Assignment 4
Due date: 11:59pm, October 8, 2020

1. **Teleporting entanglement? [10 points]** Recall the teleportation protocol that was covered in class. Alice and Bob start with entanglement $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ (between them) and then Alice receives an arbitrary one-qubit state $|\psi\rangle$. Alice performs a unitary transformation and then a measurement on the two qubits in her possession and then sends the resulting two classical bits to Bob, who can then reconstruct $|\psi\rangle$.

   Now, suppose that, instead of having Alice receive $|\psi\rangle$, she receives the second qubit of the two-qubit state $|\Phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, where a far away third party, Carol, holds on to the first qubit of $|\Phi\rangle$. What happens if Alice follows the teleportation protocol with Bob to teleport her qubit to Bob? Is the end result that Carol and Bob share the two-qubit state $|\Phi\rangle$,with Carol in possession of the first qubit and Bob in possession of the second qubit?

   Either prove that this is so for all 2-qubit states $|\Phi\rangle = \alpha_{00}|00\rangle+\alpha_{01}|01\rangle+\alpha_{10}|10\rangle+\alpha_{11}|11\rangle$, or give an example of a state $|\Phi\rangle$ where this does not occur.

2. **A simple collision-finding problem [10 points].** Call $f : \{0,1\}^2 \to \{0,1\}$ a *two-to-one function* if there are exactly two $a \in \{0,1\}^2$ such that $f(a) = 0$ and exactly two $a \in \{0,1\}^2$ such that $f(a) = 1$. Consider the problem where one is given such a function as a black-box and the goal is to find a *collision*, which is a pair $a, b \in \{0,1\}^2$ such that $a \neq b$ and $f(a) = f(b)$.

   (a) [2 points] How many queries to f does a *classical* algorithm require to find a collision? The algorithm must always succeed (the error probability for any run should be 0).

   (b) [8 points] Show how to solve this problem by a *quantum* algorithm that makes one single query to f. The algorithm must always succeed (the error probability for any run should be 0).

3. **A variant of Simon's problem [10 points].** Call $f : \{0,1\}^n \to \{0,1\}^n$ a *four-to-one* function if, for every value that the function attains, there are exactly four preimages. In other words, there are distinct $a, b, c, d \in \{0,1\}^n$ such that $f(a) = f(b) = f(c) = f(d)$. Call a set of four points $\{a, b, c, d\}$ that f maps to the same value a *colliding quartet*. A four-to-one function has the *special Simon property* if there exists $r, s \in \{0,1\}^n$ such that, every colliding quartet is of the form $\{a, a \oplus r, a \oplus s, a \oplus r \oplus s\}$, for some $a \in \{0,1\}^n$.

   Consider the problem where you are provided with a black-box computing a four-to-one function f with the special Simon property, and your goal is to determine the associated strings r, s, and $r \oplus s$ (in any order).

   (a) [1 point] Show that if you find any three colliding points a, b, c then r, s, and $r \oplus s$ can be deduced from that.

CONTINUED ON THE NEXT PAGE

(b) [1 point] Give a quantum circuit that makes one query to f and produces the state

$$\frac{1}{\sqrt{2^n}} \sum_{a \in \{0,1\}^n} |a\rangle |f(a)\rangle. \tag{1}$$

(c) [8 points] For the state in Eq. (1), suppose that the last n qubits are measured (in the computational basis), and then a Hadamard tranform is applied to each of the first n qubits, and then those qubits are measured (in the computational basis). Explain what the outcome is, where your answer should be supported by full calculations.

From the answer to part (c), the quantum algorithm can be completed; however, you are not asked to explain that.