1. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a bijection on the n-bit strings. We showed in class that if there is an efficient classical circuit, say of size m (where size is the total number of gates in the circuit), for computing $f(x)$ on input x, then there is an efficient reversible circuit (of size $O(m)$) that outputs $x \cdot f(x) \cdot 0^k$ on input $x \cdot 0^{n+k}$, where $k = O(m)$.

   Now suppose that you are also given an efficient classical circuit for computing f^{-1} (of size m'). Show that there is an efficient reversible circuit that outputs $f(x) \cdot 0^l$ on input $x \cdot 0^l$. What is the size of your circuit and l as a function of m and m'?

2. Consider the state $\left|\psi\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)$. What is the state that results from applying the 2-qubit Hadamard transform to $\left|\psi\right\rangle$?

   Repeat for the state $\left|\phi\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle)$.

3. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a 4-to-1 function with the following structure: there are n-bit strings $a, b \in \{0,1\}^n : f(x) = f(x+a) = f(x+b) = f(x+a+b)$ for every x.

   (a) Suppose you compute the superposition $\sum_{x \in \{0,1\}^n} 2^{-n/2} \left|x\right\rangle \left|f(x)\right\rangle$ and then measure the 2nd register as in Simon's algorithm. What is the resulting state of the first register?

   (b) What is the result of applying the Hadamard transform to the first register?

   (c) (Extra Credit) Can you convert this into a quantum algorithm for finding a and b?

4. You are given one of two quantum states of a single qubit: either $\left|\phi\right\rangle = \left|0\right\rangle$ or $\left|\psi\right\rangle = \cos\varepsilon\left|0\right\rangle + \sin\varepsilon\left|1\right\rangle$. In this question we will investigate the maximum probability of distinguishing the two states. Assume that $\varepsilon > 0$ is small, and you are presented either $\left|\phi\right\rangle$ or $\left|\psi\right\rangle$ with 50% probability each.

   (a) Suppose you measure in the computational/bit basis, and guess $\left|\phi\right\rangle$ if the outcome is 0, and $\left|\psi\right\rangle$ if the outcome is 1. What is your chance of correctly guessing the state?

   (b) Now you measure in the Hadamard/sign basis, and guess $\left|\phi\right\rangle$ if the outcome is $-$, and $\left|\psi\right\rangle$ if the outcome is $+$. What is your chance of correctly guessing the state?

   It turns out that the second measurement is essentially the optimal measurement for distinguishing $\left|psi\right\rangle$ from $\left|phi\right\rangle$. Can you see that this result is not specific to single qubit states, but also applies to quantum states $\left|\phi\right\rangle$ and $\left|\psi\right\rangle$ on n qubits?