C S 358H: Intro to Quantum Information Science

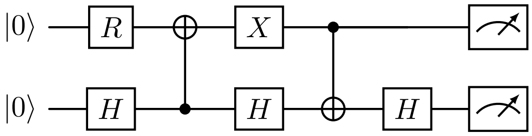
Sayam Sethi

September 2024

Contents

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:

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

Question 1.1

Question. *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. Measuring in the $|+\rangle\,/\,|-\rangle$ basis is the same as applying a H gate and then measuring in the $|0\rangle\,/\,|1\rangle$ basis. Therefore, the equivalent state before measurement in the $|0\rangle\,/\,|1\rangle$ basis is,

$$\begin{aligned} |\psi\rangle &= \frac{(|0\rangle + |1\rangle)\,|0\rangle + \sqrt{2}(|0\rangle - |1\rangle)\,|0\rangle + \sqrt{2}(|0\rangle + |1\rangle)\,|1\rangle - (|0\rangle - |1\rangle)\,|1\rangle}{\sqrt{12}} \\ &= \frac{|0\rangle\left((\sqrt{2}+1)\,|0\rangle + (\sqrt{2}-1)\,|1\rangle\right) - |1\rangle\left((\sqrt{2}-1)\,|0\rangle - (\sqrt{2}+1)\,|1\rangle\right)}{\sqrt{12}} \end{aligned} \tag{1}$$

Since the amplitudes of the the $|0\rangle$ and $|1\rangle$ states are equal, the probability of observing $|+\rangle$ on the top qubit is 50%. □

Question 1.2

Question. *If we observe $|+\rangle$ on the top qubit, then what is the state of the bottom qubit? Show your work.*

Solution. The state of the bottom qubit will be the normalised state that is tensored with the $|0\rangle$ in the state obtained in Question 1.1. Therefore, the state of the bottom qubit is $\frac{(\sqrt{2}+1)|0\rangle+(\sqrt{2}-1)|1\rangle}{\sqrt{6}}$. □

Question 1.3

Question. *What is the probability the joint outcome of the two measurements is $|+-\rangle$? Show your work.*

Solution. Since we know the probability of obtaining $|+\rangle$ state on the first qubit is 50%, it is enough to compute the probability of obtaining a $|-\rangle$ state on the residual state obtained in Question 1.2 and multiply it by $1/2$. To obtain the probability of obtaining a $|-\rangle$ state, we again apply a H gate and measure in the $|0\rangle\,/\,|1\rangle$ basis. The equivalent state is,

$$\begin{aligned}|\psi'\rangle &= \frac{\left(\sqrt{2}+1\right)(|0\rangle + |1\rangle) + \left(\sqrt{2}-1\right)(|0\rangle - |1\rangle)}{\sqrt{12}} \\ &= \sqrt{\frac{2}{3}}\,|0\rangle + \sqrt{\frac{1}{3}}\,|1\rangle\end{aligned} \tag{2}$$

Therefore, the probability of obtaining a $|-\rangle$ on the second qubit is $1/3$ and therefore, the resultant probability of getting $|+-\rangle$ is $1/6$. □

2 From Cloning To Faster-Than-Light Signaling

Question 2.1

Question. *Suppose Alice and Bob shared the entangled state*

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

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?]

Proof. Consider the following protocol:

Protocol used by Alice and Bob to communicate b

1. **Alice:** If $b = 0$, measure the qubit in the $|0\rangle\,/\,|1\rangle$ basis, else measure it in the $|+\rangle\,/\,|-\rangle$ basis.
2. **Bob:**
   (a) Use the cloning device $2n - 1$ times to obtain $2n$ copies of the qubit.
   (b) Measure the first n copies in the $|0\rangle\,/\,|1\rangle$ basis.
   (c) Measure the remaining n copies in the $|+\rangle\,/\,|-\rangle$ basis.
   (d) Output $b' = 0$ if all measurements in the $|0\rangle\,/\,|1\rangle$ basis matched, else output $b' = 1$. If all $2n$ measurements matched, output 0 or 1 with equal probability.

This protocol fails with probability $1/2^n$.

Figure 1: Faster-than-Light Communication Protocol

We now prove that the failure probability is indeed $1/2^n$. Notice that the only time the protocol fails is when all measurements match. This will happen with probability $2 \cdot 1/2^n$ (when the bit chosen by Alice is 0 and all $|+\rangle\,/\,|-\rangle$ measurement outcomes are either $|+\rangle$ or $|-\rangle$, or vice versa). There is another 1/2 chance of failure when Bob guesses the bit in this case. Therefore, the total failure probability is $1/2^n$.

Also note that if even one measurement result differs, we can deterministically identify the bit chosen by Alice. For example, if the bit chosen by Alice is 0, then it is guaranteed that all measurements in the $|0\rangle\,/\,|1\rangle$ basis will agree, however, there is an equal chance of obtaining $|+\rangle$ or $|-\rangle$ when measuring in the $|+\rangle\,/\,|-\rangle$ basis. □

3 SARG04 Quantum Key Distribution

Question 3.1

Question. *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. The state $|\psi\rangle$ will be equal to $|+\rangle \otimes |1\rangle \otimes |-\rangle \otimes |0\rangle \otimes |+\rangle \otimes |-\rangle$. □

Question 3.2

Question. *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. The state sent by Alice will *agree* in positions where b and b' agree. However, there is a 50% chance of obtaining either state for the other positions. Since b and b' only disagree at positions $2, 3$ (0-indexed), we assume that the measurement results in a 0 for both these measurements.
Therefore, the state observed by Bob will be $|+\rangle \otimes |1\rangle \otimes |0\rangle \otimes |+\rangle \otimes |+\rangle \otimes |-\rangle$ and thus a' will be 010001. □

Question 3.3

Question. *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. The bitstrings that Alice and Bob are left with are $b_{BB84} = 1011$ and $a_{BB84} = 0101$. □

Question 3.4

Question. *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. Indexing each pair from 0 to 3, a possible message that Alice can send to Bob is 021003. □

Question 3.5

Question. *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. Since Bob measures in the *correct* basis for positions $0, 1, 4, 5$, Bob will always have ambiguity for the pairs Alice sent corresponding to these positions. However, it is possible for Bob to obtain the *correct* basis for the positions where b and b' disagree, i.e., positions 2 and 3. However, for the message chosen by Alice, Bob will be unable to disambiguate since the state Bob measured is contained in the pair sent by Alice ($|0\rangle$ and $|+\rangle$ are both in the pair 0 and Alice sends the pair 0 for both the positions $2, 3$).
However, if Alice had sent 023003, then Bob will be able disambiguate the basis for position 2. The basis for position 3 will still be ambiguous. Bob will determine that $b'[2] = 1$ since Bob got $|0\rangle$ on measurement but Alice sent the pair $\{|1\rangle, |-\rangle\}$ and therefore the only possible state is the $|-\rangle$ state. □

Question 3.6

Question. *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. Since Bob was unable to disambiguate any of the positions, the secret string does not exist. However, if Alice had sent 023003, then Alice and Bob will have the secret key as 1 (the bit corresponding to the position 2). □