Homework 5: 19 October 2017
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 $S = \text{COM309HW5ISFUN}$) 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 $1 - (7/8)^N$.