CS333 - Problem Set 3

1. Now that we have a mathematical (linear algebraic) description of quantum states and measurements, we can reinterpret our cryptographic scenarios using these mathematical descriptions. Please use ket/bra notation to describe the following scenarios. If applicable, calculate the probability of different possible outcomes:

   - Alice prepares a horizontally polarized photon and sends to Bob.
   - Eve intercepts the photon and has it pass through a vertically polarized filter before trying to detect the photon. If she detects a photon, she prepares a vertically polarized photon to send to Bob, and otherwise, she sends Bob a horizontally polarized photon. (Calculate the probability of each outcome occuring using our mathematical tools.)
   - Bob measures the photon he received from Eve by putting a right diagonally polarized filter in front of his photon detector. What outcomes does he get, and with what probability?

2. Is the following a valid qubit measurement? Why or why not? (Try to do the calculation(s) only using standard basis bra/kets for practice.)

$$M = \left\{ \sqrt{\frac{1}{3}}|0\rangle + i\sqrt{\frac{2}{3}}|1\rangle, \sqrt{\frac{2}{3}}|0\rangle + i\sqrt{\frac{1}{3}}|1\rangle \right\} \tag{1}$$

3. Let $M = \{|\phi_0\rangle, |\phi_1\rangle\}$ be an orthonormal basis representing a qubit measurement, and let $|\psi\rangle$ be a vector representing a qubit quantum state. For this problem, you may want to refer to the Math Practice worksheet for properties of orthonormal bases.

   (a) Since $|\psi\rangle$ is a quantum state, we know that there must be amplitudes a_0 and a_1 such that $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$ where $|a_0|^2 + |a_1|^2 = 1$. However, show there also exist α_0, α_1 ("alpha") such that $|\psi\rangle = \alpha_0|\phi_0\rangle + \alpha_1|\phi_1\rangle$ where $|\alpha_0|^2 + |\alpha_1|^2$=1.

   (b) Suppose we measure $|\psi\rangle$ using M. Let p_0 be the probability of outcome $|\phi_0\rangle$ and let p_1 be the probability of outcome $|\phi_1\rangle$. Use part (a) to show that $p_0 + p_1 = 1$, that is, the sum of the outcome probabilities is 1.

   (c) What have you learned about about quantum measurements and quantum states from this problem?

4. Let $|\psi\rangle$ be a vector representing a qubit quantum state. Let $|\psi'\rangle = e^{i\omega}|\psi\rangle$ for $\omega \in \mathbb{R}$. We call a complex number of the form $e^{i\omega}$ a **phase**. (A phase is a complex number whose absolute value is 1.) When a phase multiplies an entire quantum state, as in the case $e^{i\omega}|\psi\rangle$, we call it a **global phase**.

   (a) Show that $|\psi'\rangle$ also represents a qubit state.

(b) Show that any measurements give exactly the same outcome statistics and states on $|\psi\rangle$ and $|\psi'\rangle$.

(c) Is it possible to tell the difference between $|\psi\rangle$ and $|\psi'\rangle$? What have you learned about quantum states and their mathematical representations from doing this problem?

5. **[Moved to next week]** Consider the 2-qubit state $|\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle_{AB} - \frac{1}{\sqrt{2}}|10\rangle_{AB}$. This state has some strange properties - in particular the two qubits are perfectly anticorrelated. It's behavior is so strange, it caused Einstein to believe that quantum mechanics couldn't possibly describe reality.

   (a) Suppose Alice and Bob each measure their qubit in the same basis. That is, Alice and Bob both each apply the measurement $M(\eta, \chi) = \{|\phi_0(\eta, \chi)\rangle, |\phi_1(\eta, \chi)\rangle\}$, where $|\phi_0(\eta, \chi)\rangle = \cos\eta|0\rangle + e^{i\chi}\sin\eta|1\rangle$ and $|\phi_1(\eta, \chi)\rangle = -\sin\eta|0\rangle + e^{i\chi}\cos\eta|1\rangle$. ($\eta$ is pronounced "ay-tah" and spelled eta, and χ is pronounced "kai" and spelled chi, and ϕ is pronounced "fie" and spelled phi.) Show that if Alice gets outcome $|\phi_0(\eta, \chi)\rangle$, Bob will get outcome $|\phi_1(\eta, \chi)\rangle$, or vice versa. $M(\eta, \chi)$ is "generic" in that by choosing any various real numbers for χ and η, we can make $M(\eta, \chi)$ represent any possible qubit measurement. Please calculate the probability of at least one outcome by hand for practice. If you feel like you don't need additional practice, you may use a computer to calculate the others.

   (b) What is the overall probability that Alice gets outcome $|\phi_0(\eta, \chi)\rangle$? What is the probability that she gets $|\phi_1(\eta, \chi)\rangle$?

   (c) This anticorrelation is strange because of the following thought experiment. Suppose Alice took her qubit to the moon, and Bob stayed on Earth. Now Alice performs her measurement first, and suppose she gets outcome $|\phi_0(\eta, \chi)\rangle$. Then, even if Bob performs his measurement before any lightspeed communication can have happened between Alice and Bob, Bob's qubit somehow knows to choose the opposite outcome. This will happen no matter which values of η and χ Alice and Bob choose. People thought that this might enable faster-than-light communication, but explain why Part (b) of this question rules out faster-than-light communication.

   (d) We also can have classical (non-quantum) bits that are probabilistically anti-correlated. Consider the following situation. I put a red sock in one box and a blue sock in another box, and I give one box to Alice and one box to Bob, without telling them which box contains which sock. Once Alice opens her box and sees a blue sock, she immediately knows that Bob's box contains a red sock. Why is the quantum situation stranger than this classical situation?

6. Optional Further Reading:

   (a) UK Government Thoughts on Quantum Cryptography

   (b) French Governmetn Thoughts on Quantum Cryptography

   (c) ID Quantique (one of the top companies selling QKD technology.)