Homework 5: Solution
Traitement Quantique de l'Information

Exercise 1 *Bennett 1992 Protocol for quantum key distribution*

1) When $d_i = e_i$, Bob measures the qubit in the same basis as the preparation basis used by Alice. In other words if $e_i = d_i = 0$ the transmitted qubit state is $|0\rangle$ and the measurement is in the Z-basis then this yields a measurement result $|0\rangle$ with probability 1. A similar argument holds if $e_i = d_i = 1$ and the transmitted qubit is $H|0\rangle$ and the measurement is in the X-basis which yields a measurement result $H|0\rangle$ with probability 1. Thus when $d_i = e_i$ we certainly have $y_i = 0$. So

$$P(y_i = 0|e_i = d_i) = 1, \qquad P(y_i = 1|e_i = d_i) = 0.$$

When $d_i \neq e_i$ then, for example $e_i = 1$ and $d_i = 0$, the transmitted state is $|\psi\rangle = H|0\rangle$ but the measurement is done in the Z-basis which results in $|0\rangle$ or $|1\rangle$ with equal probability because $|\langle 0|\psi\rangle|^2 = |\langle 1|\psi\rangle|^2 = (1/\sqrt{2})^2 = 1/2$. So

$$P(y_i = 0|e_i \neq d_i) = \frac{1}{2}, \qquad P(y_i = 1|e_i \neq d_i) = \frac{1}{2}.$$

2) We observe from the above analysis that $y_i = 1$ only when $d_i \neq e_i$. Indeed if $y_i = 1$ then Alice and Bob know that $e_i = 1 - d_i$ for sure, i.e.

$$P(e_i = 1 - d_i|y_i = 1) = 1.$$

This can be proved more formally from Bayes' rule:

$$P(e_i = 1 - d_i|y_i = 1) = \frac{P(y_i = 1|e_i = 1 - d_i)P(e_i = 1 - d_i)}{P(y_i = 1)} = \frac{\frac{1}{2} \times \frac{1}{2}}{\frac{1}{4}} = 1$$

where for the denominator we used

$$\begin{aligned} P(y_i = 1) &= P(y_i = 1|e_i = d_i)P(e_i = d_i) + P(y_i = 1|e_i \neq d_i)P(e_i \neq d_i) \\ &= 0 \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}. \end{aligned}$$

Here we have assumed that $P(e_i \neq d_i) = P(e_i = d_i) = \frac{1}{2}$.

3) The secret key is then generated as follows: Alice and Bob reveal the y_i's and keep the $e_i = 1 - d_i$ such that $y_i = 1$ as their secret bits. The other e_i and d_i are discarded. The length of the resulting secret key is around $N \times P(y_i = 1) = N/4$, a quarter of the length of the main sequence.
We observe a few differences with respect to BB84. First the common secret bits are here constituted from a subset of the encoding and decoding bits. Second the length of the secret key is halved with respect to BB84. However the main advantage of BB92 over BB84 is that in BB92 we manipulate only two non-orthogonal states instead of four in BB84.

4) Alice and Bob can do a security check by exchanging a small fraction $\epsilon N/4$, $0 < \epsilon \ll 1$of the secure bits via public channel. If the test is successful they keep the rest of the common substring secure: thus they have succeeded in generating a common secure string. If there is no attack from Eve's side and the transmission channel is perfect, then as we explained we have $e_i = 1 - d_i$ whenever $y_i = 1$. The test should check that

$$P(e_i = 1 - d_i | y_i = 1) = 1.$$

In practice Alice and Bob check that

$$\#(i \text{ such that } e_i = 1 - d_i \text{ given that } y_i = 1) = \epsilon N/4$$

which means that the empirical probability is one.

Exercise 2 *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 follows 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 applying directly the definition to $|\Psi\rangle$,

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

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 3 *Bell states*

1) For the first question we have

$$\begin{aligned} (CNOT)(H \otimes I)|x\rangle \otimes |y\rangle &= CNOT \frac{1}{\sqrt{2}}\big(|0\rangle + (-1)^x|1\rangle\big) \otimes |y\rangle \\ &= \frac{1}{\sqrt{2}} CNOT|0\rangle \otimes |y\rangle + \frac{1}{\sqrt{2}}(-1)^x CNOT|1\rangle \otimes |y\rangle \\ &= \frac{1}{\sqrt{2}}|0\rangle \otimes |y\rangle + \frac{1}{\sqrt{2}}(-1)^x|1\rangle \otimes |y \oplus 1\rangle \\ &= |B_{xy}\rangle \end{aligned}$$

2) For the second question we remark that if $CNOT$ could be written as $U_1 \otimes U_2$ then we would have

$$\begin{aligned}(CNOT)(H \otimes I)|x\rangle \otimes |y\rangle &= (U_1 \otimes U_2)(H \otimes I)|x\rangle \otimes |y\rangle \\ &= (U_1 H) \otimes (U_2 I)|x\rangle \otimes |y\rangle \\ &= (U_1 H|x\rangle) \otimes (U_2|y\rangle)\end{aligned}$$

and therefore we would have that $|B_{xy}\rangle$ are product states. But we proved in class they are entangled so we have a contradiction.