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.

   ![Circuit Diagram]

   (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:

   ![Circuit Diagram]

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

   ![Circuit Diagram]

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

   (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 \{CNOT, $H, T$\} is universal.
   (a) [1 point] \{H, T\}
   (b) [2 points] \{CNOT, T\}
   (c) [2 points] \{CNOT, H\}
   (d) [3 points] \{cZ, K, T\}, where $cZ$ denotes a controlled-Z gate and $K = \frac{1}{\sqrt{2}} (\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix})$
   (e) [challenge problem] \{CNOT, H, T^2\}
   (f) [challenge problem] \{cT^2, H\}, where $cT^2$ denotes a controlled-$T^2$ gate
4. **One-out-of-four search.** Let \( f : \{0,1\}^2 \to \{0,1\} \) 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

\[
|x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus f(x_1, x_2)\rangle.
\]

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

\[
\begin{array}{c}
|0\rangle \\
|0\rangle \\
|1\rangle
\end{array}
\begin{array}{c}
H \\
H \\
H
\end{array}
\begin{array}{c}
U_f
\end{array}
\]

(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 \(\text{swap}\) 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:

\[
\begin{array}{c}
|0\rangle \\
|\psi\rangle \\
|\phi\rangle
\end{array}
\begin{array}{c}
H \\
\text{SWAP}
\end{array}
\begin{array}{c}
H
\end{array}
\]

(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 \(\text{swap}\) 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 \( f : \{0,1\}^n \to \{0,1\} \) is a function of the form

\[
f(x) = x_1s_1 + x_2s_2 + \cdots + x_ns_n \mod 2
\]

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 $s$?