Introduction to Quantum Information Processing
Assignment 3
Due electronically at 11:59pm on Friday 26 November.

1. Let m be any integer greater than 1. Consider the following black box problem. We are given a black box computing some $f : Z_m \to Z_m$ of the form $f(x) = ax + b$, where a and b are unknown elements of Z_m (in Z_m, addition and multiplication are always performed modulo m). The goal is to determine a (determining b is not required).

   Classically, one query to f is not sufficient to determine a; however, two queries do suffice, since $f(1) - f(0) = a$. The goal of this question is to solve this problem by a quantum algorithm that makes one query to f. The algorithm will arise from parts (a) and (b) below.

   In both parts, you may assume that the QFTs F_m and $F_m^\dagger$ can be computed.

   (a) Suppose that we are given a black box that makes quantum queries to f in the following sense. We have access to a unitary U_f such that, for all $x, y \in Z_m$,
   $$U_f \,|\, x\rangle \,|\, y\rangle = |\, x\rangle \,|\, y + f(x)\rangle \,.$$
   Define the quantum state
   $$|\, \psi\rangle = \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} \left(e^{2\pi i/m}\right)^{f(x)} |\, x\rangle \,.$$
   Show how to construct $|\, \psi\rangle$ from only one query to U_f. [5 marks]

   (b) Assume that we have one copy of $|\, \psi\rangle$ as defined in part (a). Show how to transform $|\, \psi\rangle$ into $|\, a\rangle$. (Taken together, parts (a) and (b) show how to determine a from a single U_f query.) [5 marks]

2. (a) Express $U = e^{-i\alpha X\otimes Z}$ as a linear combination of tensor products of Pauli matrices. In other words, find coefficients α_{ij} so that
   $$U = \sum_{i,j} \alpha_{i,j} \sigma_i \otimes \sigma_j$$
   where the $\sigma_i, \sigma_j \in \{\mathbb{1}, \mathrm{X}, \mathrm{Y}, \mathrm{Z}\}$. [2 marks]

   (b) Consider $U = \frac{1}{\sqrt{2}} (\mathbb{1} \otimes \mathbb{1} - \mathrm{iX} \otimes \mathrm{Y})$
   Assume the initial state is of the form
   $$(\alpha \,|\, 0\rangle + \beta \,|\, 1\rangle) \otimes |\, 1\rangle \qquad (1)$$
   Find the final state of the joint system. [2 marks]
   Let F be the operation that maps one qubit states $|\, \psi\rangle = \alpha \,|\, 0\rangle + \beta \,|\, 1\rangle$ to
   $$Tr_2(U(|\, \psi\rangle \langle\psi\,| \otimes |\, 1\rangle \langle 1\,|)U^\dagger).$$
   Find the output of applying the operation F to an input qubit with amplitudes $\alpha = 1$, $\beta = 0$. [2 marks]
   Find a one-qubit state of which remains unchanged after the application of F. [2 marks]

   (c) Find the quantum operation for F under the above evolution, i.e. find the Kraus operators $\{A_i\}$ using the computational basis for the second system and show that $\sum_i A_i^\dagger A_i = \mathbb{1}$. Find a state of F which remains unchanged under the evolution. [3 marks]

(d) Let F be the 3-qubit operator $F(\rho) = \sum_{i=0}^{3} A_i \rho A_i^\dagger$ where $A_0 = \frac{1}{2}\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}$, $A_1 = \frac{1}{2} X \otimes \mathbb{1} \otimes \mathbb{1}$, $A_2 = \frac{1}{2}\mathbb{1}\otimes\mathrm{X}\otimes\mathbb{1}$, $A_3 = \frac{1}{2}\mathbb{1}\otimes\mathbb{1}\otimes\mathrm{X}$. Is it possible to distinguish $F(|\,000\rangle\,\langle 000\,|)$ and $F(|\,111\rangle\,\langle 111\,|)$ (prove your claim)? [2 marks]

3. (a) Find a purification of the mixed state $\rho = \begin{pmatrix} \frac{1}{2} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{2} \end{pmatrix}$. [2 marks]

(b) Show how to implement the operation

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

using only the CNOT gate and one-qubit gates. [1 mark]

Show how to construct the following operation using only one-qubit gates:

$$U_f\,|\,x_1\rangle\,|\,x_2\rangle = (-1)^{x_1 \oplus x_2}\,|\,x_1\rangle\,|\,x_2\rangle\,.$$

[1 mark]

(c) Consider a unitary operation A that satisfies

$$A\,|\,00\rangle = \frac{\alpha_0}{2}\,|\,01\rangle + \frac{\alpha_1}{2}\,|\,10\rangle + \frac{\sqrt{3}\beta_0}{2}\,|\,00\rangle + \frac{\sqrt{3}\beta_1}{2}\,|\,11\rangle$$

where $|\alpha_0|^2 + |\alpha_1|^2 = 1$ and $|\beta_0|^2 + |\beta_1|^2 = 1$.

What is the probability p of measuring an outcome $|\,x_1 x_2\rangle$ satisfying $x_1 \oplus x_2 = 1$? [1 mark]

Find $\theta \in [0, \pi/2]$, and normalized states $|\,\psi_1\rangle$ and $|\,\psi_0\rangle$ so that $A\,|\,00\rangle = \sin(\theta)\,|\,\psi_1\rangle + \cos(\theta)\,|\,\psi_0\rangle$ and $U_f\,|\,\psi_1\rangle = -\,|\,\psi_1\rangle$ and $U_f\,|\,\psi_0\rangle = |\,\psi_0\rangle$ (same U_f defined above). [2 marks]

(d) Assume you have access to a black boxes implementing A and $A^\dagger$. Show how to construct the state $\alpha_0\,|\,01\rangle + \alpha_1\,|\,10\rangle$ with certainty using at most 3 black boxes and standard one- and two-qubit gates. (N.B. the values α_0, α_1 are unknown) [3 marks]

4. This question is based on the Kochen-Specker Theorem, which can be stated as follows.

Theorem: There exists an explicit set of vectors $\{v_1, \ldots, v_m\}$ in $\mathbb{R}^3$ that *cannot* be $\{0,1\}$-colored so that both of the following conditions hold:
(1) For every orthogonal pair of vectors v_i and v_j, they are not both colored 1.
(2) For every mutually orthogonal triple of vectors v_i, v_j, and v_k, at least one of them is colored 1.

The original theorem used 117 vectors, but this has subsequently been reduced to 31. Let us define a game relative to some fixed sequence of vectors $(v_1, \ldots, v_m)$ from some version of the theorem, **and assume that every orthogonal pair is part of an orthogonal triple**. There are two cooperating players, Alice and Bob, who are forbidden from communicating with each other once the game starts. Each player is asked one question, and they win iff their answers satisfy certain properties.

Alice receives three numbers $(i, j, k) \in \{1, \ldots, m\}^3$ **such that v_i, v_j, v_k is an orthogonal triple (randomly selected, among all the orthogonal triples)**, and is required to answer with three bits $(a_i, a_j, a_k) \in \{0,1\}^3$ (intuitively, a_i, a_j, a_k are colors assigned to v_i, v_j, v_k, respectively). Bob receives one number $l \in \{i, j, k\}$ (randomly selected), and is required to answer with a bit $b \in \{0,1\}$

(intuitively, b is a color assigned to v_l). They win if (i) the coloring a_i, a_j, a_k of v_i, v_j, v_k satisfies both of the Kochen-Specker conditions, and (ii) Alice and Bob's colors are consistent in the sense that $a_l = b$.

(a) Prove that, for *any* classical strategy of Alice and Bob, the success probability is less than 1.
[6 marks]

(b) As a first step towards designing a quantum strategy that always succeeds, suppose that Alice and Bob have entanglement $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$, and suppose that v_i, v_j, v_k happen to be mutually orthogonal. Let Alice and Bob each measure their qutrit with respect to the basis v_i, v_j, v_k. Show that the two qutrits that result from the measurement will be the same.
[6 marks]

(c) Give a quantum strategy for Alice and Bob, based on entanglement $|\psi\rangle$, where the success probability is 1.
[4 marks bonus]

5. Consider an ion trap quantum computer, or any other quantum computer, where $|0\rangle$ and $|1\rangle$ have different energies E_0 and E_1, and one-qubit gates are effected using light fields containing photons with energy (roughly) equal to $E_1 - E_0$. If the light field interacting with the qubit consists of exactly n photons, then a transition from $|1\rangle$ to $|0\rangle$ will leave $n+1$ photons in the light field; a transition from $|0\rangle$ to $|1\rangle$ will leave $n-1$ photons in the light field, $|0\rangle \to |0\rangle$ or $|1\rangle \to |1\rangle$ leaves n photons in the light field. In other words, for general inputs, the light field will be entangled with the qubit, preventing quantum interference in the qubit.

We generally model the light field used as being in a "coherent state", which is a special superposition of different numbers of photons. For simplicity ("coherent states" have more complicated coefficients), suppose our light field, before the interaction with the qubit, is in the state

$$|\Psi_k\rangle = \sum_{n=1}^{k} \frac{1}{\sqrt{k}} |n\rangle$$

where $|n\rangle$ denotes the state with n identical photons.

Let H be the interaction between the light field and qubit that maps $|0\rangle|n\rangle \to \frac{1}{\sqrt{2}}|0\rangle|n\rangle + \frac{1}{\sqrt{2}}|1\rangle|n-1\rangle$ and $|1\rangle|n\rangle \to \frac{1}{\sqrt{2}}|0\rangle|n+1\rangle - \frac{1}{\sqrt{2}}|1\rangle|n\rangle$.

(a) 3 marks
Suppose the qubit and light field start in the state $|0\rangle|\Psi_k\rangle$ and then they interact according to H. Compute the partial trace of the qubit (i.e. trace out the light field after the interaction).

(b) 2 marks
Suppose we take the qubit at the end of part a) and interact it with another independent light field also in state $|\Psi_k\rangle$ according to H. What is the resulting state of the qubit after you trace out the second light field as well? With what probability would a measurement in the computational basis yield $|1\rangle$?