PHYS5251P: Exercise 2, Spring 2024, USTC
'Introduction to Quantum Information'

Nuo-Ya Yang, Jun-Hao Wei and Kai Chen

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

1. The four Bell states have the following mathematical expressions on the basis $\{|0\rangle, |1\rangle\}$ (the eigenstates of σ_z),

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),$$
$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

   (1) Prove that the four Bell states can be transformed to each other using single qubit rotations $\{I, \sigma_x, \sigma_y, \sigma_z\}$.

   (2) Show that each of the four Bell states is an eigenstate of the observables $\{\sigma_{1x}\sigma_{2x}, \sigma_{1y}\sigma_{2y}, \sigma_{1z}\sigma_{2z}\}$ and write down the corresponding eigenvalues.

2. For the singlet state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, prove that Alice and Bob's outcomes are always anti-correlated when they measure two particles respectively along the same direction.

3. Let $\sigma_\theta \equiv \cos\theta\sigma_z + \sin\theta\sigma_x$. Define $|+_\theta\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$ and $|-_\theta\rangle = -\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle$.

   (1) Verify that $|+_\theta\rangle$ is the eigenket of σ_θ with eigenvalue $+1$, and $|-_\theta\rangle$ is the eigenket of σ_θ with eigenvalue -1.

   (2) $R_y(\theta) = \exp\left(\frac{-i\theta\sigma_y}{2}\right)$ represents the counterclockwise rotation of angle θ around the y-axis. Verify that $\sigma_\theta = R_y(\theta)\sigma_z R_y(-\theta)$.

(3) Using the definitions of $|+_\theta\rangle$ and $|-_\theta\rangle$, show that for any θ,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|+_\theta +_\theta\rangle + |-_\theta -_\theta\rangle).$$

4. Suppose $|\psi\rangle$ is a pure state of a composite system AB. Prove that there exist orthonormal states $|i_A\rangle$ for system A, and orthonormal states $|i_B\rangle$ for system B such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle,$$

where λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ known as ***Schmidt coefficients*** .

5. Prove that a state $|\psi\rangle$ of a composite system AB is a product state if and only if it has Schmidt number 1. Prove that $|\psi\rangle$ is a product state if and only if ρ^A (and thus ρ^B) are pure states.

6. PPT (Positive Partial Transposition) criterion is a strong separability criterion for quantum states, which is very convenient and practical for entanglement detection.

(1) Describe the PPT criterion and the realignment criterion.

(2) For the 2-qubit state $\rho = p\,|\psi^-\rangle\langle\psi^-| + (1-p)\frac{\mathbb{I}}{4}$, where, $0 \le p \le 1$, $|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$, calculate the lower bound of p for ρ to be an entangled state using PPT criterion and realignment criterion respectively.

7. (1) For the 3-qubit W state $|W_3\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$, if one particle is lost, what's the reduced density matrix of the remaining two particles?

(2) For the n-qubit W state $|W_n\rangle = \frac{1}{\sqrt{n}}(|10\cdots 0\rangle + |01\cdots 0\rangle + \cdots + |00\cdots 1\rangle)$, if $(n-2)$ particles are lost, what's the reduced density matrix of the remaining two particles? Use the PPT criterion to find out whether the remaining two particles are entangled or not.

8. An entanglement witness(EW) is a functional which distinguishes a specific entangled state from separable ones.

(1) Describe the definition of the Entanglement Witness (EW).

(2) For the mixed state $\rho = p\frac{\mathbf{I}}{8} + (1-p)|GHZ\rangle\langle GHZ|$ $(0 \leq p \leq 1)$, calculate p's upper bound when ρ is an entangled state using the entanglement witness $\mathcal{W} = \frac{1}{2}\mathbf{I} - |GHZ\rangle\langle GHZ|$.

9. (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.

10. 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).)

11. (**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.