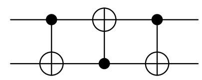
ASSIGNMENT 2 CMSC 858K(Fall 2016)

Due in class on Thursday, September 29.

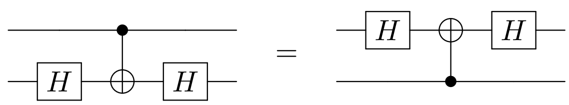
1. *Circuit identities.*

   (a) [2 points] What does the following circuit do? Show that your answer is correct.

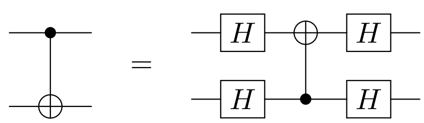
   

   (b) [1 point] Verify that $HXH = Z$, where H is the Hadamard gate and X, Z denote Pauli matrices.

   (c) [3 points] Verify the following circuit identity:

   (d) [2 points] Verify the following circuit identity:

   Give an interpretation of this identity.

2. *The Hadamard gate and qubit rotations*

   (a) [3 points] Suppose that $(n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector and $\theta \in \mathbb{R}$. Show that

   $$e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)} = \cos(\tfrac{\theta}{2})\, I - i \sin(\tfrac{\theta}{2})\, (n_x X + n_y Y + n_z Z).$$

   (b) [2 points] Find a unit vector $(n_x, n_y, n_z) \in \mathbb{R}^3$ and numbers $\phi, \theta \in \mathbb{R}$ so that

   $$H = e^{i\phi} e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)},$$

   where H denotes the Hadamard gate. What does this mean in terms of the Bloch sphere?

   (c) [3 points] Write the Hadamard gate as a product of rotations about the x and y axes. In particular, find $\alpha, \beta, \gamma, \phi \in \mathbb{R}$ such that $H = e^{i\phi} R_y(\gamma) R_x(\beta) R_y(\alpha)$.

3. *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

4. *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 $f(x_1, x_2) = 1$.

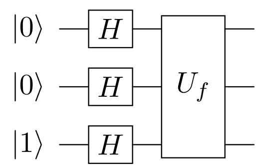
   (a) [1 point] Write the truth tables of the four possible functions f.

   (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

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

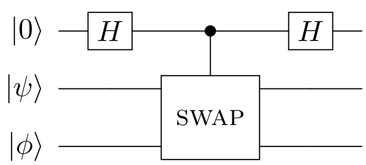
   Determine the output of the following quantum circuit for each of the possible black-box functions f:



   (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?

5. *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?

6. *The Bernstein-Vazirani problem.*

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

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

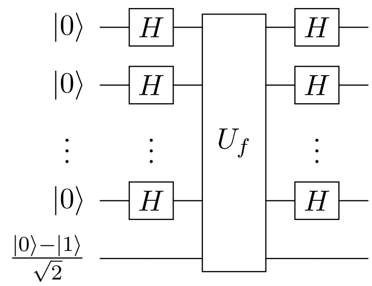
   for some unknown $s \in \{0,1\}^n$. Given a black box for f, how many classical queries are required to learn s with certainty?

(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?