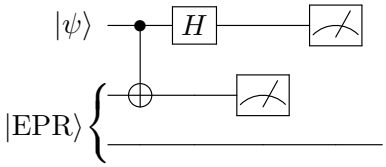
Introduction to Quantum Information Science
Recitation, week 5

Partial measurements, BB84, and some practice

1. Partial measurements in other bases Consider the following circuit:



Let $|\psi\rangle = |+\rangle$. Suppose that the measurements are not made in the standard $|0\rangle / |1\rangle$ basis, but in the $|+\rangle / |-\rangle$ basis.

a) What are the probabilities of observing $|+\rangle / |-\rangle$ on the middle qubit? And on the top qubit?

Note: If you find the math to solve this problem clunky, that's because it is. We actually are not teaching you the standard way to make partial measurements, using reduced density matrices and the partial trace, which you'll learn about later in this course. Instead, we rely on some algebra and a small bit of intuition which we hope you're learning.

Solution: Borrowing from some of the calculations we did in the previous Recitation, and plugging in the definition of our state $|\psi\rangle$, the state of the system before the measurements is

$$\frac{|000\rangle + |100\rangle + |011\rangle + |111\rangle + |010\rangle - |110\rangle + |001\rangle - |101\rangle}{2\sqrt{2}}.$$

Because there are no further interactions between the top and middle qubits, the order in which we measure does not matter. So just by personal choice, begin by measuring the top qubit.

We factor and rewrite the state as

$$|\phi\rangle := \frac{|0\rangle \otimes (|00\rangle + |11\rangle) + |1\rangle \otimes (|00\rangle + |11\rangle) + |0\rangle \otimes (|10\rangle + |01\rangle) - |1\rangle \otimes (|10\rangle + |01\rangle)}{2\sqrt{2}}$$

$$\frac{|+\rangle \otimes (|00\rangle + |11\rangle) + |-\rangle \otimes (|10\rangle + |01\rangle)}{2}$$

$$\frac{|+\rangle \otimes |\text{EPR}\rangle}{\sqrt{2}} + \frac{|-\rangle \otimes \frac{|10\rangle + |01\rangle}{\sqrt{2}}}{\sqrt{2}}$$

From this, it is clear the probability of observing $|+\rangle$ on the first qubit is $1/2$, and similarly the probability of $|-\rangle$ is $1/2$.

Now to measure the middle qubit. Because we do not know with certainty what the result of the measurement on the first qubit is, we proceed by cases. If the first measurement observes $|+\rangle$, then the state of the system is the EPR state. As we've seen in class, the probability of observing $|+\rangle$ or

$|-\rangle$ on either qubit of an EPR pair is 50%, and this could be verified by taking the inner product $|\langle +0|\text{EPR}\rangle|^2 + |\langle +1|\text{EPR}\rangle|^2$. If the first measurement observes $|-\rangle$, then the state of the system is $|\psi^+\rangle := \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$ (another one of the "Bell States"). We can rewrite that state as

$$|\psi^+\rangle = \frac{1}{2}(|+\rangle - |-\rangle) \otimes |0\rangle + \frac{1}{2}(|+\rangle + |-\rangle) \otimes |1\rangle .$$

From this, it is clear that the probability of observing $|+\rangle$ is again 50%.

Since the middle qubit has a 50% chance of $|+\rangle$ in either case after measuring the first qubit, we conclude the middle qubit has a 50% chance overall of $|+\rangle$, and similarly 50% chance of $|-\rangle$.

b) If the top and middle qubits are observed to be in state $|+-\rangle$, then what state is the bottom qubit in?

Solution: In the previous solution, we already found that if the first qubit measured as $|+\rangle$, then the remaining two qubits are in the EPR state.

We rewrite the EPR state as

$$\frac{|++\rangle + |--\rangle}{\sqrt{2}},$$

which you can verify for yourself. From this, it is clear that if $|-\rangle$ is observed on the middle qubit, then the corresponding state of the third qubit is $|-\rangle$.

Note that whenever we write the remnant state, it should be normalized. For example, one might be tempted to have answered $\frac{|-\rangle}{\sqrt{2}}$ above, but that would not be a normalized state.

2. BB84 Recap In this question we'll step through a round of BB84 to see how the mechanics work.

Suppose Alice wanted to secretly send a congratulatory message to Bob. She starts by generating a pair of random bit strings $a = 100110$ and $b = 000101$.

a) If Alice uses the string b to choose a basis ($|0\rangle / |1\rangle$ or $|+\rangle / |-\rangle$) to encode her state into, and a to choose one of the two states in that basis, then what state $|\psi\rangle$ will she generate?

Solution: Let's say that bit $b_i = 0$ corresponds to the 0/1 basis and that $b_i = 1$ to the $+/-$ basis. We'll let $a_i = 0$ mean $|0\rangle$ or $|+\rangle$ (depending on the basis determined by b_i) and $a_i = 1$ means $|1\rangle$ or $|-\rangle$.

This gives the state:

$$|\psi\rangle = |1\rangle\,|0\rangle\,|0\rangle\,|-\rangle\,|1\rangle\,|+\rangle$$

b) Alice sends $|\psi\rangle$ to Bob, and Bob generates a random string $b' = 011101$ which is used to determine the measurement bases he chooses (where Alice and Bob will use the same rules for what bits means what basis). What is a possible set of observations from Bob, encoded as a bit string a'?

Solution:

$$a' = 1??110$$

where the ?s can be either 0 or 1, e.g 101110.

c) Alice now announces b publicly and Bob announces where b and b' differ. They drop the bits a_i corresponding to bits b_i where they differed. What string is left behind for Alice and Bob?

Solution:

$$c = 1110$$

The second and third bits were dropped because Alice and Bob chose different bases.

d) Now, assume there was an eavesdropper who intercepted all of Alice's quantum messages and then sent some messages, maybe the same maybe different, to Bob. How would Alice and Bob be able to detect this with high probability? (This problem is more open-ended than the others — be creative.)

Solution: One way is for Alice to choose half of the remaining bits at random (from random positions in the string) and announce them publicly. Bob can then check his bit string at those locations and confirm that they match up. If they don't match, then they know that the states have been tampered with and discard all the bits. If they do match, then they use the remaining bits as their secret key.

Is it possible for Eve to attack this strategy? Let's say that after a while of doing BB84, Alice and Bob have n shared bits. The simplest thing Eve could do is guess a measurement basis for every qubit she intercepts, measure in that basis, and send a copy of the measured outcome on to Bob. If she picks the correct basis then Bob and Alice won't see a difference in their bit string. If Eve chooses the wrong basis, then there is a 50% chance that Bob shares a basis with Alice but recorded the wrong measurement outcome. As such, if Alice and Bob check half their bits, then the probability that none of the bits they check is incorrect is $(3/4)^{n/2}$.

Even if Eve had a more sophisticated method for analyzing the qubits, a more sophisticated argument shows that Alice and Bob can always detect the eavesdropping with probability $1 - c^{n/2}$.

3. Generalization of the X and Z gates via Clock-and-Shift Recall the following single-qubit unitary gates:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad\qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

In this problem, just for fun, we'll see one way to generalize these matrices to higher dimensions. Let's say that we're in a d-level system, such that a single qudit can be in a superposition of states from $|0\rangle$ to $|d-1\rangle$.

Suppose we define X and Z according to $X|n\rangle = |n+1 \bmod d\rangle$ and $Z|n\rangle = \omega^n |n\rangle$ where $\omega = e^{2\pi i/d}$ is the primitive d-th root of unity.

a) Verify that X and Z are unitary.

Solution: For this problem, the easiest is to check that they send the standard basis to an orthonormal basis.

First check orthogonality. Suppose $m \neq n$:

$$\langle m| X^\dagger X |n\rangle = \langle m+1 \bmod d | n+1 \bmod d\rangle = 0$$
$$\langle m| Z^\dagger Z |n\rangle = \langle m| \omega^{-m}\omega^n |n\rangle = \omega^{n-m} \langle m|n\rangle = 0$$

Second check normality. Suppose $m = n$:

$$\langle n| X^\dagger X |n\rangle = \langle n+1 \bmod d | n+1 \bmod d\rangle = 1$$
$$\langle n| Z^\dagger Z |n\rangle = \langle n| \omega^{-n}\omega^n |n\rangle = \langle n|n\rangle = 1$$

b) Show that $X^d = Z^d = I$.

Solution: We verify that the action on standard basis vectors is equal to the identity:

$$X^d |n\rangle = |n + d \bmod d\rangle = |n\rangle$$
$$Z^d |n\rangle = (\omega^n)^d |n\rangle = \omega^{nd} |n\rangle = |n\rangle$$

c) Show that $ZX = kXZ$ for some constant k that depends only on d.

Solution:

$$ZX |n\rangle = Z |n + 1 \bmod d\rangle = \omega^{n+1} |n + 1 \bmod d\rangle$$
$$XZ |n\rangle = \omega^n X |n\rangle = \omega^n |n + 1 \bmod d\rangle$$
$$ZX |n\rangle = \omega XZ |n\rangle$$

Since this holds for all basis vectors $|n\rangle$, we must have that:

$$ZX = \omega XZ$$

d) For $d = 2$, the matrices X and Z are also *Hermitian*: they satisfy $X = X^\dagger$ and $Z = Z^\dagger$. Are the generalized X and Z matrices Hermitian for $d > 2$?

Solution: No. For a Hermitian matrix U to be unitary, it must satisfy $UU^\dagger = U^2 = I$. But for $d > 2$, X and Z do not square to the identity:

$$X^2 |n\rangle = |n + 2 \bmod d\rangle$$
$$Z^2 |n\rangle = \omega^2 |n\rangle$$