PHYSICS 150

Homework 7

Due Thursday December 9, 2021 by midnight.

You must explain your work.

The FINAL EXAM will be in class on Tuesday December 7, 12:00-3:00 pm.

The final, like the midterm, will be **CLOSED BOOK** but you can use one sheet of notes that you have prepared (using both sides is OK).

To prepare for the final, I suggest that, in addition to going over the lecture material, you review the typed solutions to the homework questions available on the Canvas website. I will also put on that site last year's final and solutions. Note too that Dominic will hold his regular office hour 10:00–11:00 on Monday Dec. 6 (the day before the exam) and **I will give an extra office hour on the same day from 2:00 to 3:00 pm.** (The Zoom link for my extra office hour on Monday will be posted separately).

In this assignment there are questions on two topics: the Grover algorithm (Qu. 1–3) and quantum protocols involving photons (Qu. 4–5) (Quantum Key Distribution and Teleportation).

The class material on the Grover algorithm will be covered, at least partially, in the lecture on Tuesday Nov. 30, and could potentially be set on the final exam. To give you every possible opportunity to prepare this topic, I will **publish the solutions on the Grover questions right away**. This means that **these questions will be not graded**, but you are strongly recommended to do them, preferably without looking at the solutions first. You do not need to submit these questions.

The material related to Quantum Key Distribution and Teleportation (Questions 4 and 5) will only be be covered in the last lecture on Thursday December 2 which is too close to the final exam for me to include these topics in the final. Consequently, the solutions for these questions will only posted after the deadline for submission and **these questions will be graded and count for credit**.

1. [**no need to submit**]
   Consider the Grover algorithm in which you have to find one marked state out of $N = 4$ states. Show that the algorithm succeeds with probability 1 after 1 iteration.

2. [**no need to submit**]
   You have to find one marked state out of $N = 2$ states. Classically, picking one state at random has a probability of $1/2$ to succeed. Show that the Grover algorithm does not improve these odds.

3. [**no need to submit**]
   You are given that there are M marked states out of N. Redo the derivation of the Grover algorithm done in class and in the handout to show that one can find one of these marked states with high probability after $(\pi/4)\sqrt{N/M}$ applications of the Grover iteration. (Assume that N is large.)

4. **BB84 Quantum Key Distribution**
   Consider the BB84 Quantum Key Distribution (QKD) protocol discussed in class. **Assume that Eve intercepts every qubit (photon)** that Alice sends, and then transmits it to Bob. Like Alice and Bob, Eve chooses one the bases (the $\mathbb{1}$ or the H basis) at random. Alice and Bob compare, over a public channel which can be intercepted by Eve, which qubits they used the same basis for (Alice for sending and Bob for measuring.) The values of these qubits (0 or 1) (which Alice and Bob agree on if Eve did not eavesdrop) form the shared key.

   (a) For what fraction of the shared key qubits would Alice and Bob get different results for the qubit due to Eve's interception. (If Eve had not intercepted the qubits, then Alice and Bob would agree for all qubits in the shared key.)

   (b) Supposing that the shared key has 10 qubits, what is the probability that all of Alice's and Bob's qubits would agree (in which case Eve's eavesdropping would not be detected?

   (c) What is the probability that all qubits would agree if the shared key has 100 qubits?

5. **Teleportation**
   Suppose that Alice has a qubit in a state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1}$$

   The values of α and β are unknown to her and can not be determined as discussed in class. The no-cloning theorem means that we can't do repeated measurements on copies of this state. This qubit may be the result of a (possibly complicated) quantum computation which Alice would like to send on to Bob to continue the computation. Bob is far away and Alice can not physically transport the qubit to Bob but wants to send the state.

   Now Alice and Bob:

   - share an entangled qubit

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(\,|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b\,\right), \tag{2}$$

     where a stands for Alice's qubit and b stands for Bob's, and
   - can communicate over a classical channel (e.g. a phone).

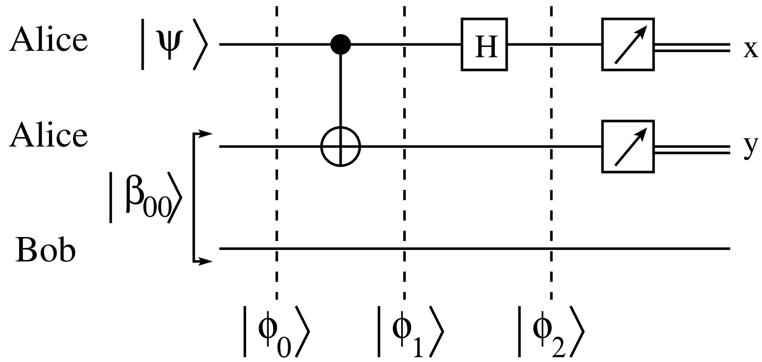
   Hence, together they have a 3-qubit state,

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}\left(\,\alpha|0\rangle_a + \beta|1\rangle_a\,\right)\otimes\left(\,|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b\,\right) \tag{3}$$

$$= \frac{1}{\sqrt{2}}\left(\,\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\,\right), \tag{4}$$

   where the leftmost two qubits refer to Alice and the rightmost qubit to Bob.

   Alice now applies a Bell measurement (discussed in class) to the two qubits in her possession, see the circuit below.



(a) Determine the states $|\phi_1\rangle$ and $|\phi_2\rangle$ shown in the figure.

(b) Alice then measures the two qubits in her possession, obtaining results x and y as shown. She then calls up Bob and tells him the result of her measurements.
Explain what Bob needs to do, depending on the results of Alice's measurements, for his qubit to be in state

$$|\psi\rangle = \alpha|0\rangle_b + \beta|1\rangle_b, \tag{5}$$

i.e. the state that was originally in Alice's possession.

Note:

- The state, but not the physical qubit, has been transported. This is called *teleportation*.
- This procedure doesn't violate relativity (information can not be transmitted faster than the speed of light) since classical communication between Alice and Bob is required.
- It does not violate the no-cloning theorem because, at the end, Alice doesn't have her original state $|\psi\rangle$, only two classical bits x and y. There is never more than one copy of $|\psi\rangle$ in existence.

Final Comment:
There are claims that teleportation has been verified experimentally which I will now discuss briefly. One would like to show the following:

- Alice stores state $|\psi\rangle$.
- The state $|\psi\rangle$ is transported to Bob who is far away.
- Bob stores state $|\psi\rangle$.

To transport qubits over a long distance one needs photons. One can teleport photons over a large distance while retaining their polarization, but at present one can not store them in a way which preserves their polarization. One can store other types of qubits, e.g. trapped ions, but can't entangle them over large distances, so they can be teleported only locally. Hence, in my view, a complete demonstration of teleportation, incorporating all three bullet points above, has not yet been achieved.