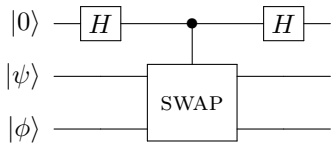
Due: March 8th, 2018
Date: February 26, 2018

Assignment 3

Please submit it electronically to ELMS. This assignment is 7% in your total points. For the simplicity of the grading, the total points for the assignment is 70.

Problem 1. *Swap test.*

1. *(Points :5)* Let $|\psi\rangle$ and $|\phi\rangle$ be arbitrary single-qubit states (not necessarily computational basis states), and let SWAP denote the 2-qubit gate that swaps its input qubits (i.e., $\text{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$ for any $x, y \in \{0,1\}$). Compute the output of the following quantum circuit:



2. *(Points :5)* Suppose the top qubit in the above circuit is measured in the computational basis. What is the probability that the measurement result is 0?

3. *(Points :3)* If the result of measuring the top qubit in the computational basis is 0, what is the (normalized) post-measurement state of the remaining two qubits?

4. *(Points :2)* How do the results of the previous parts change if $|\psi\rangle$ and $|\phi\rangle$ are n-qubit states, and SWAP denotes the $2n$-qubit gate that swaps the first n qubits with the last n qubits?

Problem 2. *One-out-of-four search.* Let $f\colon \{0,1\}^2 \to \{0,1\}$ be a black-box function taking the value 1 on exactly one input. The goal of the one-out-of-four search problem is to find the unique $(x_1, x_2) \in \{0,1\}^2$ such that $f(x_1, x_2) = 1$.

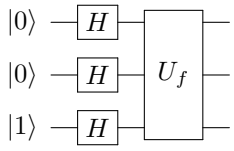
1. *(Points :2)* Write the truth tables of the four possible functions f.

2. *(Points :3)* How many classical queries are needed to solve one-out-of-four search?

3. *(Points :7)* Suppose f is given as a quantum black box U_f acting as

$$|x_1, x_2, y\rangle \overset{U_f}{\mapsto} |x_1, x_2, y \oplus f(x_1, x_2)\rangle.$$

Determine the output of the following quantum circuit for each of the possible black-box functions f:



4. *(Points :3)* Show that the four possible outputs obtained in the previous part are pairwise orthogonal. What can you conclude about the quantum query complexity of one-out-of-four search?

Problem 3. *The Bernstein-Vazirani problem.*

1. *(Points :3)* Suppose $f : \{0,1\}^n \to \{0,1\}$ is a function of the form

$$f(\underline{x}) = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n \bmod 2$$

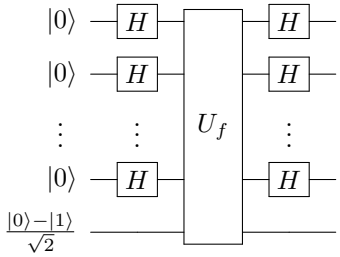
for some unknown $\underline{s} \in \{0,1\}^n$. Given a black box for f, how many classical queries are required to learn s with certainty?

2. *(Points :3)* Prove that for any n-bit string $\underline{u} \in \{0,1\}^n$,

$$\sum_{\underline{v} \in \{0,1\}^n} (-1)^{\underline{u} \cdot \underline{v}} = \begin{cases} 2^n & \text{if } \underline{u} = \underline{0} \\ 0 & \text{otherwise} \end{cases}$$

where $\underline{0}$ denotes the n-bit string $00\ldots0$.

3. *(Points :7)* Let U_f denote a quantum black box for f, acting as $U_f|\underline{x}\rangle|y\rangle = |\underline{x}\rangle|y \oplus f(\underline{x})\rangle$ for any $\underline{x} \in \{0,1\}^n$ and $y \in \{0,1\}$. Show that the output of the following circuit is the state $|\underline{s}\rangle(|0\rangle - |1\rangle)/\sqrt{2}$.



4. *(Points :2)* What can you conclude about the quantum query complexity of learning s?

Problem 4. *The Fourier transform and translation invariance.* The quantum Fourier transform on n qubits is defined as the transformation

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i x y / 2^n} |y\rangle$$

where we identify n-bit strings and the integers they represent in binary. More generally, for any nonnegative integer N, we can define the quantum Fourier transform modulo N as

$$|x\rangle \overset{F_N}{\mapsto} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle$$

where the state space is $\mathbb{C}^N$, with orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. Let P denote the unitary operation that adds 1 modulo N: for any $x \in \{0, 1, \ldots, N-1\}$, $P|x\rangle = |x+1 \bmod N\rangle$.

1. *(Points :4)* Show that F_N is a unitary transformation.

2. *(Points :7)* Show that the Fourier basis states are eigenvectors of P. What are their eigenvalues? (Equivalently, show that $F_N^{-1} P F_N$ is diagonal, and find its diagonal entries.)

3. *(Points :4)* Let $|\psi\rangle$ be a state of n qubits. Show that if $P|\psi\rangle$ is measured in the Fourier basis (or equivalently, if we apply the inverse Fourier transform and then measure in the computational basis), the probabilities of all measurement outcomes are the same as if the state had been $|\psi\rangle$.

Problem 5. *Implementing the square root of a unitary.*

1. *(Points :2)* Let U be a unitary operation with eigenvalues ± 1. Let P_0 be the projection onto the $+1$ eigenspace of U and let P_1 be the projection onto the -1 eigenspace of U. Let $V = P_0 + iP_1$. Show that $V^2 = U$.

2. *(Points :3)* Give a circuit of 1- and 2-qubit gates and controlled-U gates with the following behavior (where the first register is a single qubit):

$$|0\rangle|\psi\rangle \mapsto \begin{cases} |0\rangle|\psi\rangle & \text{if } U|\psi\rangle = |\psi\rangle \\ |1\rangle|\psi\rangle & \text{if } U|\psi\rangle = -|\psi\rangle. \end{cases}$$

3. *(Points :5)* Give a circuit of 1- and 2-qubit gates and controlled-U gates that implements V. Your circuit may use ancilla qubits that begin and end in the $|0\rangle$ state.
