QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F16)

Assignment 5
Due date: December 1, 2016

1. **A nonlocal game [12 points; 6 each].** Consider the nonlocal game where Alice are physically separated and their goal is to produce outputs that satisfy the winning conditions explained below. Alice receives a trit $s \in \{0, 1, 2\}$ (randomly sampled by the uniform distribution), and Bob receives a trit $t \in \{s, s + 1 \bmod 3\}$ (randomly sampled according to the uniform distribution).

   They each output a bit, a for Alice and b for Bob, and they win if: $a \oplus b = 1$, in the case where $(s, t) = (2, 0)$; and $a \oplus b = 0$ in the other five cases. There six possible instances of (s, t), which each arise with probability $1/6$. They are listed in the following table, along with the corresponding winning condition.

s	t	$a \oplus b$
0	0	0
0	1	0
1	1	0
1	2	0
2	2	0
2	0	1

   (a) Show that any classical strategy for this game succeeds with probability at most $5/6 \approx 0.833$.

   (b) Show that there is a quantum strategy (using entanglement) that succeeds with probability $\cos^2(\pi/12) \approx 0.933$. (Hint: Recall that the entangled strategy for the CHSH game can be expressed as starting with the state $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$ and Alice and Bob each perform a rotation depending on their respective inputs s and t. Consider a variant of this with different rotation angles.)

2. **Some reflections [12 points; 6 each].**

   (a) For $\theta \in [0, \pi]$, define the orthonormal basis

$$|\psi_\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle \qquad \text{and} \qquad |\psi_\theta^\perp\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle. \tag{1}$$

   Define the reflections $R_1 = |\psi_{\theta_1}\rangle\langle\psi_{\theta_1}| - |\psi_{\theta_1}^\perp\rangle\langle\psi_{\theta_1}^\perp|$ and $R_1 = |\psi_{\theta_2}\rangle\langle\psi_{\theta_2}| - |\psi_{\theta_2}^\perp\rangle\langle\psi_{\theta_2}^\perp|$. Prove that $R_1 R_2$ is a rotation by angle $2(\theta_1 - \theta_2)$.

   (b) Consider the following scenario. $|u\rangle$ and $|v\rangle$ are two n-qubit states with the property $\langle u|v\rangle = \cos(\pi/12)$ and all you are given is: these two black-box n-qubit unitaries

$$U = I - 2|u\rangle\langle u| \qquad \text{and} \qquad V = I - 2|v\rangle\langle v|, \tag{2}$$

   as well as one single copy of the state $|u\rangle$. (Note that U is a reflection, where $U|u\rangle = -|u\rangle$ and $U|w\rangle = |w\rangle$ for each state $|w\rangle$ that is orthogonal to $|u\rangle$; and V satisfies similar properties for $|v\rangle$.)

   Your goal is to construct a state *orthogonal* to $|u\rangle$. Show how to do this starting with state $|u\rangle$ and making queries to U and to V (make as few queries as you can).

3. **Distributed testing of $|00\rangle + |11\rangle$ states [12 points].** Consider the scenario that arises in the Lo-Chau cryptosystem, where Alice and Bob share a two-qubit state and they want to test if it is $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with local measurements and classical communication.

   We consider the following procedure. They randomly select a measurement basis: with probability $\frac{1}{2}$, they both measure in the computational basis; and, with probability $\frac{1}{2}$, they both measure in the Hadamard basis. Then they perform the measurement and they accept if and only if their outcomes are the same.

   (a) [4 points] Show that the state $|\phi^+\rangle$ is always (i.e., with probability 1) accepted by this test.

   (b) [8 points] Show that, for an arbitrary 2-qubit state $|\mu\rangle$, the probability that it passes the test is **at most**

$$\frac{1 + |\langle\mu|\phi^+\rangle|^2}{2}. \tag{3}$$

   (Hint: Consider expressing $|\mu\rangle$ as a superposition of the four Bell states.)

4. **Analysis of a particular channel [12 points; 6 each].** For each $p \in \mathbb{R}$ such that $0 < p \leq \frac{1}{2}$, consider the qubit channel C_p, with Kraus operators

$$A_0 = \begin{pmatrix} \sqrt{1-p} & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \quad \text{and} \quad A_1 = \begin{pmatrix} \sqrt{p} & 0 \\ 0 & -\sqrt{p} \end{pmatrix}. \tag{4}$$

   Thus, for any qubit in state ρ, the output of the channel is $C_p(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger$.

   (a) If the channel C_p is composed with the channel C_q, show that the result is the channel C_r for some r that is a function of p and q.

   (b) Give the set of all 1-qubit states ρ such that $C_p(\rho) = \rho$.

5. **Transpose operation [12 points; 6 each]**.

   Here we consider an operation on qubits that we denote by Λ, defined as $\Lambda(\rho) = \rho^T$ for each density matrix ρ (where ρ^T is the transpose of T).

   (a) Give an example of a one-qubit pure state $|\psi\rangle$ such that $\Lambda(|\psi\rangle\langle\psi|)$ is a pure state orthogonal to $|\psi\rangle$.

   (b) Prove that there is no unitary operation U such that $\Lambda(\rho) = U\rho U^\dagger$ for all ρ.
   (In fact, Λ is not even of the form $\rho \mapsto \sum_{k=1}^{m} A_k \rho A_k^\dagger$, where $\sum_{k=1}^{m} A_k^\dagger A_k = I$, though this is harder to show.)