Homework 5: 17-18 October 2018
Traitement Quantique de l'Information

Exercise 1 *No-cloning theorem*

In class we saw that unitarity and tensor product structure imply the no-cloning theorem. Here we show that linearity and tensor product structures also imply the no-cloning theorem.

Suppose a common cloning machine U exists for all inputs $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $\alpha^2 + \beta^2 = 1$. Alice claims that

$$U|\Psi\rangle \otimes |\text{blank}\rangle = \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle .$$

But Bob just by the definition of the copying operator claims that

$$U|\Psi\rangle \otimes |\text{blank}\rangle = \alpha^2|0\rangle \otimes |0\rangle + \alpha\beta|0\rangle \otimes |1\rangle + \alpha\beta|1\rangle \otimes |0\rangle + \beta^2|1\rangle \otimes |1\rangle .$$

This contradiction can be used to show the no-cloning theorem.

1) Elaborate in detail the steps that Alice and Bob each have in mind to reach these two equations.

2) Under what condition on α and β are the two equations equivalent? What does this mean with respect to cloning?

Exercise 2 *Quantum bank note*

In 1970's Wiesner had the idea of quantum bank notes that cannot be copied. A quantum bank note consists of one serial number S and of N small cavities each storing one quantum bit (say a polarized photon, or some magnetic moment). Each quantum bit is in a definite state

$$|\phi_i\rangle \in \left\{|0\rangle ; \frac{|0\rangle + |1\rangle}{\sqrt{2}}\right\}, i = 1 \dots N.$$

The serial number S (say $S = \text{COM309HW6ISFUN}$) indicates to the bank the preparation $p_1, \dots, p_N$ of the quantum bits where $p_i = 0$ if $|\phi_i\rangle = |0\rangle$ and $p_i = 1$ if $|\phi_i\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. There is a mapping $f(S) = (p_1 \dots p_N)$ that only the bank knows. Therefore the bank has access to the information $p_1, \dots, p_N$ by reading S; but no one else has.

We decide to counterfeit the bill as follows. We first observe the state of each qubit using measurements in the Z or X basis at random (since we have no information about p_i). This necessarily leaves each qubit in a state $\in \{|0\rangle, |1\rangle\}$ or in a state $\in \left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$. If the measured qubit is left in state $|0\rangle$ or $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ we just copy it (with the correct copy machine!). If the measured qubit is left in state $|1\rangle$ then we prepare a new state as $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and if it is left in the state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ we prepare a new state $|0\rangle$.

We thus get a "counterfeited" bill which we bring to the bank.

1) First suppose that a honest person brings a true bank note (not counterfeited) to the bank. Describe how the bank proceeds to make measurements in order to verify the bank note in such a way that the bank note is not destroyed.

2) Suppose that we bring a counterfeited note to the bank. Show that the probability the bank detects a problem is $1 - (7/8)^N$.

Exercise 3 *Copying or unitary attack from Eve in BB84*

Consider the BB84 protocol. Suppose the i-th qubit sent by Alice is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and is captured by Eve. Eve wants to make a copy of the qubit and sends one of the copies to Bob. However she does not know what the preparation basis of Alice was: here we suppose that Eve uses the wrong machine U_Z to copy this bit. Recall that U_Z is defined by

$$U_Z |0\rangle \otimes |b\rangle = |0\rangle \otimes |0\rangle\,, \quad U_Z |1\rangle \otimes |b\rangle = |1\rangle \otimes |1\rangle\,.$$

Eve then keeps one of the photons and sends the other one to Bob. Suppose now that Bob uses the X-basis to measure the state of the photon. During the public communication phase Alice and Bob notice that their preparation and measurement basis were the same so they conclude that the i-th bit (of their secret key) must be the same under the hypothesis that Eve is not present (they don't know yet that Eve is present).

The goal of this problem is to show that there is a probability 1/2 that the bit of Alice and Bob differs due to the presence of Eve. Therefore repeated such attacks of Eve over many qubits will be detectable (with probability close to one) during the security test.

1) What is the state of the two photons in the lab of Eve just after she made the copying operation.

2) The measurement process of Bob (we suppose Eve does not measure at this stage) is modeled by the two projectors:

$$\Pi_+ = I \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right), \quad \Pi_- = I \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right)$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ expresses the fact that Eve does not measure and the second term of the tensor product expresses the fact that Bob's measurement basis is $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$.

a) What are the possible resulting states in Bob's lab? Hint: no calculation.

b) Compute now $p_\pm$ the probability of these outcoming states by using the appropriate form of the measurement postulate.

Hint: It will be a good idea to expand $\Pi_\pm$ by writing $I = |0\rangle\langle 0| + |1\rangle\langle 1|$. For example you should check this kind of identity:

$$\begin{aligned}\Pi_+ &= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right) \\ &= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes \left(\frac{|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|}{2}\right) \\ &= \frac{1}{2}\big(\,|00\rangle\langle 00| + |00\rangle\langle 01| + |01\rangle\langle 00| + |01\rangle\langle 01| \\ &\qquad + |10\rangle\langle 10| + |10\rangle\langle 11| + |11\rangle\langle 10| + |11\rangle\langle 11|\,\big)\end{aligned}$$