1. Prove the principle of deferred measurement: consider the quantum state $|\phi\rangle$ of $m+n$ qubits. Let $U = I \otimes V$ be a unitary operator that acts as the identity on the first m qubits. Let $\mathcal{D}$ be the distribution that results from measuring the last n qubits of $U|\phi\rangle$. Prove that measuring the first m qubits, followed applying V to the last n qubits and then measuring them results in the same probability distribution $\mathcal{D}$.

2. Let $f : \{0,1\}^n \to \{0,1\}^m$ be a polynomial time computable function. Replacing each gate of a polynomial size classical circuit for f with Fredkin gates yields a quantum circuit on $n+m+k$ qubits realizing the unitary transformation U, which on input $|x\rangle \otimes |0^m\rangle \otimes 0^k$ outputs $|x\rangle \otimes |f(x)\rangle \otimes |j(x)\rangle$ (where $j(x)$ are the contents of scratch space). Show how to convert this quantum circuit to an efficient circuit on $n+m+k'$ qubits which on input $|x\rangle \otimes |0^m\rangle \otimes 0^{k'}$ outputs $|x\rangle \otimes |f(x)\rangle \otimes |0^{k'}\rangle$.

3. Suppose you are given a $4-1$ function $f : \{0,1\}^n \to \{0,1\}^n$, such that there exist $a \neq b$, $a, b \neq 0$ such that $f(x) = f(x+a) = f(x+b) = f(x+a+b)$. Give an efficient quantum algorithm to compute a, b.