Homework 2
Due 2005/12/15

Oded Regev & Amnon Ta-Shma
Dept. of Computer Science
Tel Aviv University

1. Show how to encode two classical bits into one qubit such that any one bit can be recovered correctly with probability greater than 85%.

2. We have seen in class that Toffoli gates are universal for classical reversible computation. Prove that no set of two-bit and one-bit gates is universal for classical reversible computation.

3. Let $f : \{0,1\}^n \to \{0,1\}^m$, $g : \{0,1\}^m \to \{0,1\}^n$ be such that g is a left-inverse of f (i.e., $g(f(x)) = x$ for all $x \in \{0,1\}^n$). Assume that both functions can be computed by a polynomial size classical circuit. Show that there exists a polynomial size classical reversible circuit (and hence also quantum circuit) that maps $|x, 0\rangle$ to $|f(x), 0\rangle$. Would you expect this to be possible without the assumption that g has a polynomial size circuit?

4. Describe a quantum algorithm that solves the following problem. Given a function $f : \mathbb{Z}_2^n \to \{0,1\}^m$ that satisfies $f(x) = f(y) \Leftrightarrow x - y \in H$ for some subgroup H of $\mathbb{Z}_2^n$, find H.

5. For any function $f : \{0,1\}^n \to \{0,1\}$ we define U_f as the unitary transformation mapping $|x, y\rangle$ to $|x, y + f(x)\rangle$ for each $x \in \{0,1\}^n$ and $y \in \{0,1\}$. Also define S_f as the unitary transformation mapping $|x\rangle$ to $(-1)^{f(x)}|x\rangle$ for each $x \in \{0,1\}^n$. Show how to obtain S_f from U_f (using an auxiliary qubit). Can you obtain U_f from S_f?

6. (a) Let $|u\rangle, |v\rangle$ be two states on n qubits each. Consider the circuit below, which uses a controlled swap gate. Find the probability of measuring $|0\rangle$ as a function of $|\langle u|v\rangle|$. What does this quantity correspond to?

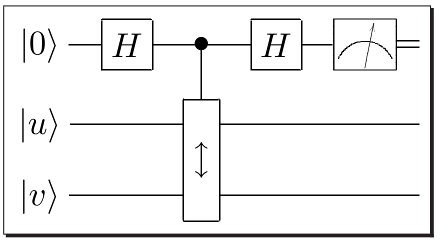

Figure 1: The swap test

   (b) Now assume there exists a quantum circuit U that transforms $|0\rangle$ to $|u\rangle$ and a quantum circuit V that transforms $|0\rangle$ to $|v\rangle$. Show how to generate the state $(|0\rangle|u\rangle + |1\rangle|v\rangle)/\sqrt{2}$ using U and V. Then, assume we apply H on the first qubit and measure it. Find the probability of measuring $|0\rangle$ as a function of $|\langle u|v\rangle|$.

7. Here we develop parts of the very useful *phase estimation* technique, due to Kitaev. Let U be a unitary transformation on n qubits and let $|v\rangle$ be an eigenvector of U with eigenvalue λ.

   (a) Show that $|\lambda| = 1$, i.e., there exists some $\theta \in [0, 2\pi)$ such that $\lambda = e^{i\theta}$.

   (b) Based on the circuit shown in Figure 2, describe how to estimate θ to within some additive error ε (with confidence, say, 90%). You can assume that you have a way to generate the state $|v\rangle$. How many operations are needed (roughly) as a function of ε?

(c) Show that you can do the same even if you are given only one copy of $|v\rangle$ (and you are unable to generate more yourself).

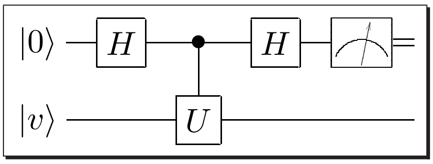

Figure 2: Phase estimation

8. (a) For $b \in \{0, 1\}$ define $|\psi_b\rangle$ as the two-qubit state $\frac{1}{\sqrt{2}}(|00\rangle + (-1)^b|11\rangle)$. Alice and Bob share the state $|\psi_b\rangle$ for some unknown b. Their goal is to determine b. Unfortunately, they are unable to communicate with each other. Convince yourself that Alice (or Bob) cannot determine b alone (no rigorous proof of this is required). Now, assume each of them is allowed to send one classical envelope to a common friend Charlie. Find a protocol that allows Charlie to determine b from the two envelopes he receives.

   (b) For each $k, l \in \{0, 1\}^{2n}$, $k \neq l$, $b \in \{0, 1\}$, define $|\psi_{k,l,b}\rangle$ as the state $\frac{1}{\sqrt{2}}(|k\rangle + (-1)^b|l\rangle)$ on $2n$ qubits. Alice and Bob share the state $|\psi_{k,l,b}\rangle$ for some unknown k, l, b (i.e., each has n qubits). Each of them can send one classical envelope to Charlie, who happens to know k and l but not b. Upon receiving the two envelopes, Charlie is asked to determine the bit b. Find a protocol that allows them to achieve this goal.