Homework 6 8.370/18.435/2.111 Due 11/2.

1. Define the *Pauli* group $\mathcal{P}$ on n qubits as the tensor product of Pauli matrices and identities, together with a power of i. For example, $i\sigma_x \otimes I \otimes \sigma_z$ is in the Pauli group on three qubits.

   Define the *Clifford group* $\mathcal{C}$ on n qubits as the group made up of all unitary matrices U that satisfy

   $$UgU^\dagger \in \mathcal{P} \text{ for all matrices } g \in \mathcal{P}$$

   (a) Show that the Clifford group is a group; that is,

      i. if $A \in \mathcal{C}$ and $B \in \mathcal{C}$, then $AB \in \mathcal{C}$, and

      ii. if $A \in \mathcal{C}$, then $A^\dagger \in \mathcal{C}$.

   (b) Show that the Hadamard gate H is in $\mathcal{C}$.

   (c) Show that the CNOT gate is in $\mathcal{C}$.

   (d) Show that the T gate $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ is not in $\mathcal{C}$.

   Hint: For 1b and 1c, you don't need to check the condition for all elements of the Pauli group, just for a set of elements that generate it (although if you use this fact, explain why it's true).

2. If you don't erase the workbits in a quantum computer, it can cause your algorithm to get incorrect results. Here is an example.

   Consider Simon's algorithm. Suppose you've programmed up Simon's algorithm on a quantum computer, and are trying to find c where $f(x) = f(x \oplus c)$, but you forgot to erase the workbits when computing the quantum oracle. As a result, for any x and y with $x \oplus c = y$, the workspace when you compute $f(x)$ and $f(y)$ contain different values of bits. What happens when you try to run Simon's algorithm? Can you find c?

3. (a) Suppose that you have a function f mapping n-bit strings to n-bit strings which is not necessarily 2-to-1, but where $f(x) = f(x \oplus c)$. Does the quantum part of Simon's algorithm still always return a binary string with $c \cdot k = 0 \pmod 2$?

   (b) Suppose that $f(x) = 0$ except for two values, d and $d \oplus c$, which have $f(x) = 1$. Approximately how many times do you need to run the algorithm in part (a) before you find a non-zero $f(x)$? How many function evaluations will it take you to find c? How does this compare to the time it would take on a classical computer?

4. *Partial transpose* Suppose you have two qubits. They have a 4×4 density matrix. We will write this matrix as a 2×2 matrix of 2×2 submatrices F, G, H, and J. Define the partial transpose of such a matrix

$$M = \begin{pmatrix} F & G \\ H & J \end{pmatrix} \qquad \text{as} \qquad pt(M) = \begin{pmatrix} F & H \\ G & J \end{pmatrix}.$$

Note that if we also took the transpose of F, G, H, and J, we would get the transpose of M.

Recall that a Hermitian matrix is said to be non-negative if it has all non-negative eigenvalues.

(a) Show that if M is separable, i.e. if

$$M = \sum_i \lambda_i \left|v_i\right\rangle\!\left\langle v_i\right| \otimes \left|w_i\right\rangle\!\left\langle w_i\right|,$$

where the λ_i are positive and v_i and w_i are unit vectors, then $pt(M)$ is non-negative. Density matrices which are not separable are said to be entangled. Hint: a matrix M is non-negative if and only if $\langle x| M |x\rangle \geq 0$ for all $|x\rangle$.

(b) Use part (a) to show that the density matrix for $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is not separable.

5. Suppose you are given a three-dimensional quantum system (a *qutrit*) with basis $|0\rangle$, $|1\rangle$, $|2\rangle$, in some unknown state $|\psi\rangle$. Can you teleport it?

One thing you can do is embed it in a set of qubits of higher dimension. So, for example, you can embed one qutrit in two qubits (since $3 < 4$), and five qutrits in eight qubits (since $3^5 < 2^8$), and then teleport these qubits. But you can also teleport qutrits directly.

Let $\omega = e^{2\pi i/3}$ be a cube root of 1, and define the 3×3 matrices

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Then the analog of the EPR pair is the state $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$, and the analog of the Pauli matrices are the nine matrices $P^a T^b$, where $0 \leq a, b < 3$.

Figure out how a qutrit teleportation algorithm works and describe it.