Quantum Information and Quantum Computing, Problem set 2

Assistants : sara.alvesdossantos@epfl.ch, david.linteau@epfl.ch, shao.chiew@epfl.ch

The goal of this problem set is to become familiar with the measurement process in quantum mechanics and in particular with the collapse of the state that generally follows the measurement. To this purpose, we will first address the problem of measuring in the eigenbasis of an arbitrary observable. Then, we will study one of the most important and widespread quantum information protocols: the *quantum key distribution* (commonly known as *quantum cryptography*).

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

Find the probability of measuring each of the computational basis states for the following quantum states:

$|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$|\psi_2\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$

$|\psi_3\rangle = \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$

$|\psi_4\rangle = \frac{1}{3}|000\rangle + \frac{\sqrt{2}}{3}|010\rangle + \frac{2}{3}|011\rangle + \frac{\sqrt{2}}{3}|111\rangle$

$|\psi_5\rangle = 2|000\rangle + \frac{3}{2}|001\rangle + 3|101\rangle + 5|110\rangle$
(Is this a valid state? What can we do to change that?)

Problem 2 : Measuring in a general basis

In this problem, we will understand how we can measure in the eigenbasis of any general Hermitian observable. First, we will see how to measure in the Pauli X and Y basis.
Recall their eigenvectors, which are given by

$$\begin{aligned} |\pm; X\rangle &= \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \\ |\pm; Y\rangle &= \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}}. \end{aligned} \tag{1}$$

Given a state $|\psi\rangle$, we want to calculate the probabilities

$$\begin{aligned} P_{|\pm;X\rangle} &= |\langle \pm; X|\psi\rangle|^2 \\ P_{|\pm;Y\rangle} &= |\langle \pm; Y|\psi\rangle|^2. \end{aligned} \tag{2}$$

We know that all measurements on quantum computers are carried out in the computational basis (Pauli Z basis). Can we apply some opertations to measure in a different basis?

1. Begin by constructing the change-of-basis matrices $R_{Z\to X}$ and $R_{Z\to Y}$ that change the Pauli Z basis into the Pauli X and Y bases. More explicitly, find the matrices $R_{Z\to X}$, such that

$$\begin{aligned} R_{Z\to X}\,|0\rangle &= |+;X\rangle \\ R_{Z\to X}\,|1\rangle &= |-;X\rangle \end{aligned} \tag{3}$$

and $R_{Z\to Y}$, such that

$$\begin{aligned} R_{Z\to Y}\,|0\rangle &= |+;Y\rangle \\ R_{Z\to Y}\,|1\rangle &= |-;Y\rangle \end{aligned} \tag{4}$$

2. Now that we established the relation between the bases, try to reformulate the right-hand sides of Equation (2) in terms of the matrices $R_{Z\to X}$, $R_{Z\to Y}$ and the computational basis elements $|0\rangle$ and $|1\rangle$.

3. Finally, devise a procedure to measure in the eigenbasis of a general observable $\hat{O}$.

4. If you are already familiar with quantum circuits, construct the circuit that performs a measurement in such a basis. For those who are not familiar yet, try it after next week's lecture.

Problem 3 : Quantum key distribution

We will study here the quantum key distribution protocol known as BB84 (Bennett, Brassard, 1984), which was the first quantum cryptography protocol to be conceived. It is more correctly called *quantum key distribution* (QKD) because the goal is to share between two parties, in a fully secure way, a random sequence of bits which can then be used as a cryptographic key for a traditional cryptography algorithm like e.g. the AES. The peculiarity of QKD is that the security of the protocol is guaranteed (within certain limits) by the very principles of quantum mechanics, and in particular by the no-cloning theorem and by the impossibility to extract information from a quantum state without disturbing it.

Here's how BB84 works. Alice and Bob want to share a key and Alice has a quantum information channel available that enables her to send the qubits to Bob. Alice can choose to set the state of each qubit, either to one of the states of the computational basis $\{|0\rangle\,,\,|1\rangle\}$ – on which the operator Z is diagonal – or to one of the states of the basis $\{|+\rangle = \frac{|0\rangle+|1\rangle)}{\sqrt{2}},\, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ – on which the operator X is diagonal. Alice uses the two states in each of these two bases to represent the classical information: $0 \to |0\rangle$ and $1 \to |1\rangle$ or $0 \to |+\rangle$ and $1 \to |-\rangle$. Bob on his side can choose to measure either Z or X on each of the incoming qubits, and translates the result of the measurements into the classical values 0 and 1.

Alice generates two sequences of random bits, each of length N. For example:

$$(a_i) = (0,1,1,0,1,1,0,0,0,\dots) \tag{5}$$

$$(b_i) = (0,0,1,0,1,1,1,0,1,\dots). \tag{6}$$

The sequence (a_i) is the one that Alice wishes to transmit to Bob. The sequence (b_i) determines which of the two bases will be used by Alice for encoding the corresponding bits in (a_i): $\{|0\rangle\,,\,|1\rangle\}$ if $b_i = 0$, and $\{|+\rangle\,,\,|-\rangle\}$ if $b_i = 1$. On his side, Bob generates a random sequence (b'_i) of N bits, for example

$$(b'_i) = (0,1,0,0,1,1,0,0,1,\dots). \tag{7}$$

This sequence will determine which of the two operators Bob will measure for each qubit received: Z if $b'_i = 0$, and X if $b'_i = 1$. Bob denotes (a'_i) the sequence of bits obtained as a result of this measurement protocol.

1. Write a table containing the sequences (5), (6) and (7), as well as, for $i = 1, .., 9$, the state of the qubit sent to Bob, the measurement basis, the possible results a'_i of the measurements, and the associated probabilities.

After this quantum communication stage, Alice and Bob make the two basis choices b and b' public, they compare them, and they retain in the sequences a and a' only the bits a_i and a'_i for which $b_i = b'_i$.

2. Show that this procedure enables Alice and Bob to share a sequence of bits that they can use as a key. Use the table previously written. Assume that no external disturbance affects the measurement.

3. For large N, what is the average length of the key shared in this way? Justify the result by showing that the probability $p(N, n)$ of having n coincidences $b'_i = b_i$ is distributed according to a binomial distribution $f(N, n, \rho) = \rho^n(1-\rho)^{N-n}N!/[(N-n)!n!]$ with $\rho = 1/2$, and in particular using the fact that the average of this distribution is $N\rho$ and its variance $N\rho(1-\rho)$.

We assume now that the length of the sequence is $N = 4n + \delta$, with n large and δ equally large so that the probability of a number of coincidences smaller than $2n$ is negligible. In the absence of eavesdropping, Alice and Bob can thus retain a key of length $2n$.

The fact that the choices b and b' are only published at the end of the protocol, is important for its security. If the eavesdropper – named Eve – can only eavesdrop the quantum communication channel, to extract information she must intercept the qubits sent by Alice, measure them in a basis that she chooses without knowing the basis used by Alice to encode the information, and then prepare a qubit to be sent to Bob in the state that she actually measured, in the hope that Bob doesn't notice her intervention. We are therefore going to assume that Eve will eavesdrop all qubits sent by Alice.

4. What is the probability that the basis b''_i, chosen by Eve for one given qubit, is not compatible with that used by Alice for encoding?

5. By examining for example the case $b_1 = b'_1 = 0$, $a_1 = 0$ and $b''_1 = 1$, as well as the probabilities associated to all possible results of Eve's and then Bob's measurements (that we denote a''_1 and a'_1), explain which is the impact of the eavesdropping on the transmission.

In order to detect whether an eavesdropping took place, Alice (or Bob) publish a random subset of n bits chosen among the $2n$ bits a_i (or a'_i) that have been retained after the bases b and b' have been published. Bob (Alice) compares this published sequence to his (her) corresponding sequence. Eve's intervention will then appear as discrepancies between these two sequences. If Eve's intervention is detected, all sequences are thrashed and the protocol is started again from scratch.

6. Compute the probability that Eve's eavesdropping is not detected, as a function of n. Draw your own conclusions as to the effectiveness of the protocol.