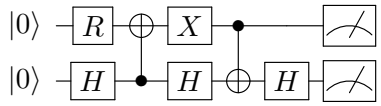
Introduction to Quantum Information Science
Homework 4

Due Wednesday, September 29 at 11:59 PM

1. Multi-qubit measurements in other bases Consider the following circuit:



where $R = \frac{1}{\sqrt{3}}\begin{bmatrix}\sqrt{2} & 1\\ 1 & -\sqrt{2}\end{bmatrix}$. The final state of the system before measuring is:

$$|\psi\rangle = \frac{|00\rangle + \sqrt{2}\,|10\rangle + \sqrt{2}\,|01\rangle - |11\rangle}{\sqrt{6}}.$$

a) [2 points] Suppose the top measurement is in the $|+\rangle\,/\,|-\rangle$ basis. What is the probability we observe $|+\rangle$ on the top qubit? Show your work.

Solution: (Solution 1) Rewrite $|\psi\rangle$ so the first qubit is in the $|+\rangle\,/\,|-\rangle$ basis. Begin by grouping terms according to the first qubit:

$$|\psi\rangle = \frac{\left(|0\rangle + \sqrt{2}\,|1\rangle\right)\otimes|0\rangle + \left(\sqrt{2}\,|0\rangle - |1\rangle\right)\otimes|1\rangle}{\sqrt{6}}.$$

Next, we change the basis of the first qubit from $|0\rangle\,/\,|1\rangle$ to $|+\rangle\,/\,|-\rangle$:

$$\begin{aligned}|\psi\rangle &= \frac{\left(\frac{|+\rangle+|-\rangle}{\sqrt{2}} + \sqrt{2}\frac{|+\rangle-|-\rangle}{\sqrt{2}}\right)\otimes|0\rangle + \left(\sqrt{2}\frac{|+\rangle+|-\rangle}{\sqrt{2}} - \frac{|+\rangle-|-\rangle}{\sqrt{2}}\right)\otimes|1\rangle}{\sqrt{6}}\\ &= \frac{\left(\frac{1+\sqrt{2}}{\sqrt{2}}\,|+\rangle + \frac{1-\sqrt{2}}{\sqrt{2}}\,|-\rangle\right)\otimes|0\rangle + \left(\frac{\sqrt{2}-1}{\sqrt{2}}\,|+\rangle + \frac{\sqrt{2}+1}{\sqrt{2}}\,|-\rangle\right)\otimes|1\rangle}{\sqrt{6}}.\end{aligned}$$

Now, the probabilities are clear from inspection. The probability of observing $|+\rangle$ on the first qubit is $\left|\frac{1+\sqrt{2}}{\sqrt{2}\sqrt{6}}\right|^2 + \left|\frac{\sqrt{2}-1}{\sqrt{2}\sqrt{6}}\right|^2 = \frac{1}{2}$ (we sum the probabilities, not the amplitudes, because the amplitudes belong to orthogonal/mutually exclusive states).

(Solution 2) The probability is $|\langle+0|\psi\rangle|^2 + |\langle+1|\psi\rangle|^2$. We compute

$$|\langle+0|\psi\rangle|^2 = \left|\frac{\langle+|0\rangle + \sqrt{2}\,\langle+|1\rangle + 0 - 0}{\sqrt{6}}\right|^2 = \left|\left(\frac{1}{\sqrt{2}} + \frac{\sqrt{2}}{\sqrt{2}}\right)\frac{1}{\sqrt{6}}\right|^2 = \left|\frac{1+\sqrt{2}}{\sqrt{12}}\right|^2 = \frac{3+2\sqrt{2}}{12},$$

$$|\langle+1|\psi\rangle|^2 = \left|\frac{0 + 0 + \sqrt{2}\,\langle+|0\rangle - \langle+|1\rangle}{\sqrt{6}}\right|^2 = \left|\left(\frac{\sqrt{2}}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right)\frac{1}{\sqrt{6}}\right|^2 = \left|\frac{\sqrt{2}-1}{\sqrt{12}}\right|^2 = \frac{3-2\sqrt{2}}{12}.$$

The sum of these expressions is $\frac{6}{12} = \frac{1}{2}$.

b) [2 points] If we observe $|+\rangle$ on the top qubit, then what is the state of the bottom qubit? Show your work.

Solution: If Solution 1 was followed for part (a), then rearrange to group by $|+\rangle$ on the first qubit:

$$\frac{|+\rangle \otimes \left(\frac{1+\sqrt{2}}{\sqrt{2}}|0\rangle + \frac{\sqrt{2}-1}{\sqrt{2}}|1\rangle\right) + |-\rangle \otimes \left(\frac{1-\sqrt{2}}{\sqrt{2}}|0\rangle + \frac{\sqrt{2}+1}{\sqrt{2}}|1\rangle\right)}{\sqrt{6}}.$$

Then, it is clear which components of the second qubit are compatible with an observation $|+\rangle$ on the first qubit. We just need to normalize the vector:

$$\left\| \left(\frac{1+\sqrt{2}}{\sqrt{2}}|0\rangle + \frac{\sqrt{2}-1}{\sqrt{2}}|1\rangle\right)\frac{1}{\sqrt{6}} \right\| = \frac{1}{\sqrt{2}}.$$

So, divide the vector by $\frac{1}{\sqrt{2}}$, simplify, and the state of the second qubit is

$$|\psi_2\rangle = \frac{1}{\sqrt{6}}\left(\left(1+\sqrt{2}\right)|0\rangle + \left(\sqrt{2}-1\right)|1\rangle\right).$$

c) [2 points] What is the probability the joint outcome of the two measurements is $|+-\rangle$? Show your work.

Solution: This can be computed by starting with the original state and finding $|\langle +-|\psi\rangle|^2$, or viewing the measurements as sequential and combining our results from parts a and b; the methods are equivalent.

From part a, the probability of observing $|+\rangle$ on the first qubit is 1/2. From part b, we compute

$$|\langle -|\psi_2\rangle|^2 = \left|\frac{1}{\sqrt{6}}\left(\frac{1+\sqrt{2}}{\sqrt{2}} - \frac{\sqrt{2}-1}{\sqrt{2}}\right)\right|^2 = \left|\frac{2}{\sqrt{12}}\right|^2 = \frac{1}{3}.$$

Therefore, the overall probability is $\frac{1}{2}\cdot\frac{1}{3} = \frac{1}{6}$.

2. From Cloning To Faster-Than-Light Signaling [3 Points] Suppose Alice and Bob shared the entangled state

$$|\text{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

And suppose also that Bob had in his possession a magic box that could clone qubits, mapping any qubit $|\psi\rangle$ to $|\psi\rangle \otimes |\psi\rangle$. (Of course, by the No-Cloning Theorem, such a box would violate quantum mechanics.) Explain how, by using the entangled state together with the magic cloning box, Alice could instantaneously transmit a 1-bit message of her choice to Bob, so that Bob could read it (succeeding with high probability). [Hint: What happens when Alice measures her qubit in different bases?]

Solution: Recall that the EPR-pair can alternately be expressed as

$$|\text{EPR}\rangle = \frac{|++\rangle + |--\rangle}{\sqrt{2}}.$$

Thus, if Alice measures her half in the $\{|0\rangle, |1\rangle\}$-basis, Bob's qubit will also collapse to either $|0\rangle$ or $|1\rangle$ depending on her outcome. While if Alice measures in the $\{|+\rangle, |-\rangle\}$-basis, Bob's qubit will assume the state $|+\rangle$ or $|-\rangle$.

Now assume Bob could clone his qubit. Then he could tell which of the above is the case by simply making many copies of his half and measuring them all in the $\{|0\rangle, |1\rangle\}$-basis. If he either consistently measures $|0\rangle$ or he consistently measures $|1\rangle$, then he can conclude that Alice must've measured in the $\{|0\rangle, |1\rangle\}$-basis. Otherwise, if he sometimes gets $|0\rangle$ and sometimes gets $|1\rangle$, then Alice must've used the $\{|+\rangle, |-\rangle\}$-basis.

3. Elitzur-Vaidman Counterfeiting [5 Points] Recall, from lecture, the "Elitzur-Vaidman bomb attack" on Wiesner's money scheme. In the example that we discussed, the counterfeiter has a control qubit $|c\rangle$, initially in the state $|0\rangle$, as well as a qubit $|\psi_i\rangle$ in a quantum money bill that she would like to learn. The counterfeiter repeats the following $\frac{\pi}{2\epsilon}$ times, for some small ϵ (this is one of up to four subroutines the counterfeiter will run until they find the one that succeeds):

1. Apply R_ϵ to $|c\rangle$ where
$$R_\epsilon = \begin{bmatrix} \cos(\epsilon) & -\sin(\epsilon) \\ \sin(\epsilon) & \cos(\epsilon) \end{bmatrix}.$$
2. Apply a CNOT with $|c\rangle$ as the control and $|\psi_i\rangle$ as the target.
3. Submit the bill with $|\psi_i\rangle$ to the bank for verification.

Finally the counterfeiter measures $|c\rangle$ in the $\{|0\rangle, |1\rangle\}$-basis. If they observe $|1\rangle$, then they conclude the qubit on the banknote was $|+\rangle$, and if they observe $|0\rangle$, then conclude it was not.

We showed in class that if $|\psi_i\rangle = |0\rangle$, then with high probability this procedure leaves $|c\rangle$ in the state $|0\rangle$, while if $|\psi_i\rangle = |+\rangle$ then it slowly rotates $|c\rangle$ to the state $|1\rangle$, and that in both cases, there is little or no chance that the bank will be tipped off by a failed verification. What happens here if $|\psi_i\rangle$ is $|1\rangle$? What if it is $|-\rangle$? Show your work.

Solution: If $|\psi_i\rangle = |1\rangle$, then the three steps produce

$$\begin{gathered} |01\rangle \\ \downarrow R_\epsilon \otimes I \\ \cos(\epsilon)\,|01\rangle + \sin(\epsilon)\,|11\rangle \\ \downarrow \text{CNOT} \\ \cos(\epsilon)\,|01\rangle + \sin(\epsilon)\,|10\rangle. \end{gathered}$$

At this point the counterfeiter hands the second qubit back to the bank for verification. The bank then measures in the $\{|0\rangle, |1\rangle\}$-basis, gets the result $|1\rangle$ with probability $\cos(\epsilon)^2 = 1 - O(\epsilon^2)$, and thereby puts the first qubit back into the $|0\rangle$ state in all likelihood.

On the other hand, if $|\psi_i\rangle = |-\rangle$, then the steps are

$$\begin{gathered} |0-\rangle \\ \downarrow R_\epsilon \otimes I \\ \big(\cos(\epsilon)\,|0\rangle + \sin(\epsilon)\,|1\rangle\big) \otimes |-\rangle = \frac{\cos(\epsilon)\big(|00\rangle - |01\rangle\big) + \sin(\epsilon)\big(|10\rangle - |11\rangle\big)}{\sqrt{2}} \\ \downarrow \text{CNOT} \end{gathered}$$

$$\frac{\cos(\epsilon)\big(|00\rangle - |01\rangle\big) - \sin(\epsilon)\big(|10\rangle - |11\rangle\big)}{\sqrt{2}} = \big(\cos(\epsilon)\,|0\rangle - \sin(\epsilon)\,|1\rangle\big) \otimes |-\rangle\,.$$

In this case, since the bank will measure in the $\{|+\rangle, |-\rangle\}$-basis, its measurement outcome will be $|-\rangle$ with certainty, leaving $|c\rangle$ in its current state; slightly rotated towards $-|1\rangle$. The second iteration then immediately rotates $|c\rangle$ back to $|0\rangle$ upon which the state evolves as

$$\begin{gathered} |0-\rangle \\ \downarrow \text{CNOT} \\ |0-\rangle\,. \end{gathered}$$

$|c\rangle$ thus oscillates back and forth between $|0\rangle$ and $R_{-\epsilon}\,|0\rangle$ and is ultimately almost certainly measured to be $|0\rangle$.

4. SARG04 Quantum Key Distribution In class we discussed the BB84 QKD scheme. There is a similar key distribution protocol, called SARG04, which we study in this problem.

a) [1 Point] Alice randomly samples two bitstrings a and b. She prepares a six qubit state $|\psi\rangle$ that encodes the string a according to bases given by b using the following protocol: for the i-th qubit, if $b_i = 0$ then she maps $a_i = 0 \mapsto |0\rangle, a_i = 1 \mapsto |1\rangle$, and if $b_i = 1$ then she sets $a_i = 0 \mapsto |+\rangle, a_i = 1 \mapsto |-\rangle$.

Suppose the strings are $a = 011001$ and $b = 101011$. Write down $|\psi\rangle$.

Solution:

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

b) [1 Point] Alice sends $|\psi\rangle$ to Bob on a public quantum channel. An attacker Eve could intercept it, but say for now she leaves $|\psi\rangle$ untouched. Bob samples a bitstring b', and measures $|\psi\rangle$ in the basis specified by b' (following the same convention used by Alice).

Suppose $b' = 100111$. Give a possible state that Bob might observe with this protocol. If Bob assumes that he used the "correct" measurement bases, what bitstring a' does the state you just gave encode?

Solution: When Bob's basis matches Alice's basis, the measurement will be certain, and the corresponding bit in Bob's a' will match Alice's a. Otherwise, the result will flip with a 50/50 chance.

$$\big|\psi'\big\rangle = |+\rangle \otimes |1\rangle \otimes |0 \text{ or } 1\rangle \otimes |+ \text{ or } -\rangle \otimes |+\rangle \otimes |-\rangle \quad \rightarrow \quad a' = 01??01.$$

A specific example is $|+10 - +-\rangle$ and $a' = 011001$.

c) [1 Point] In BB84, Alice now publicly announces b and Bob publicly announces where it differs from b'. They then discard the parts of a and a' where b and b' differ.

Suppose Alice and Bob did that now. What bitstrings are they left with?

Solution: They are always left with a and a' reduced to 0101, and b and b' reduced to 1011, discarding the middle two bits.

d) [1 Point] In SARG04, for each qubit i in $|\psi\rangle$, Alice sends a classical message encoding one of the pairs $\{|0\rangle, |+\rangle\}$, $\{|0\rangle, |-\rangle\}$, $\{|1\rangle, |+\rangle\}$ or $\{|1\rangle, |-\rangle\}$ such that the state of her i-th qubit is part of that pair.

Ignore part (c). Give a possible string of pairs she could send given the choices of a, b.

Solution: Recall Alice's state is

$$|\psi\rangle = |+\rangle \otimes |1\rangle \otimes |-\rangle \otimes |0\rangle \otimes |+\rangle \otimes |-\rangle .$$

Example: $\rightarrow \{|0\rangle, |+\rangle\}, \{|1\rangle, |+\rangle\}, \{|1\rangle, |-\rangle\}, \{|0\rangle, |+\rangle\}, \{|0\rangle, |+\rangle\}, \{|1\rangle, |-\rangle\}$

e) [1 Point] Bob now analyses each pair, and sees if the a' he used to measure can be used to determine Alice's bases b.

For the a' you gave in (b) and the string you gave in (d), for which pairs is the basis (and so the correct state in each tuple) unambiguous? *Hint: if Alice sends* $\{|0\rangle, |+\rangle\}$*, what is the only way for Bob to measure* $|1\rangle$*?*

Solution: The results will depend on a student's choices in (b) and (d). Here, we continue with the examples we gave above.

Consider the first qubit. Alice tells Bob that her qubit was either $|0\rangle$ or $|+\rangle$, Bob measured in the $|+\rangle / |-\rangle$ basis, and Bob observed $|+\rangle$. Consider both cases. If Alice's qubit was $|0\rangle$, would it have been possible for Bob's measurement to show $|+\rangle$? Yes, since they are not orthogonal. If Alice's qubit was $|+\rangle$, would it have been possible for Bob to observe $|+\rangle$? Yes.

Now consider the third qubit. Alice tells Bob that her qubit was either $|1\rangle$ or $|-\rangle$, Bob measured in the $|0\rangle / |1\rangle$ basis, and Bob observed $|0\rangle$. Consider both cases. If Alice's qubit was $|1\rangle$, would it have been possible for Bob's measurement to show $|0\rangle$? No, since they are orthogonal. If Alice's qubit was $|-\rangle$, would it have been possible for Bob to observe $|0\rangle$? Yes, since they are not orthogonal.

For each qubit:

Alice's qubit is one of	Bob measured in	Bob observed	Bob's outcome is consistent with?
$\{|0\rangle, |+\rangle\}$	+/-	+	both
$\{|1\rangle, |+\rangle\}$	0/1	1	both
$\{|1\rangle, |-\rangle\}$	0/1	0	$|-\rangle$
$\{|0\rangle, |+\rangle\}$	+/-	-	$|0\rangle$
$\{|0\rangle, |+\rangle\}$	+/-	+	both
$\{|1\rangle, |-\rangle\}$	+/-	-	both

So at this point, Bob's knowledge of Alice's a looks like ??10??, and his knowledge of Alice's b is ??10??.

f) [1 point] Bob announces the positions where a' and b were unambiguous. Alice and Bob use those unambiguous bits of b as their secret key.

Given what you found in (e), what is Alice and Bob's secret string?

Solution: Results will depend on a student's choices in (b) and (d). In our example, the middle two qubits were unambiguous, so their secret secret key taken from b is 10.