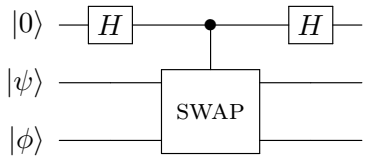
ASSIGNMENT 3 CO 481/CS 467/PHYS 467 (Winter 2014)

Due in class on Tuesday, February 25.
(Please remember that your project proposal is due by February 27.)

1. *Swap test.*

   (a) [3 points] 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:



   (b) [3 points] Suppose the top qubit in the above circuit is measured in the computational basis. What is the probability that the measurement result is 0?

   (c) [2 points] 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?

   (d) [1 point] 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?

2. *The Bernstein-Vazirani problem.*

   (a) [2 points] Suppose $f : \{0,1\}^n \to \{0,1\}$ is a function of the form

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

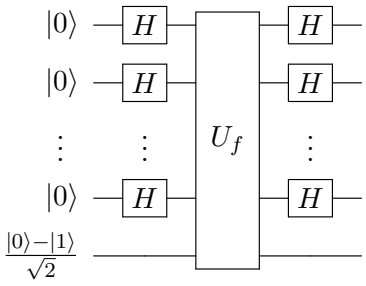
   for some unknown $\underline{s} \in \{0,1\}^n$. Given a black box for f, how many classical queries are required to learn s with certainty?

   (b) [2 points] 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 $00\ldots0$.

   (c) [4 points] 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 $|\underline{s}\rangle(|0\rangle - |1\rangle)/\sqrt{2}$.



   (d) [1 point] What can you conclude about the quantum query complexity of learning s?

3. *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 $x \in \{0, 1, \ldots, N-1\}$, $P|x\rangle = |x+1 \bmod N\rangle$.

(a) [3 points] Show that F_N is a unitary transformation.

(b) [5 points] 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.)

(c) [3 points] 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 $|\psi\rangle$.

4. *A fast approximate QFT.*

(a) [2 points] In class, we saw a circuit implementing the n-qubit QFT using Hadamard and controlled-R_k gates, where $R_k|x\rangle = e^{2\pi i x/2^k}|x\rangle$ for $x \in \{0, 1\}$. How many gates in total does that circuit use? Express your answer both exactly and using Θ notation.

(b) [3 points] Let $\mathrm{C}R_k$ denote the controlled-R_k gate, with $\mathrm{C}R_k|x, y\rangle = e^{2\pi i x y/2^k}|x, y\rangle$ for $x, y \in \{0, 1\}$. Show that $E(\mathrm{C}R_k, I) \leq 2\pi/2^k$, where I denotes the 4×4 identity matrix, and where $E(U, V) = \max_{|\psi\rangle} \|U|\psi\rangle - V|\psi\rangle\|$. You may use the fact that $\sin x \leq x$ for any $x \geq 0$.

(c) [5 points] Let F denote the exact QFT on n qubits. Suppose that for some constant c, we delete all the controlled-R_k gates with $k > \log_2(n) + c$ from the QFT circuit, giving a circuit for another unitary operation, $\tilde{F}$. Show that $E(F, \tilde{F}) \leq \epsilon$ for some ϵ that is independent of n, where ϵ can be made arbitrarily small by choosing c arbitrarily large. (Hint: Use equation 4.3.3 of KLM.)

(d) [1 point] For a fixed c, how many gates are used by the circuit implementing $\tilde{F}$? It is sufficient to give your answer using Θ notation.

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

(a) [1 point] 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 $V^2 = U$.

(b) [2 points] 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):

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

(c) [3 points] 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.