Quantum Computing (CS5100) : Problem Set 1

Department of Computer Science and Engineering
IIT Hyderabad

Deadline: Sept. 15, 2024 before 11:59PM

Please read the following comments before you work on the problems.

- Plagiarism leads to **F** grade and a meeting with disciplinary committee!
- Assignments after the deadline will not be accepted at any cost. So plan for your internet outages etc. beforehand. You may submit a hard copy as well.
- All the problems are easy and builds on what has been taught in the class. Try to attempt them all.

---

1. (a) Prove that there doesn't exist a 2-qubit unitary U that maps $|\phi\rangle|0\rangle \to |\phi\rangle|\phi\rangle$ for every qubit $|\phi\rangle$. **(8 marks)**

   (b) Prove that there doesn't exist a 2-qubit unitary U that maps $|0\rangle|0\rangle \to |0\rangle|0\rangle$ and $|+\rangle|0\rangle \to |+\rangle|+\rangle$. **(15 marks)**

2. Alice and Bob prepare an EPR pair, that is, two qubits in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. They each take one qubit home. Suddenly, Alice decides she wishes to convey one of 4 messages to Bob; in other words, she wants to convey a classical string $ab \in \{0,1\}^2$ to Bob. Alice does the following in the privacy of her own home: First, if $a = 1$ she applies a NOT gate to her qubit (else if $a = 0$ she does nothing here). Next, if $b = 1$, she applies a Z (phaseflip) gate, $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, to her qubit (else if $b = 0$ she does nothing here).

   (a) Write the resulting 2-qubit state for the four different cases that ab could take. **(8 marks)**

   (b) Suppose Alice sends her half of the state to Bob, who now has two qubits. Show that Bob can determine both a and b from his state. **(14 marks)**

3. Let $\theta \in [0, 2\pi)$, $U_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $|\phi\rangle = U_\theta|0\rangle$ and $|\phi^\perp\rangle = U_\theta|1\rangle$.

(a) Show that $ZX|\phi^\perp\rangle = |\phi\rangle$. Recall, X is the NOT gate. **(5 marks)**

(b) Show that an EPR-pair, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, can also be written as $\frac{1}{\sqrt{2}}(|\phi\rangle|\phi\rangle + |\phi^\perp\rangle|\phi^\perp\rangle)$. **(10 marks)**

(c) Suppose Alice and Bob start with an EPR-pair. Alice applies U_θ^{-1} to her qubit and then measures it in the standard computational basis. What (pure) state does Bob have if her outcome was 0, and what (pure) state does he have if her outcome was 1? **(8 marks)**

(d) Suppose Alice knows the number θ but Bob does not. Give a protocol that uses one EPR-pair and 1 classical bit of communication where Bob ends up with the qubit $|\phi\rangle$ (in contrast to general teleportation of an unknown qubit, which uses 1 EPR-pair and 2 bits of communication). **(10 marks)**

4. Recall the CHSH game we saw in class:

- Alice gets $x \in \{0,1\}$ and Bob gets $y \in \{0,1\}$
- Alice outputs $a \in \{0,1\}$ and Bob outputs $b \in \{0,1\}$ (recall they can't communicate)
- the success condition for the game is $a \oplus b = x \wedge y$.
- their goal is to succeed with high probability when the inputs are given uniformly at random.

Now suppose that Alice and Bob can build magic "non-local boxes" that would allow them to succeed at the CHSH game with 100% probability. That is, a *non-local box* is an imaginary device that has an input-output port at Alice's and another one at Bob's, even though they are spatially distant; furthermore, Alice can put a bit $x \in \{0,1\}$ into the box and get back a bit $a \in \{0,1\}$, Bob can put a bit $y \in \{0,1\}$ into the box and get back a bit $b \in \{0,1\}$, and these bits will always satisfy $a \oplus b = x \wedge y$. Also, inspired by entanglement, we assume that a non-local box is a *one-shot* device, that is, one box can only be used once.

(a) Assume that Alice and Bob are spatially distant, but they have access to n of these magical non-local boxes. Assume also that Alice knows n bits $x_1, \ldots, x_n \in \{0,1\}$, Bob knows n bits $y_1, \ldots, y_n \in \{0,1\}$, and they wish to compute the "inner product mod 2" function of their bits,

$$\mathsf{IP}_2(x_1, \ldots x_n, y_1, \ldots, y_n) = x_1 \cdot y_1 + \cdots + x_n \cdot y_n \pmod 2.$$

Show that by using the non-local boxes, and then allowing *one* classical bit of communication from Alice to Bob, Bob can learn the value $\mathsf{IP}_2(x_1, \ldots, x_n, y_1, \ldots, y_n)$. **(10 marks)**

(b) Show that every Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ can also be computed by a polynomial over $\mathbb{F}_2$. Recall $\mathbb{F}_2$ is the field with two elements $\{0,1\}$ with addition and multiplication being performed (mod 2). **(8 marks)**

(c) Let $f(x_1, \ldots, x_n, y_1, \ldots, y_n)\colon \{0,1\}^{2n} \to \{0,1\}$ be a Boolean function over $2n$ variables. Now suppose Alice knows $x_1, \ldots, x_n$, Bob knows $y_1, \ldots, y_n$, and they wish to compute f applied to their two inputs: $f(x_1, \ldots, x_n, y_1, \ldots, y_n)$. Show that by using as many non-local boxes as they want, and then using *two* classical bits of communication, both of them can learn the value $f(x_1, \ldots, x_n, y_1, \ldots, y_n)$. (Quantify the number of non-local boxes used in your protocol.) **(14 marks)**

5. We had seen one-qubit teleportation in class. In fact, entangled states can also be teleported. Suppose Alice has prepared a two-qubit entangled state $|\phi\rangle := \alpha|00\rangle + \beta|11\rangle$. She wishes to teleport one half of $|\phi\rangle$ to Bob and another half to Charlie, so that in the end Bob and Charlie will hold halves of the entangled state $|\phi\rangle$ despite never physically interacting. Give a protocol to achieve this. **(10 marks)**

6. Alice and Bob prepare the following 2-qubit state:

$$|\psi\rangle = H \otimes H \left(\frac{1}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}}|01\rangle + \frac{1}{\sqrt{3}}|10\rangle \right).$$

Alice now takes control of the first qubit and Bob takes control of the second qubit.

Each of Alice and Bob now flips a coin and does the following: If they flip Tails, they directly measure their qubit; if they flip Heads, they first apply a Hadamard to their qubit and then they measure.

(a) Prove the following statements: **(10 marks)**
If Alice flips T and Bob flips T, it's *possible* A & B will measure 1, 1 respectively.
If Alice flips T and Bob flips H, it's *impossible* A & B will measure 1, 0 respectively.
If Alice flips H and Bob flips T, it's *impossible* A & B will measure 0, 1 respectively.
If Alice flips H and Bob flips H, it's *impossible* A & B will measure 1, 1 respectively.

The next two questions carry zero marks and needn't be turned in. But it would be good if you spend some time thinking about them.

(b) Lucien says the following: "Let's consider the situation before any coin flips or measurement happens, and try to decide what outcomes the qubits are capable of producing when measured.

- Consider the first statement in (a). Since it's possible that Alice will flip Tails and Bob will flip Tails, we conclude that prior to any coin flips/measuring, it's *possible* for Alice's qubit to register 1 after being directly measured.
- Now consider the second statement in (a). Since Alice's qubit is capable of generating a 1 when she flips Tails, it must be *impossible* for Bob's qubit to produce a 0 when he flips Heads, and consequently Hadamards-then-measures.
- Let's repeat the previous two bullet points, interchanging 'Alice' and 'Bob'. By the first statement in (a), we conclude that prior to any coin flips/measuring, it's *possible* for Bob's qubit to register a 1 when directly measured. Hence

by the third statement in (a), since Bob's qubit is capable of generating a 1 when directly measured, we conclude that it must be *impossible* for Alice's qubit to produce a 0 when she Hadamards-then-measures.

- We've concluded that in case of flipping Heads, for both Alice and Bob it's impossible for them to register a 0 when they Hadamard-and-measure; i.e., they must both register a 1 in this case. But this contradicts the fourth statement in (a)."

Critique the four bullet points above. Do you agree or disagree with Lucien?

(c) Read Scott Aaronson's blog post from Sept. 25, 2018, *It's hard to think when someone Hadamards your brain*. Critique his argument. Do you agree or disagree with him?