Homework 5: 19 October 2017
Traitement Quantique de l'Information

Exercise 1 *No-cloning theorem*

1) For $|\Psi\rangle = |0\rangle$, the machine should give $U|0\rangle \otimes |\text{blank}\rangle = |0\rangle \otimes |0\rangle$. For $|\Psi\rangle = |1\rangle$, the machine should give $U|1\rangle \otimes |\text{blank}\rangle = |1\rangle \otimes |1\rangle$. The first claim is then followed by linearity,

$$\begin{aligned} U(\alpha|0\rangle + \beta|1\rangle) \otimes |\text{blank}\rangle &= \alpha U|0\rangle \otimes |\text{blank}\rangle + \beta U|1\rangle \otimes |\text{blank}\rangle \\ &= \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle . \end{aligned}$$

The second claim is based on

$$\begin{aligned} U(\alpha|0\rangle + \beta|1\rangle) \otimes |\text{blank}\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|0\rangle \otimes |0\rangle + \alpha\beta|0\rangle \otimes |1\rangle + \alpha\beta|1\rangle \otimes |0\rangle + \beta^2|1\rangle \otimes |1\rangle . \end{aligned}$$

2) The two equations are equivalent when $(\alpha, \beta) = (0, 1)$ or $(\alpha, \beta) = (1, 0)$, which corresponds to two orthogonal input states $|\Psi\rangle = |0\rangle$ and $|1\rangle$. This means that it is possible to copy two orthogonal states with an appropriate machine U but no cloning is possible when the set of input states is not orthogonal.

Remark: In class we showed that no cloning theorem follows from unitary and the tensor product structure. Here we show that it also follows from linearity and tensor product structure. Thus in principle we could make a theory that preserves the no-cloning theorem that abandons linearity or unitarity (but not both).

Exercise 2 *Quantum bank note*

1) The bank finds the sequence $p_1, \ldots, p_N$ from S. The sequence $p_1, \ldots, p_N$ indicates the preparation basis of the true quantum bits $|\phi_1\rangle, \ldots, |\phi_N\rangle$. This allows the bank to measure the quantum bits using the preparation basis (so the measurement basis is Z if $p_i = 0$ and X if $p_i = 1$). If the bank note is authentic, each measurement on $|\phi_i\rangle$ does not destroy the quantum bit and the measurement certainly gives an output state $|\phi_i\rangle$. If the bank note is counterfeited, then the measurement does not guarantee to always give the output state $|\phi_i\rangle$.

2) Suppose the counterfeited bank note contains quantum bits in state $|\phi'_1\rangle \otimes \cdots \otimes |\phi'_N\rangle$. The bank detects a problem if for some i the measurement on $|\phi'_i\rangle$ does not give the state $|\phi_i\rangle$. Thus the probability that the bank detects a problem is

$$\begin{aligned} P(\text{detect a problem}) &= 1 - P(\text{not detect a problem}) \\ &= 1 - \prod_{i=1}^{N} P(\text{meas. on } |\phi'_i\rangle \text{ gives } |\phi_i\rangle) \end{aligned}$$

We expand $P(\text{meas. on } |\phi_i'\rangle \text{ gives } |\phi_i\rangle)$ into

$$\begin{aligned} &P(\text{meas. on } |\phi_i'\rangle \text{ gives } |\phi_i\rangle \,\big|\, |\phi_i'\rangle = |\phi_i\rangle) \cdot P(|\phi_i'\rangle = |\phi_i\rangle) \\ &\qquad + P(\text{meas. on } |\phi_i'\rangle \text{ gives } |\phi_i\rangle \,\big|\, |\phi_i'\rangle \neq |\phi_i\rangle) \cdot P(|\phi_i'\rangle \neq |\phi_i\rangle) \\ &= 1 \cdot (1 - P(|\phi_i'\rangle \neq |\phi_i\rangle)) + \frac{1}{2} \cdot P(|\phi_i'\rangle \neq |\phi_i\rangle) \end{aligned}$$

where $P(\text{meas. on } |\phi_i'\rangle \text{ gives } |\phi_i\rangle \,\big|\, |\phi_i'\rangle \neq |\phi_i\rangle) = 1/2$ can be checked explicitly for the two possible cases: $|\phi_i'\rangle = |0\rangle$ and $|\phi_i\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, or $|\phi_i'\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\phi_i\rangle = |0\rangle$.

The event $|\phi_i'\rangle \neq |\phi_i\rangle$ happens in either of the following cases:

- The true quantum bit $|\phi_i\rangle$ is $|0\rangle$; the counterfeiter measures it with X basis; and upon the measurement the counterfeiter observes $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. This happens with probability $\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$.
- The true quantum bit $|\phi_i\rangle$ is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$; the counterfeiter measures it with Z basis; and upon the measurement the counterfeiter observes $|0\rangle$. This happens with probability $\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$.

We conclude that

$$\begin{aligned} P(|\phi_i'\rangle \neq |\phi_i\rangle) &= \frac{1}{8} + \frac{1}{8} = \frac{1}{4}, \\ P(\text{meas. on } |\phi_i'\rangle \text{ gives } |\phi_i\rangle) &= 1 \cdot \left(1 - \frac{1}{4}\right) + \frac{1}{2} \cdot \frac{1}{4} = \frac{7}{8}, \\ P(\text{detect a problem}) &= 1 - \left(\frac{7}{8}\right)^N. \end{aligned}$$