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, $i\sigma_x \otimes I$ is in the Pauli group.

   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
      Solution: For all $g \in \mathcal{P}$, let $g' = BgB^\dagger$. then $g \in \mathcal{P}$, which means $Ag'A^\dagger \in \mathcal{P}$. Thus $AB \in \mathcal{C}$.

      ii. if $A \in \mathcal{C}$, then $A^\dagger \in \mathcal{C}$.
      Solution: Note that since A is a unitary matrix, the function $f : \mathcal{P} \to \mathcal{P}$, $f(g) = AgA^\dagger$ is a bijection. In other words, every $g \in \mathcal{P}$ can be written as $Ag'A^\dagger$ for a unique g'. Therefore we have for all g, $A^\dagger gA = A^\dagger f^{-1}(g)A = f^{-1}(g) \in \mathcal{P}$.

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

      Solution: Note that we only need to check for a set of generators of the Pauli group $\mathcal{P}$, because for any unitary U, if $Ug_1U^\dagger, Ug_2U^\dagger \in \mathcal{P}$, then $Ug_1g_2U^\dagger = Ug_1U^\dagger Ug_2U^\dagger \in \mathcal{P}$.
      It is then easy to check that $HIH^\dagger = I, HZH^\dagger = X, HXH^\dagger = Z, HYH^\dagger = -Y$. Technically, we don't need to check Y here since $Y = -iZX$.

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

      Solution: FOllowing part (a), we only need to check the cases

$$\begin{aligned}
\text{CNOT}(X \otimes I)\text{CNOT}^\dagger &= X \otimes X \\
\text{CNOT}(I \otimes X)\text{CNOT}^\dagger &= I \otimes X \\
\text{CNOT}(Z \otimes I)\text{CNOT}^\dagger &= Z \otimes I \\
\text{CNOT}(I \otimes Z)\text{CNOT}^\dagger &= Z \otimes Z.
\end{aligned}$$

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

      Solution: Consider

$$TXT^\dagger = \begin{bmatrix} 0 & e^{-i\pi/4} \\ e^{i\pi/4} & 0 \end{bmatrix} \notin \mathcal{P}.$$

      Therefore $T \notin \mathcal{C}$.

   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?

Solution: If you do not uncompute $f(x)$, the state you have before applying the second Hadamard transform in Simon's algorithm is

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle |\text{junk}_x\rangle |f(x)\rangle .$$

Now if we apply the Hadamard to the first qubit, the state is

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} \left(\sum_{y=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle \right) |f(x)\rangle |\text{junk}_x\rangle |f(x)\rangle = \frac{1}{2^n} \sum_{x,z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle |f(x)\rangle |\text{junk}_x\rangle |f(x)\rangle .$$

Since $|\text{junk}_x\rangle \neq |\text{junk}_y\rangle$ for $y = x \oplus c$, if we now measure the first two registers in the standard basis, for any x and y, the probability that we get $|y\rangle |f(x)\rangle$ is $\frac{1}{2^{2n}} + \frac{1}{2^{2n}} = \frac{1}{2^{2n-1}}$, and the measurement result gives us no information on c. Therefore Simon's algorithm will fail.

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 $c \cdot k = 0 \pmod 2$?

   Solution:

   The analysis of Simon's algorithm proceeds exactly as it does in the two-to-one case until we compute the probability of seeing a state $|k\rangle |\ell\rangle$.

   Now, the probability of seeing $|k\rangle |\ell\rangle$ is

   $$\frac{1}{2^n} \sum_{(j, j \oplus c): f(j) = \ell} (-1)^{j \cdot k} (1 + (-1)^{c \cdot k}).$$

   If $c \cdot k = 1 \pmod 2$, then the above sum is still 0. Therefore we still only see k 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?

   Solution:

   i. Approximately how many times do you need to run the algorithm in part (a) before you find a non-zero $f(x)$?

      The probability you see a specific $|k\rangle |1\rangle$ with $k \cdot c = 0$ is

      $$\left| \frac{1}{2^n} \left((-1)^{d \cdot k} + (-1)^{(d \oplus c) \cdot k} \right) \right|^2 = \frac{4}{2^{2n}} = \frac{1}{2^{2n-2}}.$$

      There are 2^{n-1} possible k's with $k \cdot c = 0$. So the probability of seeing $|1\rangle$ in the second register is $\frac{1}{2^{n-1}}$, and the expected number of times you will have to run the algorithm for this is 2^{n-1}.

ii. How many function evaluations will it take you to find c?
The challenge here is that the probability of measuring $|k\rangle|0\rangle$ where $k = 0$ is quite high. The probability is

$$\left| \frac{1}{2^n} \sum_{j:f(j)=0} (-1)^{j\cdot 0} \right|^2 = \left| \frac{2^n - 2}{2^n} \right|^2 = (1 - \frac{1}{2^{n-1}})^2.$$

However, measuring $k = 0$ is not useful. We need to get $n - 1$ linearly independent values of k before we find c. If the second register is $|1\rangle$, for any k such that $c \cdot k = 0$, the probability that the first register is $|k\rangle$ is $1/2^{2n-2}$ as in part (i).
If the second register is $|0\rangle$, for any k, the probability of seeing $|k\rangle|0\rangle$ is

$$\left| \frac{1}{2^n} \sum_{j:f(j)=0} (-1)^{j\cdot k} \right|^2.$$

There are $2^n - 2$ possible j's with $f(j) = 0$, and 2^{n-1} will give you $(-1)^{j\cdot k} = 1$ while $2^{n-1} - 2$ will give you $(-1)^{j\cdot k} = -1$ (or maybe the other way around). This means that the probability of seeing $|k\rangle|0\rangle$ is

$$\frac{4}{2^{2n}} = \frac{1}{2^{2n-2}}.$$

Since there are $2^{n-1} - 1$ non-zero k such that $c \cdot k = 0$, the total probability of getting a non-zero, desirable k is roughly $\frac{1}{2^{n-2}}$, and the expected time before we see a non-zero k is 2^{n-2}. However, we need $n-1$ linearly independent non-zero k to find c, so Simon's algorithm takes approximately $n2^{n-2}$ time in this case. (Even if we get an output with $|1\rangle$ in the second register, the first register only gives us a vector perpendicular to c.)

iii. How does this compare to the time it would take on a classical computer?
On a classical computer, you can search all possibilities for $f(x) = 1$ in time 2^n, which is less than what Simon's algoirthm takes. Randomized algorithm will not help here, because we need to find the two values where $f(x) = 1$ to determine c.

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.

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

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

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 $|x\rangle$.

Solution: Here let's assume that $|v_i\rangle = [v_{i,0}, v_{i,1}]^T$, $|w_i\rangle = [w_{i,0}, w_{i,1}]^T$. Then we have

$$\begin{aligned} pt(M) &= \sum_i \lambda_i pt \begin{bmatrix} v_{i,0}v_{i,0}^* |w_i\rangle\langle w_i| & v_{i,0}v_{i,1}^* |w_i\rangle\langle w_i| \\ v_{i,1}v_{i,0}^* |w_i\rangle\langle w_i| & v_{i,1}v_{i,1}^* |w_i\rangle\langle w_i| \end{bmatrix} \\ &= \sum_i \lambda_i \begin{bmatrix} v_{i,0}v_{i,0}^* |w_i\rangle\langle w_i| & v_{i,1}v_{i,0}^* |w_i\rangle\langle w_i| \\ v_{i,0}v_{i,1}^* |w_i\rangle\langle w_i| & v_{i,1}v_{i,1}^* |w_i\rangle\langle w_i| \end{bmatrix} \\ &= \sum_i \lambda_i |v_i^*\rangle\langle v_i^*| \otimes |w_i\rangle\langle w_i| . \end{aligned}$$

Where $|v_i^*\rangle = [v_{i,0}^*, v_{i,1}^*]^T$. Now given any state $|x\rangle$, we have

$$\begin{aligned} \langle x| pt(M) |x\rangle &= \sum_i \lambda_i \langle x| |v_i^* w_i\rangle\langle v_i^* w_i| |x\rangle \\ &= \sum_i \lambda_i |\langle x|v_i^* w_i\rangle|^2 \geq 0, \end{aligned}$$

since $\lambda_i \geq 0$ for all i.

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

Solution: Here we note that the density matrix for the EPR pair is

$$\rho = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Therefore

$$pt(\rho) = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

This matrix has eigenvalue -1 with eigenvector $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, which means the EPR pair 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

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

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.

Solution:

We follow the standard teleportation protocol. Suppose A has a qutrir in state $a\left|0\right\rangle + b\left|1\right\rangle + c\left|2\right\rangle$, and A has one qubit from the state $\left|\Phi\right\rangle = \frac{1}{\sqrt{3}}(\left|00\right\rangle + \left|11\right\rangle + \left|22\right\rangle)$. Suppose B has the other entangled qubit. The overall three qutrit state is

$$\frac{1}{\sqrt{3}}\left[a\left|000\right\rangle + a\left|011\right\rangle + a\left|022\right\rangle + b\left|100\right\rangle + b\left|111\right\rangle + b\left|122\right\rangle + c\left|200\right\rangle + c\left|211\right\rangle + c\left|222\right\rangle\right]$$

A measures her two qubits in the following basis (on the left, here P, T are both applied to A's entangled qutrit), and given her measurement results, B applies the correction (on the right).

Resulting state of measurement	State held by B after measurement by A	Correction by B
$P^0T^0\left|\phi\right\rangle = \left|\phi\right\rangle$	$a\left|0\right\rangle + b\left|1\right\rangle + c\left|2\right\rangle$	P^0T^0
$P^0T^1\left|\phi\right\rangle = \frac{1}{\sqrt{3}}(\left|02\right\rangle + \left|10\right\rangle + \left|21\right\rangle)$	$a\left|2\right\rangle + b\left|0\right\rangle + c\left|1\right\rangle$	P^0T^2
$P^0T^2\left|\phi\right\rangle = \frac{1}{\sqrt{3}}(\left|01\right\rangle + \left|12\right\rangle + \left|20\right\rangle)$	$a\left|1\right\rangle + b\left|2\right\rangle + c\left|0\right\rangle$	P^0T^1
$P^1T^0\left|\phi\right\rangle = \frac{1}{\sqrt{3}}(\left|00\right\rangle + \omega\left|11\right\rangle + \omega^2\left|22\right\rangle)$	$a\left|0\right\rangle + b\omega\left|1\right\rangle + c\omega^2\left|2\right\rangle$	P^2T^0
$P^1T^1\left|\phi\right\rangle = \frac{1}{\sqrt{3}}(\omega^2\left|02\right\rangle + \left|10\right\rangle + \omega\left|21\right\rangle)$	$a\omega^2\left|2\right\rangle + b\left|0\right\rangle + c\omega\left|1\right\rangle$	P^2T^2
$P^1T^2\left|\phi\right\rangle = \frac{1}{\sqrt{3}}(\omega\left|01\right\rangle + \omega^2\left|12\right\rangle + \left|20\right\rangle)$	$a\omega\left|1\right\rangle + b\omega^2\left|2\right\rangle + c\left|0\right\rangle$	P^2T^1
$P^2T^0\left|\phi\right\rangle = \frac{1}{\sqrt{3}}(\left|00\right\rangle + \omega^2\left|11\right\rangle + \omega\left|22\right\rangle)$	$a\left|0\right\rangle + b\omega^2\left|1\right\rangle + c\omega\left|2\right\rangle$	P^1T^0
$P^2T^1\left|\phi\right\rangle = \frac{1}{\sqrt{3}}(\omega\left|02\right\rangle + \left|10\right\rangle + \omega^2\left|21\right\rangle)$	$a\omega\left|2\right\rangle + b\left|0\right\rangle + c\omega^2\left|1\right\rangle$	P^1T^2
$P^2T^2\left|\phi\right\rangle = \frac{1}{\sqrt{3}}(\omega^2\left|01\right\rangle + \omega\left|12\right\rangle + \left|20\right\rangle)$	$a\omega^2\left|1\right\rangle + b\omega\left|2\right\rangle + c\left|0\right\rangle$	P^1T^1

Note that the states on the left form a measurement basis, i.e they are orthonormal because $1 + \omega + \omega^2 = 0$. This can be most easily seen by the fact that multiplying this sum by ω does not change it. We see that this protocol achieves teleportation of qutrits.