ASSIGNMENT 3 CMSC/PHYS 457 (Spring 2019)

Due by 12:30 pm on Thursday, March 7. Submit your solutions in PDF via Gradescope. Please include a list of students in the class with whom you discussed the problems, or else state that you did not discuss the assignment with your classmates.

1. *A qubit cannot send more than a bit.*

   Suppose Alice wants to send a trit of classical information (i.e., an element $x \in \{0,1,2\}$) to Bob, and she is able to send him a qubit. Specifically, suppose that on input x she sends him $|\psi_x\rangle = \alpha_x|0\rangle + \beta_x|1\rangle$. Clearly, Bob can only reliably distinguish two outcomes by measuring $|\psi_x\rangle$ in some basis. However, if he interacts the qubit he receives with $n-1$ ancilla qubits for $n > 1$, he can perform a measurement with more than two outcomes on the resulting n-qubit state. In this problem you will show that even using such a protocol, Bob cannot reliably determine a trit encoded by Alice.

   In Bob's protocol, suppose he applies the unitary operation U to the state $|\psi_x\rangle \otimes |0\rangle^{\otimes n-1}$ and measures in the computational basis, obtaining an outcome $m \in \{0,1\}^n$. He then applies some function $f\colon \{0,1\}^n \to \{0,1,2\}$ to obtain a trit. He succeeds if $f(m) = x$.

   (a) [4 points] For $x \in \{0,1,2\}$, let V_x denote the span of the rows of the matrix U that are indexed by some $m \in \{0,1\}^n$ such that $f(m) = x$. In other words, if $U = \sum_{m\in\{0,1\}^n} |m\rangle\langle\phi_m|$, we have $V_x = \operatorname{span}\{|\phi_m\rangle : f(m) = x\}$. Show that the subspaces V_0, V_1, V_2 are pairwise orthogonal.

   (b) [3 points] Explain why, for Bob to succeed, we must have $|\psi_x\rangle|0\rangle^{\otimes n-1} \in V_x$ for all $x \in \{0,1,2\}$.

   (c) [3 points] Prove that it is impossible to have $|\psi_x\rangle|0\rangle^{\otimes n-1} \in V_x$ for all $x \in \{0,1,2\}$.

2. *The Hadamard gate and qubit rotations.*

   (a) [4 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) [3 points] Find a unit vector $(n_x, n_y, n_z) \in \mathbb{R}^3$ and numbers $\phi, \theta \in \mathbb{R}$ so that

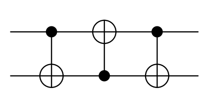
   $$H = e^{i\phi} e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)},$$

   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 $H = e^{i\phi} R_y(\gamma) R_x(\beta) R_y(\alpha)$.

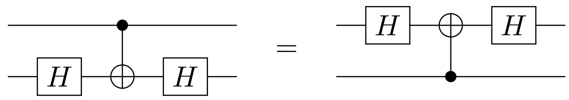
3. *Circuit identities.*

   (a) [3 points] What does the following circuit do? Show that your answer is correct.

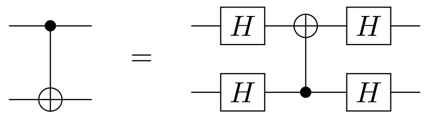
   

   (b) [1 point] Verify that $HXH = Z$, where H is the Hadamard gate and X, Z denote Pauli matrices.

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



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



Give an interpretation of this identity.

4. *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) [2 points] $\{H, T\}$

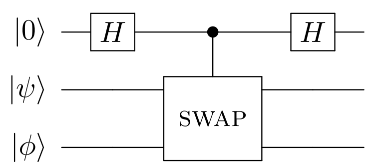
(b) [2 points] $\{\textsc{cnot}, T\}$

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

(d) [4 points] $\{\textsc{c}Z, K, T\}$, where $\textsc{c}Z$ denotes a controlled-Z gate and $K = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & i \\ i & 1 \end{smallmatrix}\right)$

5. *Swap test.*

(a) [4 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 $\textsc{swap}$ denotes the $2n$-qubit gate that swaps the first n qubits with the last n qubits?