ASSIGNMENT 2 CMSC 858K (Fall 2015)

Due in class on Thursday, October 1.

1. *Universality of gate sets.* Prove that each of the following gate sets either is or is not universal. You may use the fact that the set $\{\textsc{cnot}, H, T\}$ is universal.

   (a) [1 point] $\{H, T\}$

   (b) [2 points] $\{\textsc{cnot}, T\}$

   (c) [2 points] $\{\textsc{cnot}, H\}$

   (d) [3 points] $\{\textsc{c}Z, K, T\}$, where $\textsc{c}Z$ denotes a controlled-Z gate and $K = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & i \\ i & 1 \end{smallmatrix}\right)$

   (e) [challenge problem] $\{\textsc{cnot}, H, T^2\}$

   (f) [challenge problem] $\{\textsc{c}T^2, H\}$, where $\textsc{c}T^2$ denotes a controlled-T^2 gate

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 $f(x_1, x_2) = 1$.

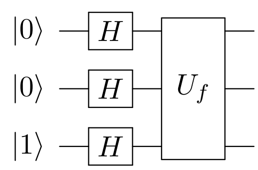
   (a) [1 point] Write the truth tables of the four possible functions f.

   (b) [2 points] How many classical queries are needed to solve one-out-of-four search?

   (c) [4 points] Suppose f is given as a quantum black box U_f acting as

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

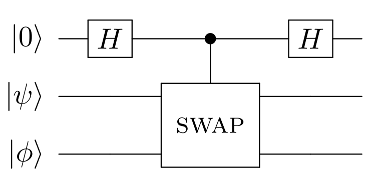
   Determine the output of the following quantum circuit for each of the possible black-box functions f:

   (d) [2 points] 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?

3. *Swap test.*

   (a) [3 points] Let $|\psi\rangle$ and $|\phi\rangle$ be arbitrary single-qubit states (not necessarily computational basis states), and let $\textsc{swap}$ denote the 2-qubit gate that swaps its input qubits (i.e., $\textsc{swap}|x\rangle|y\rangle = |y\rangle|x\rangle$ 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?

4. *The Bernstein-Vazirani problem.*

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

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

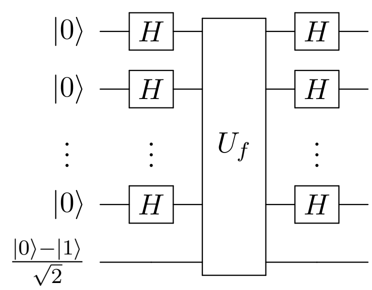
for some unknown $s \in \{0,1\}^n$. Given a black box for f, how many classical queries are required to learn s with certainty?

(b) [2 points] Prove that for any n-bit string $u \in \{0,1\}^n$,

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

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

(c) [4 points] Let U_f denote a quantum black box for f, acting as $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ for any $x \in \{0,1\}^n$ and $y \in \{0,1\}$. Show that the output of the following circuit is the state $|s\rangle(|0\rangle - |1\rangle)/\sqrt{2}$.



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

5. *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. (See the introduction to chapter 9 of KLM for a review of asymptotic notation.)

(b) [3 points] Let $\mathrm{C}R_k$ denote the controlled-R_k gate, with $\mathrm{C}R_k|x,y\rangle = e^{2\pi i xy/2^k}|x,y\rangle$ for $x, y \in \{0,1\}$. Show that $E(\mathrm{C}R_k, I) \le 2\pi/2^k$, 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 $\sin x \le x$ for any $x \ge 0$.

(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 $E(F, \tilde{F}) \le \epsilon$ for some ϵ that is independent of n, where ϵ can be made arbitrarily small by choosing c arbitrarily large.

(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.

6. *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.