PHYS5251P: Exercise 4, Fall 2025, USTC 'Introduction to Quantum Information'

Nuo-Ya Yang and Kai Chen

Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China

1. Consider two qubits A and B, and an arbitrary unknown quantum state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $|\alpha|^2 + |\beta|^2 = 1$. Can we design an operator $\Omega_{AB} = I_A \otimes |0\rangle_{BB}\langle 0|$, which remove the copy state of B: $|\Psi\rangle_A |\Psi\rangle_B \longrightarrow |\Psi\rangle_A |0\rangle_B$?

2. (1) Write down the communication process of BB84 quantum key distribution (QKD) protocol.

   (2) Write down the secure key rate formula of single-photon BB84 QKD and explain the relationship with entanglement purification protocol. (Hint: read Shor and Preskill's security proof.)

   (3) Suppose in BB84 QKD Alice and Bob both choose their bases with uniform probability and we neglect photon losses and systematic errors. Given no eavesdropping, compute the mutual information between Alice and Bob $H(A:B)$ *before* basis sifting.

3. Quantum teleportation is a process by which quantum information can be transmitted from one location to another, with the help of quantum entanglement.

   (1) Suppose the initials states are $|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1, |\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3)$. Show that particle 3 can be projected onto the same state as particle 1 by some local operators after Bell state measurement on particle 1 and 2.

(2) Suppose the initials states are $|\psi\rangle_1 = \alpha\,|0\rangle_1 + \beta\,|1\rangle_1$, $|GHZ\rangle_{234} = \frac{1}{\sqrt{2}}(|0\rangle_2\,|0\rangle_3\,|0\rangle_4 + |1\rangle_2\,|1\rangle_3\,|1\rangle_4)$. Show that particle 4 can be projected onto the same state as particle 1 by some local operators after Bell state measurement on particle 1 and 2 and local X measurement on particle 3.

(3) Explain why we can't use quantum teleportation to achieve superluminal communication.

4. Let $|\psi\rangle = a|0\rangle + b|1\rangle$ be an arbitrary qubit state. Let $|\phi\rangle$ be another arbitrary qubit state. Let U be a unitary operator which acts on two qubits. Determine the implications of measuring the first two qubits of

$$|\theta\rangle = |\psi\rangle \otimes \frac{1}{\sqrt{2}}(I_2 \otimes U)((|00\rangle + |11\rangle) \otimes |\phi\rangle)$$

with respect to the Bell basis. How can we obtain $U(|\psi\rangle \otimes |\phi\rangle)$ as the last two qubits?

5. Consider a noisy entangled pair with density matrix

$$\rho_\epsilon = (1-\epsilon)\,|\psi^-\rangle\,\langle\psi^-| + \epsilon\frac{I}{4},$$

where $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The fidelity between two density matrices σ and τ is defined as $F(\sigma,\tau) = (\mathrm{Tr}\,\sqrt{\sqrt{\sigma}\tau\sqrt{\sigma}})^2 = F(\tau,\sigma)$.

(1) Calculate the fidelity between ρ_ϵ and $|\psi^-\rangle\,\langle\psi^-|$. (Recall that for pure state σ, we have $\sqrt{\sigma} = \sigma = \sigma^2$.)

(2) Give the lower bound of fidelity $F(\rho_\epsilon, |\psi^-\rangle\,\langle\psi^-|)$ when the state ρ_ϵ is entangled using PPT criterion.

(3) Suppose one uses ρ_ϵ instead of perfect EPR states to teleport a pure qubit state ρ. Find the fidelity between the teleported qubit state and ρ.

6. Suppose three EPR sources produce three pairs of entangled photons, pair 1-2, 3-4 and 5-6. The initial states are $|\phi^+\rangle_{12} = \frac{|00\rangle_{12}+|11\rangle_{12}}{\sqrt{2}}$, $|\phi^+\rangle_{34} = \frac{|00\rangle_{34}+|11\rangle_{34}}{\sqrt{2}}$, $|\phi^+\rangle_{56} = \frac{|00\rangle_{56}+|11\rangle_{56}}{\sqrt{2}}$. Then 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?

7. 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.

8. Alice and Bob now devise the following protocol: Assume that the state Alice wants to transmit is on the equator of the Bloch sphere, i.e. one of the states $|\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{-i\alpha}|1\rangle)$ for $0 \leq \alpha \leq 2\pi$. As in the regular teleportation protocol,they share a maximally entangled state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice measures her half of this previously shared state in the basis $\{|\alpha\rangle, |\alpha^\perp\rangle\}$, where $|\alpha^\perp\rangle = |\alpha + \pi\rangle$. Show that communicating the outcome of this measurement (one bit) is sufficient for Bob to faithfully obtain the state $|\alpha\rangle$.

9. Devise a quantum teleportation protocol for teleporting two qubits whose state is always of the form

$$|\psi\rangle = a|00\rangle + b|11\rangle,$$

where $|a|^2 + |b|^2 = 1$.

10. (**The six state protocol**) An alternative to the BB84 protocol is the six state protocol in which Alice and Bob have three bases to choose from when encoding and measuring. That is, Alice uniformly chooses a basis out of the σ_z, σ_x and σ_y bases and then sends one of the two orthogonal states in the chosen basis. Explicitly, Alice sends either $\{|0\rangle$ or $|1\rangle\}$ or $\{|+\rangle$ or $|-\rangle\}$ or $\{|+i\rangle$ or $|-i\rangle\}$,where $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ are the eigenstates of σ_y. Similarly Bob has three choices from which to uniformly choose a basis to measure in: σ_z, σ_x or σ_y.

    Assuming that Eve performs an intercept resend attack on every qubit (i.e., she measures in a uniformly chosen random basis out of the three and sends her resulting

state onto Bob), what is the error rate Alice and Bob will see during the error estimation stage.

11. The action of creation operator $a^\dagger$ and annihilation operator a on Fock states $|n\rangle$ is as follows,

$$a\,|n\rangle = \sqrt{n}\,|n-1\rangle\,,\ a^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,,$$

where n denotes the number of particles and is a non-negative integer. The coherent state is defined as the unique eigenket of the annihilation operator a,

$$a\,|\alpha\rangle = \alpha\,|\alpha\rangle\,,$$

where α is a complex number.

(1) Prove that the coherent state $|\alpha\rangle$ can be expanded in Fock basis as

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,.$$

(2) Prove that the phase randomized coherent state $\int_0^{2\pi}\frac{1}{2\pi}\,|e^{i\theta}\sqrt{\mu}\rangle\,\langle e^{i\theta}\sqrt{\mu}|\,\mathrm{d}\theta$ is a mixture of Fock states with Poisson distribution, where μ is a positive real number.

(3) Describe the photon number splitting attack and the principle of decoy QKD protocol. (Hint: read Phys. Rev. Lett. 94, 230504 (2005).)

12. Give a noisy entanglement state with purity F for the singlet state $|\Psi^-\rangle$,

$$W_F = F|\Psi^-\rangle\langle\Psi^-| + \frac{1-F}{3}|\Psi^+\rangle\langle\Psi^+| + \frac{1-F}{3}|\Phi^+\rangle\langle\Phi^+| + \frac{1-F}{3}|\Phi^-\rangle\langle\Phi^-|.$$

Supposing $F = \frac{3}{5}$, please design a two-way LOCC purification protocol that can obtain the singlet state $|\Psi^-\rangle$ with as high fidelity as possible from the above mixed state in five steps.

13. The polarization dependent beam splitter (PDBS), which has transmission rate T_H for horizontal polarization mode and transmission rate T_V for vertical polarization

mode, can be used to construct controlled phase gate. In figure (a), a PDBS performs the following transformation on input single photon with path mode a:

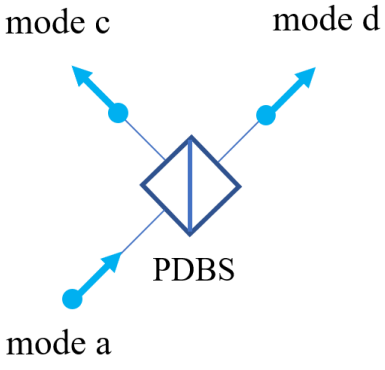
$$\alpha\,|H_a\rangle + \beta\,|V_a\rangle \longrightarrow \alpha(\sqrt{T_H}\,|H_d\rangle + i\sqrt{1-T_H}\,|H_c\rangle) + \beta(\sqrt{T_V}\,|V_d\rangle + i\sqrt{1-T_V}\,|V_c\rangle),$$

where $|H_d\rangle$ denotes horizontal polarized photon on path mode d and similar for the other terms. In figure (b), two input modes a and b are overlapped at PDBS_0, with a $\mathrm{PDBS}_{1/2}$ on each of its output mode.

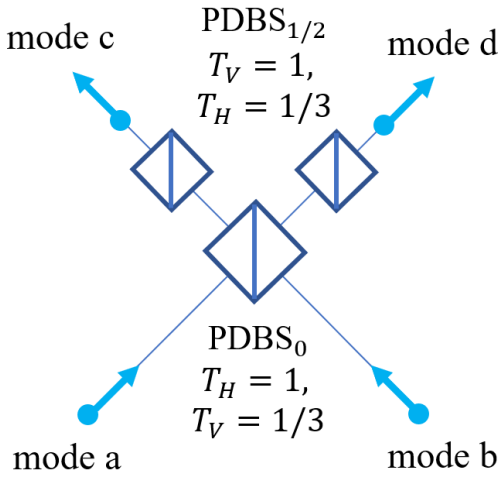
(1) Show that, conditioned on the coincidence detection of output modes c and d, the setup in figure (b) can implement the controlled phase gate perfectly,

$$\begin{aligned} &c_{HH}\,|H_aH_b\rangle + c_{HV}\,|H_aV_b\rangle + c_{VH}\,|V_aH_b\rangle + c_{VV}\,|V_aV_b\rangle \\ \longrightarrow\ &c_{HH}\,|H_dH_c\rangle + c_{HV}\,|H_dV_c\rangle + c_{VH}\,|V_dH_c\rangle - c_{VV}\,|V_dV_c\rangle\,. \end{aligned}$$

(2) Calculate the probability to obtain a coincidence in the outputs.



(a) PDBS



(b) Setup for the controlled phase gate

14. We can construct a nondestructive CNOT gate by polarizing beam splitters (PBS), half-wave plates (HWP), and an ancilla entangled photon pair $|\phi^+\rangle_{ab} = \frac{1}{\sqrt{2}}(|00\rangle_{ab} + |11\rangle_{ab})$ shown as Fig. 1. Consider an arbitrary input state of the form $|\psi\rangle_{2'3'} = \alpha_1|H_{2'}H_{3'}\rangle + \alpha_2|H_{2'}V_{3'}\rangle + \alpha_3|V_{2'}H_{3'}\rangle + \alpha_4|V_{2'}V_{3'}\rangle$, with control photon in mode $2'$ and target photon in mode $3'$. Please prove that one can implement the CNOT

operation between photons $2'$ and $3'$ when detecting a $|+\rangle$ photon in mode c and a $|H\rangle$ photon in mode d.

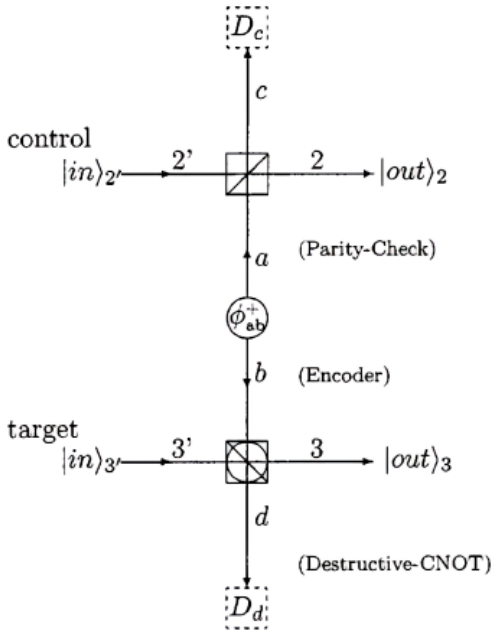


FIG. 1. The nondestructive CNOT gate constructed by polarizing beam splitters (PBS), half-wave plates (HWP),and an ancilla entangled photon pair $|\phi^+\rangle_{ab}$. The PBS at the bottom is accomplished by inserting one half-wave plate (HWP) in each of the two inputs ($3'$ and b) and two outputs (3 and d) of an ordinary polarizing beam splitter. Note that, all four HWP were oriented at 22.5° with respect to the horizontal direction, which corresponds to a 45° polarization rotation.

15. Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in a different BB84 polarization state which is selected, independently and at random for each signal, by means of a polarization modulator (Pol-M). Decoy states are generated using an intensity modulator (Decoy-IM). Inside the measurement device, signals from Alice and Bob interfere at a 50 : 50 beam splitter (BS) that has on each end a polarizing beam splitter (PBS) projecting the input photons into either horizontal (H) or vertical (V) polarization states (see Fig. 2). Four single-photon detectors are employed to detect the photons and the detection results are publicly announced. A successful Bell state measurement corresponds to the observation of precisely two

detectors (associated to orthogonal polarizations) being triggered.

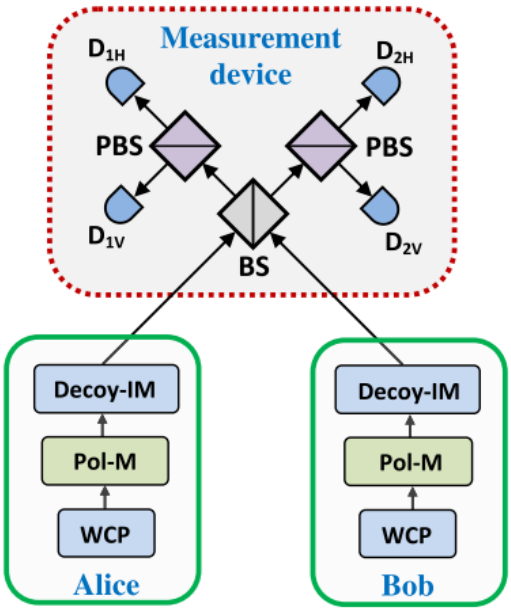


FIG. 2. Basic setup of a MDI-QKD protocol.

(1) Which state are the two photons projected into when there is a click on D_{1H} and D_{2V}, or in D_{1V} and D_{2H}?

(2) Which state are the two photons projected into when there is a click on D_{1H} and D_{1V}, or in D_{2H} and D_{2V}?

(3) Alice and Bob post-select the events where the relay outputs a successful result and they use the same basis in their transmission. To guarantee that their bit strings are correctly correlated, either Alice or Bob has to apply a bit flip to her or his data. Please give a protocol which make their bit strings correctly correlated.