Quantum Information and Quantum Computing, Solutions 2

Assistant : sara.alvesdossantos@epfl.ch, clemens.giuliani@epfl.ch

Problem 1 : Short practice on measurements and Born's rule

1. $p(0) = p(1) = \frac{1}{2}$
2. $p(0) = \frac{1}{3}$, $p(1) = \frac{2}{3}$
3. $p(01) = p(10) = \frac{1}{4}$, $p(11) = \frac{1}{2}$
4. $p(000) = \frac{1}{9}$, $p(010) = p(111) = \frac{2}{9}$, $p(011) = \frac{4}{9}$, $p(001) = p(100) = p(101) = p(110) = 0$
5. We compute the norm $\|\psi\| = \sqrt{\langle\psi_5|\psi_5\rangle} = \frac{\sqrt{161}}{2}$ and obtain the normalized state $|\tilde{\psi_5}\rangle = \frac{|\psi_5\rangle}{\|\psi_5\|} = \frac{4}{\sqrt{161}}|000\rangle + \frac{3}{\sqrt{161}}|001\rangle + \frac{6}{\sqrt{161}}|101\rangle + \frac{10}{\sqrt{161}}|110\rangle$.
   Then $p(000) = \frac{16}{161}$, $p(001) = \frac{9}{161}$, $p(101) = \frac{36}{161}$, $p(110) = \frac{100}{161}$ and the probabilities of measuring the remaining basis states are 0.

Problem 2 : Measuring in a general basis

1. The operator $\hat{R}_{Z\to X}$ maps the eigenstates $\{|0\rangle, |1\rangle\}$ of the $\hat{Z}$ operator onto the eigenstates $\{|+;X\rangle, |-;X\rangle\}$ of the $\hat{X}$ operator. Mathematically, this can be expressed as:

$$\begin{aligned}\hat{R}_{Z\to X} &= |+;X\rangle\langle 0| + |-;X\rangle\langle 1| = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1| \\ &= \frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\Big).\end{aligned} \tag{1}$$

   Having written it in the form $\hat{R} = \sum_{i,j}\langle i|\hat{R}|j\rangle\,|i\rangle\langle j|$ we can directly read off the coefficients of the matrix representation of $\hat{R}_{Z\to X}$ in the computational basis:

$$R_{Z\to X} = \begin{bmatrix}\langle 0|\hat{R}_{Z\to X}|0\rangle & \langle 0|\hat{R}_{Z\to X}|1\rangle \\ \langle 1|\hat{R}_{Z\to X}|0\rangle & \langle 1|\hat{R}_{Z\to X}|1\rangle\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{2}$$

   Similarly,

$$\begin{aligned}\hat{R}_{Z\to Y} &= |+;Y\rangle\langle 0| + |-;Y\rangle\langle 1| = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}\langle 1| \\ &= \frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + i\,|1\rangle\langle 0| - i\,|1\rangle\langle 1|\Big).\end{aligned} \tag{3}$$

and thus

$$R_{Z\to Y} = \begin{bmatrix} \langle 0|\hat{R}_{Z\to Y}|0\rangle & \langle 0|\hat{R}_{Z\to Y}|1\rangle \\ \langle 1|\hat{R}_{Z\to Y}|0\rangle & \langle 1|\hat{R}_{Z\to Y}|1\rangle \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}. \tag{4}$$

2. Recall that $|\psi\rangle^\dagger = \langle\psi|$ and $\langle\psi|\,\hat{R}^\dagger = \left(\hat{R}\,|\psi\rangle\right)^\dagger$. We obtain that $\langle +; X| = \langle 0|\,\hat{R}^\dagger_{Z\to X}$ and $\langle -; X| = \langle 1|\,\hat{R}^\dagger_{Z\to X}$ and the probabilities

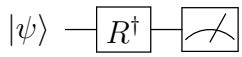
$$\begin{aligned} P_{|+;X\rangle} &= |\langle +; X|\psi\rangle|^2 \quad = \left|\,\langle 0|\hat{R}^\dagger_{Z\to X}|\psi\rangle\right|^2 \\ P_{|-;X\rangle} &= |\langle -; X|\psi\rangle|^2 \quad = \left|\,\langle 1|\hat{R}^\dagger_{Z\to X}|\psi\rangle\right|^2. \end{aligned} \tag{5}$$

Similarly, for $\hat{R}_{Z\to Y}$

$$\begin{aligned} P_{|+;Y\rangle} &= \left|\,\langle 0|\hat{R}^\dagger_{Z\to Y}|\psi\rangle\right|^2 \\ P_{|-;Y\rangle} &= \left|\,\langle 1|\hat{R}^\dagger_{Z\to Y}|\psi\rangle\right|^2. \end{aligned} \tag{6}$$

3. The procedure to measure a state $|\psi\rangle$ in the eigenbasis of a general hermitian observable $\hat{O}$ on a single qubit is as follows:
   (a) Diagonalize $\hat{O}$ to find its eigenstates $|\phi_0\rangle$ and $|\phi_1\rangle$.
   (b) Construct the operator $\hat{R} = |\phi_0\rangle\langle 0| + |\phi_1\rangle\langle 1|$ that maps the computational basis states to the eigenbasis of the operator.
   (c) Apply $\hat{R}^\dagger$ to the state $|\psi\rangle$ and measure the resulting state in the computational basis.

4. The corresponding quantum circuit is



Problem 3 : Quantum key distribution

In this problem we are going to see how the BB84 protocol for quantum cryptography works. In this case Alice wants to send a random binary number to Bob, but she wants to keep it secret for everyone else. She decides to use quantum mechanics for her purpose and the protocol BB84.

1. Looking at the whole process, we can create a table that contains all the useful information about it. states are defined as $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, $|0\rangle = \frac{|+\rangle+|-\rangle}{\sqrt{2}}$, and $|1\rangle = \frac{|+\rangle-|-\rangle}{\sqrt{2}}$. Therefore, measuring X when a computational basis state is produced gives us a 0 or a 1 with probability $\frac{1}{2}$.

2. After comparing the two strings b and b', Alice and Bob retain only the bit in which b and b' coincide, with the result

a_i	b_i	qubit sent	b'_i	a'_i	probability
0	0	$\|0\rangle$	0	0	1
1	0	$\|1\rangle$	1	1,0	$\frac{1}{2},\frac{1}{2}$
1	1	$\|-\rangle$	0	1,0	$\frac{1}{2},\frac{1}{2}$
0	0	$\|0\rangle$	0	0	1
1	1	$\|-\rangle$	1	1	1
1	1	$\|-\rangle$	1	1	1
0	1	$\|+\rangle$	0	1,0	$\frac{1}{2},\frac{1}{2}$
0	0	$\|0\rangle$	0	0	1
0	1	$\|+\rangle$	1	0	1

a_i	0	0	1	1	0	0
a'_i	0	0	1	1	0	0

3. Given N qubits transmitted, we want to know the probability of having n concidences. When Alice produces a qubit and sends it to Bob to measure it, we have 4 possible basis choices:

$$(A,B): \quad (Z,Z) \quad (Z,X) \quad (X,Z) \quad (X,X) \quad . \tag{7}$$

Every event has probability $\frac{1}{4}$, this means that the probability to produce and measure in the same basis is the sum of (Z,Z) and (X,X), so $p=\frac{1}{2}$. As a consequence, the probability of having n coincidenecs in a N-qubit process is given by the binomial distribution

$$P(N,n) = \frac{N!}{(N-n)!n!}\left(\frac{1}{2}\right)^n\left(\frac{1}{2}\right)^{N-n} \tag{8}$$

and the average is $Np=\frac{N}{2}$. Due to the Central Limit Theorem (CLT), in the limit of $N \gg 1$, keeping p fixed, $P(N,n)$ approaches a normal distribution $P_g(\mu,\sigma)=P_g(pN,Np(1-p))$, that again gives an average length of the string of $\frac{N}{2}$.

4. if we now consider an eavesdropper in the process, called Eve, she must measure the qubit sent by Alice, prepare a new state equal to the one she measured and send it to Bob, thus hoping that she is not detected. Remember that Eve cannot know the quantum state of the qubit, nor clone it. For the measurement, Eve must choose a basis, so we have again 4 possibilities

$$(A,E): \quad (Z,Z) \quad (Z,X) \quad (X,Z) \quad (X,X) \quad . \tag{9}$$

If Eve does not choose the same basis as Alice, then her measurement will certainly modify the state of the qubit because of the collapse. These are the cases where Eve may be detected. In cases where Eve chooses the same basis as Alice, Eve can successfully know the state of the qubit without modifying it. The probability of Eve choosing a basis different from Alice's one is $p'=\frac{1}{2}$.

5. Even if $b_i=b'_i$, Bob may measure the wrong bit of information, because the state of the qubit has been projected onto the other basis by Eve, which results in equal probabilities for Bob to measure the two outcomes. As Alice and Bob do not share the key, but only the different

basis choices, Bob won't notice the intrusion. The eavesdropper damages the communication. Bob and Alice have to share part of their key in order to check if someone was eavesdropping the transmission.

6. Suppose Alice and Bob compared their basis choices and found $2n$ coincidences. They decide to share n bits of the key. When $b_i = b'_i$, again we have 4 different situations

$$(A, E, B): \quad (Z, Z, Z) \quad (Z, X, Z) \quad (X, Z, X) \quad (X, X, X) \quad . \tag{10}$$

When Eve chooses the wrong basis, she prepares the wrong state and there is a probability $\frac{1}{2}$ that Bob won't measure the same bit sent by Alice. For each case the probability of not detecting Eve in a single coincidence event is

$$\begin{aligned}
(Z, Z, Z) &\longrightarrow \frac{1}{4} \\
(X, X, X) &\longrightarrow \frac{1}{4} \\
(Z, X, Z) &\longrightarrow \frac{1}{4} * \frac{1}{2} = \frac{1}{8} \\
(X, Z, X) &\longrightarrow \frac{1}{4} * \frac{1}{2} = \frac{1}{8}
\end{aligned}$$

totaling to $\frac{3}{4}$. For n coincidences, the probability of not detecting Eve is then

$$P_e = \left(\frac{3}{4}\right)^n \tag{11}$$

which exponentially approaches 0. This means that there's never the certainty of detecting Eve. However, by choosing n large enough, we can make the detection of Eve arbitrarily accurate. As a result, after each batch of $4n$ qubits, Alice and Bob can almost certainly detect if the transmission was eavesdropped, and consequently decide whether to retain the subset of n bits that haven't been compared as a good key, or rather to start the process over.

As a final comment, it is important to notice that in this case we are not considering the intrinsic noise of the channel and of the measurements. Noise will induce a certain amount of error in the procedure, making it more difficult to detect eavesdropping. Therefore is important to fully characterize the transmission channel before using it.