Solution 3 for 2019∼ 2020 USTC class 'Physics of Quantum Information'

Qing Zhou, Xin-Yu Xu and Kai Chen

National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, 230026, P.R. China

1. (1) Prove the CHSH inequality

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

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

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

Answer:

(1) Read page 103-104 of "Principles of Quantum Information Physics " by Yong-De Zhang for reference.

(2) the maximum violation allowed by quantum mechanics is $2\sqrt{2}$, and the corresponding quantum state and measurement operator are $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, $A_1 = X, A_2 = Z, B_1 = \frac{X+Z}{\sqrt{2}}, B_2 = \frac{X-Z}{\sqrt{2}}$. The derivation can be found at page 103-104 of "Principles of Quantum Information Physics " by Yong-De Zhang.

2. (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 $\vec{\sigma} = (\sigma_x\ \sigma_y\ \sigma_z)$. 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

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

Answer: For a real unit vector $\vec{n}$ in three dimensions, $(\vec{n}\cdot\vec{\sigma})^2 = I$, then

$$
\begin{aligned}
&(Q\otimes S + R\otimes S + R\otimes T - Q\otimes T)^2 \\
=&4I + (Q\otimes S)\cdot(R\otimes S) + (R\otimes S)\cdot(Q\otimes S) - (R\otimes T)\cdot(Q\otimes T) - (Q\otimes T)\cdot(R\otimes T) \\
&-(Q\otimes S)\cdot(Q\otimes T) - (Q\otimes T)\cdot(Q\otimes S) + (Q\otimes T)\cdot(Q\otimes S) + (R\otimes S)\cdot(R\otimes T) \\
&+(Q\otimes S)\cdot(R\otimes T) - (R\otimes S)\cdot(Q\otimes T) - (Q\otimes T)\cdot(R\otimes S) + (R\otimes T)\cdot(Q\otimes S) \\
=&4I + QR\otimes I + RQ\otimes I - RQ\otimes I - QR\otimes I - I\otimes ST - I\otimes TS + I\otimes ST + I\otimes TS \\
&+QR\otimes ST - RQ\otimes ST - QR\otimes TS + RQ\otimes TS \\
=&4I + [Q,R]\otimes[S,T].
\end{aligned}
$$

As $[Q,R]\leq 2,\ [S,T]\leq 2$, we have $4I + [Q,R]\otimes[S,T]\leq 8$. That is

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

3. 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.

   Answer:

   Read page 20-24 in the lecture "QIP2019chapt_3_1_Kai Chen.pdf" for reference.

4. 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.

   Answer:

   Read page 16-19 in the lecture "QIP2019chapt_3_1_Kai Chen.pdf" for reference.

5. Derive the Bell's theorem without inequalities from the GHZ state

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

Answer:

Read page 34 in the lecture "QIP2019chapt_3_1_Kai Chen.pdf" for reference.

6. (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.

   Answer:

   (1) Read page 14 in the lecture "QIP2019chapt_4_1_Kai Chen.pdf" for reference.

   (2) The security of BB84 QKD is built under the quantum non-clone principle and Heisenberg uncertainty principle, which guarantees that no eavesdropper can get information escaped detection.

   (3) Read the lecture "QIP2019chapt_4_1_Kai Chen.pdf" for reference.

   (4) Read the lecture "QIP2019chapt_4_1_Kai Chen.pdf" for reference.

   (5) Read the lecture "QIP2019chapt_4_1_Kai Chen.pdf" for reference.

7. 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

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

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.

Answer:

(1) The protocol is as follows:

(a) An EPR pair $|\psi\rangle_{23} = \frac{1}{\sqrt{2}}(|00\rangle_{23} + |11\rangle_{23})$ is generated, one qubit sent to Alice, the other to Bob.

(b) 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.

(c) Alice sends the Bell measurement result to Bob using a classical channel.

(d) The joint state of the three particles can be rephased as following:

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

Bell measurements on the first two particles would project the state of Bob's particle into a variant of $|\psi\rangle$ of the state $|\psi\rangle_1$, where

$$|\psi\rangle = |\psi\rangle_1 \text{ or } \sigma_x |\psi\rangle_1 \text{ or } \sigma_z |\psi\rangle_1 \text{ or } \sigma_z\sigma_x |\psi\rangle_1$$

Which of these four possibilities actually obtains is encoded in the two classical bits. The unknown state $|\psi\rangle_1$ can therefore be obtained from $|\psi\rangle$ by applying one of the four operations

$$I, \sigma_x, \sigma_y, \sigma_z.$$

(2) From the protocol we can see that without knowledge of the Bell measurement's results, Bob can't turn the state of particle 3 into the Alice's original state. To see this, just calculate the density matrix of particle 3 before any information is received, which is $\rho_3 = Tr_{12}(\rho_{123}) = \frac{I}{2}$.(You can prove it by yourself). So Bob can't tell the difference between what Alice did and a random measurement (or whether she did anything at all) before he gets the result sent by Alice. Since the quantum teleportation must contain the classical communication which can't transfer faster than light, so we can't use it to communicate faster than light.

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

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

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.

Answer:

The joint state of the four particles can be rephased as following:

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

Since

$$\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha\,|00\rangle-\beta\,|11\rangle)=\sigma_x\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha\,|01\rangle-\beta\,|10\rangle),$$
$$\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha\,|00\rangle-\beta\,|11\rangle)=\sigma_z\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha\,|00\rangle+\beta\,|11\rangle),$$
$$\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha\,|00\rangle-\beta\,|11\rangle)=\sigma_x\sigma_z\frac{1}{\sqrt{\alpha^2+\beta^2}}(\alpha\,|01\rangle+\beta\,|10\rangle)$$

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

9. 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?

   Answer:
   Let $|GHZ\rangle=\frac{|000\rangle+|111\rangle}{\sqrt{2}}$

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

   Hence, photons 1,3,5 are projected into GHZ state $\frac{|000\rangle+|111\rangle}{\sqrt{2}}$.

10. 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

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B),$$

    Show the detailed protocol to realize the dense coding.

    Answer:
    Please read 'section §13.3.4 at page 286 of Yong-De Zhang's Principles of Quantum Information Physics' for reference.

11. (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?

Answer:

(1) (a) Symmetric key system in cryptography refers to encryption in which both the sender and receiver share the same key.

(b) In public key system, the sender and receive have different key, i.e. the private key and the public key. The public key can be freely distributed, anyone can get the public key, however, its paired private key must remain secret. The public key is used for encryption, while, the private key is used for decryption.

(c) There are some disadvantages for symmetric key system,

- 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.
- Key management. Key numbers required increases fast as network members increase. It's difficult to keep them all consistent and secret.

In practice, the symmetric key is distributed by public key system. Also, there are some disadvantages for public key system, the most important disadvantage 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.

(2) Post-quantum cryptography refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer.