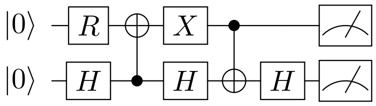
Introduction to Quantum Information Science
Homework 4

Due Wednesday, October 2 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.

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

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

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?]

3. 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 $|\psi\rangle$.

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?

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?

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.

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* $|1\rangle$*?*

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?