Week 5 work: Sept. 4 — Oct. 11
9-hour week
Obligatory problems are marked with [**]

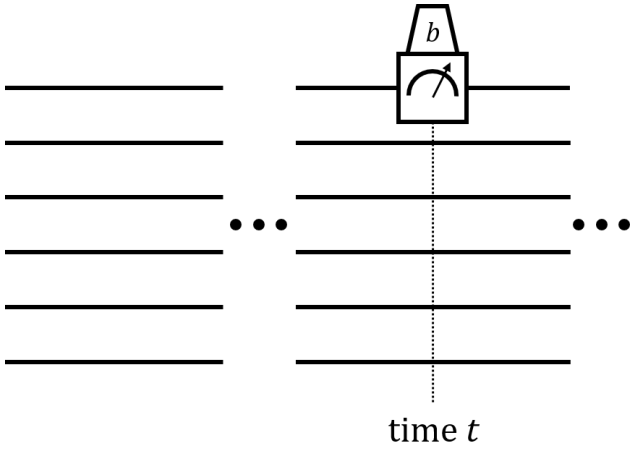
---

1. **[Ground-to-satellite quantum teleportation?]** [$**$] Read the 2017 Nature paper by Jian-Wei Pan's group on the experiment to do quantum teleportation between Earth and a satellite. (A couple of Wikipedia articles I found helpful during the reading: Coincidence counting, Spontaneous parametric down-conversion (SPDC).) What do you think? In my opinion, there were two major aspects of the full quantum teleportation experiment that were missing. Write a two-paragraph critique.

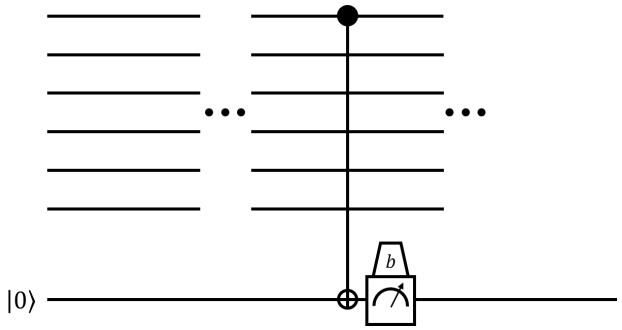
   (One piece of technical knowledge you will find helpful: Let $|\psi\rangle$ and $|\widetilde{\psi}\rangle$ be two quantum states, where we think of $|\psi\rangle$ as the ideal "ground truth" and $|\widetilde{\psi}\rangle$ as some potentially noisy/inaccurate version of $|\psi\rangle$. The *fidelity* between $|\widetilde{\psi}\rangle$ and $|\psi\rangle$ is defined to be $|\langle\psi|\widetilde{\psi}\rangle|^2$; in other words, the probability you'd get $|\psi\rangle$ if you measured $|\widetilde{\psi}\rangle$ in a orthonormal basis where one of the basis vectors was $|\psi\rangle$.)

2. **[Principle of Deferred Measurement.]** The point of this problem is to show that if one has a quantum circuit with (partial) measurement gates in the middle, one can (without much loss in efficiency) replace it with an equivalent quantum in which all the measurement gates are at the end. This is nice, because a very useful simplifying assumption in quantum computation is that measurement gates only occur at the end of the computation.

   So suppose we have some n-qubit quantum circuit, and we look at the first intermediate measurement gate that is applied; say (without loss of generality) it is applied to the 1st qubit, at time step t. Let $|\psi\rangle$ denote the quantum state just prior to time t. Now when the measurement gate is applied, two things happen: First, one classical bit of information — call it b — appears on the measurement gate's readout. Second, the state collapses according to the usual rules.



   (a) [**] Suppose we do the following: First, we introduce a new $(n+1)$st qubit, initialized in the state $|0\rangle$. Second, we replace the measurement gate on qubit #1 at time t with a CNOT gate whose control qubit is #1 and whose target qubit is $\#(n+1)$. Finally, we immediately apply a measurement gate to the $(n+1)$st qubit, and treat its readout as "b". Assume we then henceforth ignore the (collapsed) $(n+1)$st qubit. Show that this gives an exact simulation of the original circuit's operation. (Hint: you may want to somehow write $|\psi\rangle = \alpha\,|0\rangle \otimes |\psi_0\rangle + \beta\,|1\rangle \otimes |\psi_1\rangle$.)



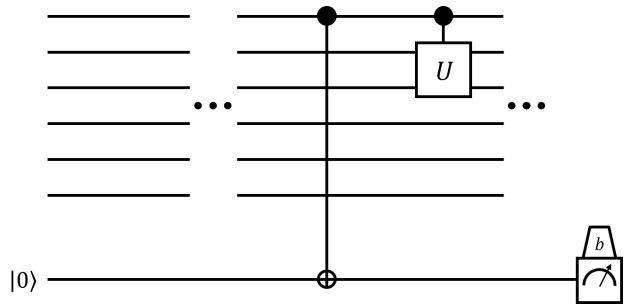
   Remark: As we saw in class, operations that are applied to disjoint sets of qubits commute (this was the $(U \otimes I)\cdot(I \otimes V) = (I \otimes V)\cdot(U \otimes I) = U \otimes V$ stuff in the case of applying unitary gates, and similarly for the commuting of partial measurements). Thus, if we're

never going to do anything with that $(n+1)$st qubit again, we can imagine that instead of measuring it immediately (just after time t), we instead delay its measurement to the very end of the computation. In this way, we've effectively deferred the first intermediate measurement of the quantum circuit to the end. By repeating this for all intermediate measurement gates, we can always move all measurement gates to the end (at the cost of adding one extra qubit and CNOT per deferral).

(b) [$**$] Let's look back at the original circuit and see "what was done" with the first qubit after it was measured. In some cases, that measurement gate was there because we genuinely wanted to know the 1 bit of classical information, b. In other cases, we don't care about b's value per se; rather, we just want to do different subsequent quantum operations to the other qubits, depending on whether $b = 0$ or $b = 1$. (The Quantum Teleportation scenario is a bit like this.) In other words, the rest of the quantum circuit might include something like

$$\textit{do } U \in \mathbb{C}^{4\times 4} \textit{ to qubits } 2 \textit{ and } 3 \textit{ if } b = 1\textit{, else do nothing.}$$

Given that the post-measurement qubit's state is precisely $|b\rangle$, one can instead think of the above conditional-instruction as a "controlled-U gate applied to qubits 1 (control), 2 and 3 (targets)", rather than as some interactive intervention wherein U is applied or not applied, depending on the readout b.



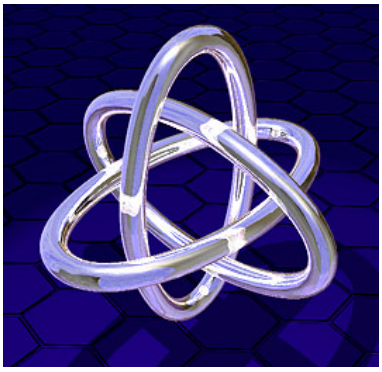
So suppose we're in this case, where we don't really care to know b, we're simply doing some "controlled-U" quantum gates based off the outcome. And suppose we apply the Deferred Measurement trick from part (a). Since we don't actually care to know the classical bit b, do we really have to do the measurement of the $(n+1)$st qubit at the end? (I.e., will the circuit work just as well if we ignore that qubit?) If yes, give an example illustrating the necessity. If not, answer this: do we really have to do the CNOT, either?

3. **[Borromean entanglement vs. non-Borromean entanglement.]**

(a) The "GHZ state" is $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$. Prove that this state is entangled (i.e., it is not *unentangled*).

(b) Suppose Alice, Bob, and Charlie each hold one qubit of a GHZ state. Suppose Charlie measures her bit. Prove that with 100% probability, Alice and Bob's qubits become unentangled.

Remarks: Had Charlie first taken her qubit to Jupiter and Alice and Bob never really hear from her again, then they would have no way of distinguishing whether or not Charlie actually *does* measure her qubit. Thus the "mixed" state that Alice and Bob's two qubits are in is said to be "unentangled" either way. By symmetry of the GHZ state $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$, we therefore have a funny situation: Any two of the three qubits are not entangled, but all three of them *are* entangled.



(c) The 3-qubit "W state" is defined to be $\frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle$. Prove that this state is entangled, Furthermore, prove that if Charlie measures one of the three qubits, there is a positive probability that the remaining two qubits *are* still entangled.

4. **[The best counterfeiting attack on Wiesner's quantum money scheme.]** [∗∗] Solve Problem 4(b) on the homework from Aaronson's 2017 course at UT Austin.

   Remarks: we saw the 5/8 procedure for part (a) in class. Also, by "discard (perform partial trace over)", you can read "measure the first qubit". Finally, by "higher than what was achieved in part a", you should specifically achieve probability 3/4.

5. **[Entanglement swapping.]** [$**$] After demonstrating one-qubit teleportation in class, I stated the following: Entangled states can also be teleported, and in fact, if Alice & Bob share an EPR pair, and Alice & Charlie share an EPR pair, then Alice can prepare a *third* EPR pair, teleport one half to Bob, teleport one half to Charlie, and in the end Bob and Charlie will hold halves of an entangled EPR pair despite never physically interacting. I didn't actually prove that this works though. Do so.

6. **[BB84 quantum key distribution.]** Alice is at spy headquarters and Bob is an agent in the field. Alice wants to convey a "one-time pad" to Bob; i.e., she wants to secretly convey a purely random string $k \in \{0,1\}^n$. They perform the following protocol.

   - Alice prepares a random "Wiesner money state" $|\psi\rangle$ of $4n$ qubits; i.e., $4n$ unentangled qubits in which each $|\psi_i\rangle$ is randomly chosen to be either $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$.
   - Alice sends $|\psi\rangle$ out to Bob along some fiber optic channel.
   - Bob receives some $4n$-qubit state $|\phi\rangle$. (Ideally, $|\phi\rangle = |\psi\rangle$, but....) Bob then sort of tries to perform the "classical communication quantum money verification" routine described in class, except he doesn't wait for Alice to send him the bases to measure in. Rather, as each qubit $|\phi_i\rangle$ flies in off the fiber optic channel, Bob randomly chooses $b_i \in \{0,1\}$. Then if $b_i = 0$ he measures $|\phi_i\rangle$ in the standard basis, and if $b_i = 1$ he measures $|\phi_i\rangle$ in the sign basis.[1]
   - Bob texts the string $b \in \{0,1\}^{4n}$ to Alice.
   - Alice texts the string $a \in \{0,1\}^{4n}$ to Bob, where $a_i = 0$ if $|\psi_i\rangle$ was created in the standard basis, $a_i = 1$ if $|\psi_i\rangle$ was created in the sign basis.
   - At this point, Alice and Bob (and the rest of the world) know some subset of coordinates $S \subseteq \{1, 2, \ldots, 4n\}$ for which $a_i = b_i$; i.e., for which Bob "guessed the right basis". With high probability, $|S| \approx 2n$.
   - At this point, if nothing strange has happened, the measurement outcomes r_i Bob got on the S-qubits should be the same as the original prepared states q_i that Alice made. Further, since we've conditioned on whether these outcomes are $0/1$ outcomes or $\pm$ outcomes, these common values $(r_i = q_i : i \in S)$ effectively amount to a shared random string of length $\approx 2n$.
   - Out of paranoia, Alice and Bob further do the following. One of them (say, Bob) randomly partitions S into two sets C and K (i.e., each coordinate in S is randomly assigned to either C or K; hence $|C|, |K| \approx n$ with high probability). Then Bob texts both C and the outcomes $(r_i : i \in C)$ to Alice.
   - Finally, if Alice finds that any of these $(r_i : i \in C)$ do not match her q_i, she texts "ABANDON PROTOCOL" to Bob. Otherwise, Alice treats her info $(q_i : i \in K)$ as the (hopefully secret) one-time pad "k" and Bob treats his info $(r_i : i \in K)$ as the (hopefully matching) one-time pad. Note that this info is (with high probability) about n bits long.

   Of course, if the fiber optic channel and the text messages are completely secure then this protocol succesffully produces a shared random one-time pad (and in fact the final "paranoia" step is not necessary). But if we're assuming completely secure text message transmission, then we could have just had Alice directly text a one-time pad in the first place. (Or just directly text the secret message!) So what we assume is that there is a malicious eavesdropper Eve, who can potentially eavesdrop on all of the text messages, and who can potentially tap the fiber optic channel. Of course, Eve has to be careful about tapping the quantum channel. If she wants, she can capture qubits off it, measure them, and then send replacement qubits down the channel. We will assume she can do this without Alice or Bob being able to directly notice at all. But the point of this whole "BB84 Quantum Key Distribution" protocol is to help Alice and Bob detect and evade this.

[1] Remark: The fact that Bob can immediately measure each qubit here, and does have to "store" the qubits for any amount of time, is precisely the property that makes quantum key distribution actually real-life practical.

(a) Assume that Eve does not touch the quantum channel at all, but merely eavesdrops on all the text messages. Write a short (informal) justification for why this in no way helps her learn any bits of the final secret one-time pad.

(b) Explain how if perfect qubit cloning *were* possible, Eve could successfully learn the final one-time pad without Alice and Bob being able to detect her presence.

(c) Explain some things Eve can do (in our actual No-Cloning world) that at least somewhat mess up Alice and Bob. E.g., Eve should have a reasonably large probability of causing the following situation: Alice and Bob do not notice anything strange, yet their "matching strings k" actually disagree on a couple of bits.

(d) Nevertheless, write an informal explanation for why, no matter what Eve does, there is only an exponentially small probability that Alice and Bob will end up: (i) not detecting any tampering; and, (ii) either disagreeing on many bits of k, or having Eve know many bits of k.

Of course, I have not given you a precise statement here, so your explanations will necessarily be informal.

7. [**剩余定理。**]

(a) [∗∗] Recall Problem 5(a) on Weekly Work #3, in which you needed to show that if P and Q are positive integers, then there are some other integers C and D such that

$$C \cdot P + D \cdot Q = \mathrm{GCD}(P, Q).$$

Using this fact, show that if P and Q are distinct prime numbers, then the following system of equations has an integer solution:

$$X \equiv 1 \ (\mathrm{mod})\ P$$
$$X \equiv 0 \ (\mathrm{mod})\ Q,$$

as does the system

$$Y \equiv 0 \ (\mathrm{mod})\ P$$
$$Y \equiv 1 \ (\mathrm{mod})\ Q.$$

(b) [∗∗] Continuing to assume henceforth that P and Q are distinct primes, deduce that for any $0 \leq S < P$ and $0 \leq T < Q$ there is an integer solution $0 \leq Z < PQ$ to the system

$$Z \equiv S(\mathrm{mod})\ P$$
$$Z \equiv T(\mathrm{mod})\ Q.$$

(c) [∗∗] Show that the solution $0 \leq Z < PQ$ to the above system is unique.

(d) Conclude that when we think of the number system "integers modulo PQ, together with the operations plus, minus, and times", we can equivalently think of "pairs of integers (S, T) where S is an integer modulo P and T is an integer modulo Q (and the plus, minus, and times operations act component-wise on the pair)".