\sigma})|\psi\rangle = \vec{a} \cdot \vec{b} = \cos\theta \tag{34}$$

where θ is the angle between $\vec{a}$ and $\vec{b}$. (Notice that for general vector with nonzero y component, this is not true).

Define

$$A_1 = \sigma_z, \quad A_2 = \sigma_x, \tag{35}$$

$$B_1 = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z), \quad B_2 = \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x). \tag{36}$$

We known that

$$E(A_1, B_1) + E(A_1, B_2) + E(A_2, B_1) - E(A_2, B_2) = 2\sqrt{2}. \tag{37}$$

Problem 4 continued on next page...

Then the quantum strategy works as follows, when Alice receive $r = 0$ she choose A_1 to measure, when she receive $r = 1$, She choose A_2 to measure; similarly, When Bob receive $s = 0$ he choose A_1 to measure, when he receive $r = 1$, he choose A_2 to measure.

Alice and Bob denote the outcome of their measurements as a and b respectively. In this way, we have

$$p(00|00) + p(11|00) = \frac{1 + E(A_1, B_1)}{2} \tag{38}$$

$$p(00|01) + p(11|01) = \frac{1 + E(A_1, B_2)}{2} \tag{39}$$

$$p(00|10) + p(11|10) = \frac{1 + E(A_2, B_1)}{2} \tag{40}$$

$$p(01|11) + p(10|11) = \frac{1 + E(A_2, B_2)}{2} \tag{41}$$

This implies that

$$\begin{aligned} p_{succ} =& \frac{1}{4}\{[p(00|00) + p(11|00)] + [p(00|01) + p(11|01)] + [p(00|10) + p(11|10)] + [p(01|11) + p(10|11)]\} \\ =& \frac{4 + [E(A_1, B_1) + E(A_1, B_2) + E(A_2, B_1) - E(A_2, B_2]}{2 \times 4} \\ =& \frac{2 + \sqrt{2}}{4} \simeq \frac{3.414}{4} \end{aligned} \tag{42}$$

This shows that quantum strategy has advantages over all possible classical strategies. ■

Problem 5 Consider the GHZ game in which the referee chooses questions $rst \in \{000, 011, 101, 110\}$ uniformly, and Alice, Bob and Charles must each answer a single bit: a for Alice, b for Bob, c for Charles, in which $a, b, c \in \{0, 1\}$. They win if $a \oplus b \oplus c = r \vee s \vee t$ and lose otherwise. Suppose Alice, Bob and Charles share a GHZ state $|\psi\rangle = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$, give a quantum strategy that maximize probability of winning.

Solution: The quantum strategy can reach the a maximum success probability $p_{succ} = 1$.

In this strategy, each of three parties using the same strategy and the strategy works as follows:

- If the question is $q = 1$, then the player performs a Hadamard transform on their qubit of the given state state. If $q = 0$, the player does not perform a Hadamard transform.
- The player measures their qubit in the standard computational basis and sends the measurement outcome to the referee.

To analyze the success probability, let's discuss for different input values of rst respectively:

Case 1: $rst = 000$. The goal is to make $a \oplus b \oplus c = 0$. In this case the players all just measure their qubit, and it is obvious that the results satisfy $a \oplus b \oplus c = 0$ as required.

Case 2: $rst = \{011; 101; 110\}$. The goal is to make $a \oplus b \oplus c = 1$. All three possibilities will work the same way by symmetry, so without loss of generalities, let us assume $rst = 011$. Notice that after receiving the question bit, Alice do nothing but Bob and Charles must first perform Hadamard transformation, recall that

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{43}$$

Thus the resulting state is

$$I \otimes H \otimes H|\psi\rangle = |\varphi\rangle = \frac{1}{2}(|001\rangle + |010\rangle - |100\rangle + |111\rangle) \tag{44}$$

When they measure, the results satisfy $a \oplus b \oplus c = 1$ as required.

No matter in which case, we will with probability 1. Therefore shown that there is a quantum strategy that wins every time, i.e.,$p_{succ} = 1$. ■

Problem 6 Derive the Bell's theorem without inequalities from the GHZ state

$$|\psi\rangle_{GHZ} = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

Solution: Recall that Bell theorem states that quantum mechanics do not satisfy local realism.

Thus to prove Bell theorem using the GHZ state (in fact this is a variation of GHZ state, not GHZ state, but the proof is in the same spirit):

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \tag{45}$$

First, let us observe that it is the unique common eigenstate with eigenvalues being 1 of the following observables: (to simplify the notations, here we use X, Y, Z to denote Pauli matrices)

$$\{Z_A \otimes Z_B \otimes I_C, I_A \otimes Z_B \otimes Z_C, -X_A \otimes X_B \otimes X_C\} \tag{46}$$

Then, we use the above set of observables as the generator to generate the following group:

$$\begin{gathered}\{I_A \otimes I_B \otimes I_C, Z_A \otimes Z_B \otimes I_C, I_A \otimes Z_B \otimes Z_C, Z_A \otimes I_B \otimes Z_C \\ -X_A \otimes X_B \otimes X_C, Y_A \otimes Y_B \otimes X_C, Y_A \otimes X_B \otimes Y_C, X_A \otimes Y_B \otimes Y_C\}\end{gathered} \tag{47}$$

Obviously, the GHZ state is also the eigenstate with eigenvalue being 1 for all the observables in the group. Let's consider four special elements in this group

$$-X_A \otimes X_B \otimes X_C, \tag{48}$$
$$Y_A \otimes Y_B \otimes X_C, \tag{49}$$
$$Y_A \otimes X_B \otimes Y_C, \tag{50}$$
$$X_A \otimes Y_B \otimes Y_C. \tag{51}$$

For a theory satisfying local realism. If we take a measurement of a Pauli operator Λ with $\Lambda \in \{X, Y, Z\}$, we always get its value, 1 or -1. Then, the value of a Pauli matrix $v(\Lambda)$ can take a value 1 or -1. The quantum theory, in the viewpoint of local realistic world, implies that

$$\begin{aligned} -v(X_A)\, v(X_B)\, v(X_C) &= 1 \\ v(Y_A)\, v(Y_B)\, v(X_C) &= 1 \\ v(Y_A)\, v(X_B)\, v(Y_C) &= 1 \\ v(X_A)\, v(Y_B)\, v(Y_C) &= 1 \end{aligned} \tag{52}$$

However, this is impossible because the product of the above four equations leads to a contradiction $-1 = 1$. This means quantum theory does not satisfy Bell local realism assumption, we thus prove the Bell theorem. ■

Problem 7 (1) Write down the communication process of BB84 QKD (Quantum key distribution).

(2) Analyze the security of single-photon BB84 QKD from the principle of quantum mechanics under intercept-resend attack.

(3) Write down the secure key rate formula of single-photon BB84 QKD and explain the relationship with entanglement purification protocol.

(4) Write down the GLLP formula of BB84 QKD and explain the meaning of each item in the formula.

(5) Describe the PNS (photon number split) attack and the principle of decoy QKD protocol.

Solution:

(1) The BB84 protocol works as follows

1. Alice chooses $(4+\delta)n$ random data bits.

Problem 7 continued on next page...

2. Alice chooses a random $(4+\delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1
3. Alice sends the resulting state to Bob.
4. Bob receives the $(4+\delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basis at random.
5. Alice announces b.
6. Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits.
7. Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
8. Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
9. Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

(2) The security of BB84 is guaranteed by no-cloning theorem and uncertainty principle. More precisely, no-cloning theorem prevent the eavesdropper from cloning the unknown state he obtained by intercept the photon sent by Alice and resend it to Bob without being found. Uncertainty relation reflects in the basis must be chosen as eigenstates of some non-commuting observables.

(3) The secure key rate of BB84 protocol is defined as

$$r = \frac{l(n)}{n} \tag{53}$$

where $l(n)$ is the number of generated key bits and the n is the size of the raw key. Asymptotic definition is

$$r' = \lim_{n\to\infty} \frac{l(n)}{n}. \tag{54}$$

Entanglement purification protocol is crucial for proving the security of BB84 protocol. Noticing that entanglement purification protocol is equivalent to error-correcting codes. The original Shor-Preskill paper using one-way entanglement purification protocol to construct a QKD protocol (based on CSS codes), this protocol's security can be proved and the security of this protocol implies the security of BB84. Later, Gottesmann and Lo generalized the idea to two-way entanglement purification protocols. More precisely, the correspondence is

CSS codes:	BB84:
bit-flip error detection $\Leftrightarrow$	advantage distillation
bit flip error correction $\Leftrightarrow$	error correction
phase error correction $\Leftrightarrow$	privacy amplification

(4) The GLLP formula is of the form

$$S \geq 1/2[-Q_\mu \cdot f(E_\mu) \cdot H_2(E_\mu) + Q_1(1 - H_2(e_1))]. \tag{55}$$

where

- Q_μ is total number of detection events of signals. E_μ is overall bit error rate of signals.
- Q_1 is the number of detection events due to single photon states.
- e_1 is the bit error rate for single photon state.

Problem 7 continued on next page...

- $f(e) \geq 1$ is the error correction efficiency.

Notice that $-Q_\mu \cdot f(E_\mu) \cdot H_2(E_\mu)$ is for error correction and $Q_1(1 - H_2(e_1)$ is for privacy amplification.

(5) In practice, we usually use the weakly coherent optic or parametric down-conversion optic, this makes there may be many photons in the channel. But ideal BB84 protocol require singlet photon in channel (where the security supplied by no-cloning theorem works). Thus there is multi-photon loophole. Since the photon deter can not distinguish photon numbers exactly, there is a possibility for eavesdropper to do Photon Number Splitting (PNS) attack.

In PNS attack, we assume that eavesdropper can perform non-destructive photon number measurement; there is an ideal channel and a quantum memory; the photon detector of Bob can only detect if there is photon or not but can not detect the exact number of photons. The PNS attack works as follows

- Eavesdropper perform non-destructive photon number measurement, if there is no photon, do nothing; if there is one photon, intercept the photon with probability p with p determined by the efficiency η of QKD; if there are many photons, choose one photon to save in his quantum memory and let all other photons be sent to Bob;
- After Alice and Bob compared their basis choice, eavesdropper choose proper basis to measure the photons in his quantum memory and obtain the key.

Decoy state QKD protocol is used to solve the above problem (PNS attack). In decoy state technique, we can use multiple intensity levels at the transmitter's source, i.e. qubits are transmitted by Alice using randomly chosen intensity levels (one signal state and several decoy states), resulting in varying photon number statistics throughout the channel. At the end of the transmission Alice announces publicly which intensity level has been used for the transmission of each qubit. A successful PNS attack requires maintaining the bit error rate (BER) at the receiver's end, which can not be accomplished with multiple photon number statistics. By monitoring BERs associated with each intensity level, the two legitimate parties will be able to detect a PNS attack, with highly increased secure transmission rates or maximum channel lengths, making QKD systems suitable for practical applications. ■

Problem 8 Quantum teleportation is a process by which quantum information can be transmitted from one location to another, with the help of quantum entanglement. Suppose the initial states are

$$|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1, |\psi\rangle_{23} = \frac{1}{\sqrt{2}}\left(|0\rangle_2|0\rangle_3 + |1\rangle_2|1\rangle_3\right)$$

The state of the particle 1 can be transmitted to the particle 3 by quantum teleportation.

(1) Describe the process of the quantum teleportation protocol and show that particle 3 is projected onto the same state as particle 1 after quantum teleportation.

(2) Explain why we can't use it to achieve superluminal communication.

Solution: (1) The teleportation need to communicate two classical bits to achieve the goal to transmit a qubit by using the pre-shared Bell states. The protocol works as follows

Step 1. A Bell state $|\psi\rangle_{23} = \frac{1}{\sqrt{2}}\left(|00\rangle_{23} + |11\rangle_{23}\right)$ is generated, one qubit (labelled as 2) sent to Alice, the

Problem 8 continued on next page...

other (labelled as 3) to Bob. Alice hold another qubit $|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$. Thus their state is

$$\begin{aligned}
|\psi\rangle_1|\psi\rangle_{23} =& \left(\alpha|0\rangle_1 + \beta|1\rangle_1\right)\frac{1}{\sqrt{2}}\left(|00\rangle_{23} + |11\rangle_{23}\right) \\
=& \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle) \\
=& \frac{1}{\sqrt{2}}\left(\alpha\frac{1}{\sqrt{2}}\left(|\phi^+\rangle + |\phi^-\rangle\right)|0\rangle + \alpha\frac{1}{\sqrt{2}}\left(|\psi^+\rangle + |\psi^-\rangle\right)|1\rangle\right. \\
&\left. + \beta\frac{1}{\sqrt{2}}\left(|\psi^+\rangle - |\psi^-\rangle\right)|0\rangle + \beta\frac{1}{\sqrt{2}}\left(|\phi^+\rangle - |\phi^-\rangle\right)|1\rangle\right) \\
=& \frac{1}{2}\left(|\phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + |\phi^-\rangle(\alpha|0\rangle - \beta|1\rangle)\right. \\
&\left. + |\psi^+\rangle(\beta|0\rangle + \alpha|1\rangle) + |\psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle)\right).
\end{aligned}$$

Step 2. At Alice's side, a Bell measurement of particle 1 and particle 2 is performed, yielding one of four measurement outcomes, which can be encoded in two classical bits of information in the following way:

$$|\phi^+\rangle : 00; \quad |\phi^-\rangle : 01; \quad |\psi^+\rangle : 10; \quad |\psi^-\rangle : 11. \tag{57}$$

Then Alice sends the Bell measurement result to Bob using a classical channel.

Step 3. When received Alice's two-bit information, Bob do the following: (a) for 00 he do nothing, and obtain the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$; (b) for 01, he perform σ_z, he obtain the state $\sigma_z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle$; (c) for 10, he perform σ_x, he obtain $\sigma_x(\beta|0\rangle + \alpha|1\rangle) = \alpha|0\rangle + \beta|1\rangle$; (d) for 11, he perform $\sigma_z\sigma_x$, he obtain $\sigma_z\sigma_x(-\beta|0\rangle + \alpha|1\rangle)$.

In this way Alice and transmit $|\psi\rangle$ to Bob by sending two classical bits with the pre-shared Bell.

(2) Notice that to achieve the quantum teleportation, two classical bits which encodes the information of the choice of Bell basis must be sent from Alice to Bob. Without knowledge of the Bell measurement's results, Bob can't turn the state of particle 3 into the Alice's original state. His state is a uniform probabilistic mixture of four states

$$\alpha|0\rangle \pm \beta|1\rangle; \quad \pm\beta|0\rangle + \alpha|1\rangle. \tag{58}$$

Which means that the state for Bob is maximally mixed state $\rho_3 = \frac{I}{2}$. This can also be checked by taking partial trace $\rho_3 = \mathrm{Tr}_{12}\left(\rho_{123}\right) = \frac{I}{2}$. There is no information Bob can infer to obtain the information of the state that Alice sent. Since classical communication cannot be superluminal, thus this cannot be used to achieve superluminal communication. ■

Problem 9 Suppose two EPR sources produce two pairs of entangled photons, pair 1-2 and pair 3-4. The initial states are

$$|\psi\rangle_{12} = \frac{1}{\sqrt{2}}\left(|00\rangle_{12} - |11\rangle_{12}\right), |\psi\rangle_{34} = \frac{1}{\sqrt{2}}\left(|01\rangle_{34} + |10\rangle_{34}\right)$$

One photon from each pair (say photons 2 and 3) is subjected to a Bell-state measurement. Show that photons 1 and 4 are projected onto the same entangled state as photons 1 and 2 after entanglement swapping.

Solution: Let's consider more general case for entanglement swapping when

$$|\psi\rangle_{12} = \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2}}(\alpha|00\rangle_{12} + \beta|11\rangle_{12}) \tag{59}$$

and

$$|\psi\rangle_{34} = \frac{1}{\sqrt{2}}(|01\rangle_{34} + |10\rangle_{34}). \tag{60}$$

Problem 9 continued on next page...

Then we can rewrite the initial state as

$$\begin{aligned}
|\psi\rangle_{12}|\psi\rangle_{34} =& \frac{1}{\sqrt{|\alpha|^2+|\beta|^2}}\left(\alpha|00\rangle_{12}-\beta|11\rangle_{12}\right)\left(\frac{1}{\sqrt{2}}\left(|01\rangle_{34}+|10\rangle_{34}\right)\right.\\
=& \frac{1}{\sqrt{2\left(|\alpha|^2+|\beta|^2\right)}}\left[\alpha|01\rangle_{14}\frac{1}{\sqrt{2}}\left(\left|\phi^+\right\rangle+\left|\phi^-\right\rangle\right)_{23}+\alpha|00\rangle_{14}\frac{1}{\sqrt{2}}\left(\left|\psi^+\right\rangle+\left|\psi^-\right\rangle\right)_{23}\right.\\
&\left.-\beta|11\rangle_{14}\frac{1}{\sqrt{2}}\left(\left|\psi^+\right\rangle-\left|\psi^-\right\rangle\right)_{23}-\beta|10\rangle_{14}\frac{1}{\sqrt{2}}\left(\left|\phi^+\right\rangle-\left|\phi^-\right\rangle\right)_{23}\right] \qquad (61)\\
=& \frac{1}{2}\left[\left|\phi^+\right\rangle_{23}\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|01\rangle-\beta|10\rangle)_{14}+\left|\phi^-\right\rangle_{23}\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|01\rangle+\beta|10\rangle)_{14}\right.\\
&\left.+\left|\psi^+\right\rangle_{23}\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|00\rangle-\beta|11\rangle)_{14}+\left|\psi^-\right\rangle_{23}\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|00\rangle+\beta|11\rangle)_{14}\right]
\end{aligned}$$

Notice that

$$\begin{aligned}
\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|00\rangle-\beta|11\rangle) &= \sigma_x\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|01\rangle-\beta|10\rangle)\\
\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|00\rangle-\beta|11\rangle) &= \sigma_z\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|00\rangle+\beta|11\rangle) \qquad (62)\\
\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|00\rangle-\beta|11\rangle) &= \sigma_x\sigma_z\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha|01\rangle+\beta|10\rangle)
\end{aligned}$$

Therefore by applying the operation $I, \sigma_z, \sigma_x, \sigma_x\sigma_z$ when the Bell measurement gets $\left|\psi^+\right\rangle, \left|\psi^-\right\rangle, \left|\phi^+\right\rangle, \left|\phi^-\right\rangle$ respectively, we can project photons 1 and 4 onto the same entangled state as photons 1 and 2 .

Take $\alpha=\beta=1$ we obtain the result we want. ■

Problem 10 Suppose three EPR sources produce three pairs of entangled photons, pair 1-2, 3-4 and 5-6. The initial states are $|\phi^+\rangle_{12}=\frac{|00\rangle_{12}+|11\rangle_{12}}{\sqrt{2}}$, $|\phi^+\rangle_{34}=\frac{|00\rangle_{34}+|11\rangle_{34}}{\sqrt{2}}$, $|\phi^+\rangle_{56}=\frac{|00\rangle_{56}+|11\rangle_{56}}{\sqrt{2}}$. Photons $2,4$, and 6 are projected to GHZ-state $\frac{|000\rangle+|111\rangle}{\sqrt{2}}$. What is the state of the photons 1,3 and 5?

Solution: This can be solved by just direct calculation. Since that $|GHZ\rangle=\frac{|000\rangle+|111\rangle}{\sqrt{2}}$ where taking the projective measurement $(|GHZ\rangle\langle GHZ|)_{246}$, the post-measurement state is (up to a normalization factor)

$$(|GHZ\rangle\langle GHZ|)_{246}|\phi^+\rangle_{12}|\phi^+\rangle_{34}|\phi^+\rangle_{56}=\frac{1}{2\sqrt{2}}|GHZ\rangle_{246}|GHZ\rangle_{135} \qquad (63)$$

From this we see that, after the measurement, photons 1,3,5 are projected into GHZ state $\frac{|000\rangle_{135}+|111\rangle_{135}}{\sqrt{2}}$. ■

Problem 11 In quantum information theory, dense coding is a technique used to send two bits of classical information using only one qubit. Suppose that Alice and Bob share an EPR pair

$$\left|\phi^+\right\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B\right)$$

Show the detailed protocol to realize the dense coding.

Solution: The dense coding protocol works in the following four stages:

Entangled-state preparation and sharing: Suppose that Charlie prepares the Bell state

$$|\phi^+\rangle_{AB}=\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B) \qquad (64)$$

Problem 11 continued on next page...

and he sends the two particles to Alice and Bob respectively.

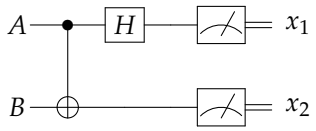
Encoding: Now Alice and Bob share the Bell pair $|\phi^+\rangle_{AB}$. Alice encodes two classical information as

- $x_1x_2 = 00$ as do nothing on her state, i.e. operates I_A, the resulting states is $|\phi^+\rangle_{AB}$;
- $x_1x_2 = 01$ as bit-flip, i.e., operates σ_x^A, the resulting state is $|\psi^+\rangle_{AB}$;
- $x_1x_2 = 10$ as phase-flip, i.e., operates σ_z^A, the resulting state is $|\phi^-\rangle_{AB}$;
- $x_1x_2 = 11$ as both bit-flip and phase-flip, i.e., operates $\sigma_z^A\sigma_x^A$, the resulting state is $|\psi^-\rangle_{AB}$.

Qubit sending: After encoding, Alice sends her half of qubit to Bob, there is only one-qubit communication.

Decoding: When Bob receives the qubit, he performs measurements in four Bell state basis, the measurement outcome unambiguously distinguishes the four possible actions that Alice could have performed. Thus Bob obtain two classical bit of information.

Another way Bob can decode two classical bits of information works as follows.



(65)

From the above process we see that dense coding can be regarded as the opposite of teleportation. ■

Problem 12 (1) Describe the symmetric key system and public key system in classical cryptography, and why are they becoming not secure enough?

(2) Describe the Post-quantum cryptography, and what do you think about the Post-quantum cryptography?

Solution: (1) We know that in classical cryptography:

- In symmetric key system, both the sender and receiver share the same key. Using algorithms like Advanced Encryption Standard (AED) for key extension and distribution.
- In public key system, the sender and receiver have different keys: the private key and the public key. The public key is used for encryption, and the private key is used for decryption. The public key can be freely distributed and is accessible to anyone, while its paired private key must keep secret. Examples are RSA system and Rabin system which are based on factoring of large numbers; Diffie-Hellman system and Elgamal system which are based on discrete log problem on finite fields or elliptic curves.

Why are they becoming not secure enough:

- For symmetric key system, there is the key distribution problem. It's insecurity for two network members to distribute symmetric keys without a secure channel, This presents a chicken-and-egg problem.
- For symmetric Key problem, Key management. Key numbers required increases fast as network members increase. It's difficult to keep them all consistent and secret.
- There are some disadvantages for public key system, the most important dis- advantage is that public key is based on a one-way function, such as RSA. Once the one-way function is cracked, it is no more secure for the public key.
- The existing key systems are based on the assumption that some calculation problem do not has a classical polynomial time algorithm is not proved yet.

Problem 12 continued on next page...

- Recently years, 1024-bits RSA system has been cracked.
- The MD5 which is based on Hashing function has been cracked by Wang et al.
- Shor's factoring algorithm can crack the RSA system.
- The development of computation power of modern computers made it more easy to crack the key system.

(2) By definition, Post-quantum cryptography is known as the cryptographic algorithms that are thought to be secure against an attack by a quantum computer.

Maybe we can try to design some tasks for which, even quantum computers can not solve efficiently. And we can try to design some tasks which is, in principle, secure from eavesdropper, like QKD, and our goal is to develop quantum technology to improve the fidelity of state and fidelity of quantum operations etc. ■

Lu Wei | PB16000702 | December 20, 2020