QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F19)

Assignment 5
Due date: November 21, 2019

1. **Some properties of Shor's 9-qubit code [12 points, 4 each].** Here we consider Pauli errors, which are 9-fold tensor products of $\{I, X, Z, Y\}$, and the *weight* of an error is the number of components that are not I.

   (a) The Shor code can correct for the set of errors of weight ≤ 1. For this error set, does the error syndrome uniquely determine the error? Either way, justify your answer.

   (b) Note that the Shor code corrects a larger set of errors than those of weight ≤ 1. For example, it corrects $I \otimes X \otimes I \otimes X \otimes I \otimes I \otimes I \otimes I \otimes X$ (because this is one X error in each of the three blocks and hence corrected by the "inner code"). On the other hand, it does *not* correct the error $X \otimes X \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$.

   There are $4^9 = 262,144$ potential errors. The code corrects: 1 error of weight 0 (namely, $I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$); 27 errors of weight 1 (X, Y, or Z in nine possible positions). How many errors of weight 2 does it correct?

   (c) What is the maximum weight of error that the Shor code corrects? Give an example of such an error.

2. **Hadamard transform on uniform superposition of affine linear space [12 points; 6 each].** Let C be any linear subspace of $\{0,1\}^n$ (viewed as a vector space over $\mathbb{Z}_2$). Define $C^\perp = \{x \in \{0,1\}^n : \text{such that } x \cdot y = 0 \text{ for all } y \in C\}$, where we define $x \cdot y = x_1 y_1 + \cdots + x_n y_n \bmod 2$.

   (a) Prove that $H^{\otimes n}\left(\frac{1}{\sqrt{|C|}} \sum_{x \in C} |x\rangle\right) = \frac{1}{\sqrt{|C^\perp|}} \sum_{y \in C^\perp} |y\rangle.$

   (b) Prove that, for any $z \in \{0,1\}^n$, $H^{\otimes n}\left(\frac{1}{\sqrt{|C|}} \sum_{x \in C} |x + z\rangle\right) = \frac{1}{\sqrt{|C^\perp|}} \sum_{y \in C^\perp} (-1)^{y \cdot z} |y\rangle.$

   Note: Since part (b) subsumes part (a), a correct solution to (b) alone results in full marks for (a). The purpose of part (a) is as a warm-up to part (b).

3. **Is the transpose a valid quantum operation? [14 points].** 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) [4] Give an example of a one-qubit pure state $|\psi\rangle$ such that $\Lambda\big(|\psi\rangle\langle\psi|\big)$ is a pure state orthogonal to $|\psi\rangle$.

   (b) [5] Prove that there is no unitary operation U such that $\Lambda(\rho) = U\rho U^\dagger$ for all ρ.

   (c) [5] Prove that there is no qubit-to-qubit quantum channel χ such such that $\chi(\rho) = \Lambda(\rho)$ for all ρ. (Note: part (c) subsumes part (b), so a correct solution to (c) alone results in full marks for (b).)

4. **Searching with good guessing algorithm [12 points, 6 each].** Consider the search problem where, we are given a black box computing $f : \{0,1\}^n \to \{0,1\}$, and the goal is to find a satisfying input to f (i.e., an $x \in \{0,1\}^n$ such that $f(x) = 1$). But now suppose that, in addition to the black box for f, we may use a probabilistic "guessing procedure" g that produces a random $x \in \{0,1\}^n$ distributed as $\Pr[f(x) = 1] = p_x$, where

$$\sum_{\substack{x \in \{0,1\}^n \\ f(x)=1}} p_x = 1/4. \tag{1}$$

If g is run multiple times, it produces an independent sample from the same probability distribution for each run.

Intuitively, if $x \in \{0,1\}^n$ is repeatedly sampled using g, until an x such that $f(x) = 1$ occurs then the expected number of rounds (and calls to f) will be 4 (since there is a success probability 1/4 per round).

(a) Let $\epsilon > 0$ be given and suppose that we have the aforementioned guessing procedure g at our disposal. How many times must f be queried to produce a satisfying assignment to f with probability at least $1 - \epsilon$?

(b) Now, suppose that we are given a "quantum guessing procedure", which is an n-qubit unitary operation U_g, with the following property. For each $x \in \{0,1\}^n$, define $p_x = |\langle x|U_g|0^n\rangle|^2$ (so p_x is the probability of outcome x occuring if state $U_g|0^n\rangle$ is measured in the computational basis). Then the property of U_g is that the probabilities p_x ($x \in \{0,1\}^n$) satisfy the above equation, Eq. (1). Show how to find a satisfying assignment to f by making just one query to f, assuming that we have U_g and $U_g^\dagger$ at our disposal. (Note: as usual, a *query to f* is the unitary operation that, for all $x \in \{0,1\}^n$ and $b \in \{0,1\}$, maps $|x\rangle|b\rangle$ to $|x\rangle|f(x) \oplus b\rangle$.)

5. **Characterizing $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ [10 points, 5 each].** Suppose that Alice and Bob are each given one qubit of $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and *either* they both measure in the computational basis *or* they both measure in the Hadamard basis. Let $a, b \in \{0,1\}$ be their respective measurement outcomes. Note than $a = b$ holds in either case (computational basis or Hadamard basis).

(a) Show that $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is the *only* two qubit state with the above property (i.e., that the measurement outcomes of both of the above procedures satisfies $a = b$).

(b) Consider the variant of the above: *either* Alice measures in the computational basis and Bob in the Hadamard basis *or* vice versa. What are all the states that result in $a = b$ in both cases?