Fall 2012 QIC 890 / CO 781 Assignment 5

Due Nov 01, 2012 (in class)

Question 1. The optimal ensemble for $\chi(\mathcal{N})$. [6 marks]

Recall $\chi(\mathcal{N}) = \max_{p_x,\rho_x} S(\mathcal{N}(\sum_x p_x\rho_x)) - \sum_x p_x S(\mathcal{N}(\rho_x))$.

(a) [1 mark] Show that

$$\chi(\mathcal{N}) = \max_{\rho} S(\mathcal{N}(\rho)) - \max_{\rho} \min_{\substack{p_x,\rho_x:\\ \sum_x p_x\rho_x=\rho}} \sum_x p_x S(\mathcal{N}(\rho_x)).$$

Assume that for any ρ, the minimization of the second term above can be attained by some ensemble $\{p_x, \rho_x\}$ where there is no bound on the number of states in the ensemble.

(b) [1 mark] Show that there is some ensemble $\{q_t, |\psi_t\rangle\langle\psi_t|\}$ achieving the same minimum.

The Caratheodory's theorem says, for any set S in $\mathbb{R}^n$, if $a \in \text{conv}(S)$, then, a is a convex combination of some $n+1$ elements of S.

(c) [4 mark] Use Caratheodory's theorem to show that there is a distribution r_t such that $\{r_t, |\psi_t\rangle\langle\psi_t|\}$ attains the same minimum, but $r_t > 0$ for only d^2 values of r. (Hint available.)

Question 2. Nondegenerate stabilizer code for depolarizing channel [14 marks]

Let $\mathcal{P}_1 = \{I, X, Y, Z\}$ be the Pauli operators acting on 1 qubit. Here, $Y = XZ$.

Let $\mathcal{P}_n = \mathcal{P}_1^{\otimes n}$ be the Pauli operators acting on n qubits.

Throughout, for a Pauli operator Q, we count $\pm Q, \pm iQ$ as one operator. In particular, $|\mathcal{P}_n| = 4^n$.

For $P, Q \in \mathcal{P}_n$, let $f(P,Q) = \pm$ if $PQ = \pm QP$. (So, f denotes whether P, Q commute or anticommute.)

Let $G_1, G_2, \cdots, G_k \in \mathcal{P}_n \backslash \{I\}$ be k commuting Pauli operators that are *independent* (that is, no G_i is a product of the others). (These will be the generators of an $[[n, n-k]]$ stabilizer code.)

An $[[n, n-k]]$ stabilizer code $\mathcal{C}$ is the simultaneously $+1$ eigenspace of $G_1, \cdots, G_k$. It has 2^{n-k} dimensions.

Let $|\psi\rangle \in \mathcal{C}$.

If $E \in \mathcal{P}_n$ commutes with G_i, then $G_i E|\psi\rangle = EG_i|\psi\rangle = E|\psi\rangle$, so $E|\psi\rangle$ is a $+1$ eigenvector of G_i.

If $E \in \mathcal{P}_n$ anticommutes with G_i, then $G_i E|\psi\rangle = -EG_i|\psi\rangle = -E|\psi\rangle$, so $E|\psi\rangle$ is a -1 eigenvector of G_i.

The syndrome of E is the string of n symbols $(f(E, G_1), \cdots, f(E, G_k))$. Note, this is the outcome of measuring $G_1, G_2, \cdots, G_k$ on any state in $E\mathcal{C} = \{E|\psi\rangle : |\psi\rangle \in \mathcal{C}\}$.

(a) Show that $E_t, E_s \in \mathcal{P}_n$ have identical syndromes if and only if $E_t^\dagger E_s$ commutes with every G_i.

(b) Given any m independent Pauli operators $P_1, \cdots, P_m$, and a specific string $(s_1, \cdots, s_m) \in \{+,-\}^m$, show that the set $\{P \in \mathcal{P}_n : \forall i \;\; f(P, P_i) = s_i\}$ has size 2^{2n-m}. (For example, if $n = 3, m = 4, P_1 = XXI, P_2 = ZII, P_3 = IIY, P_4 = IIZ$, and $(s_1, s_2, s_3, s_4) = (+,+,-,-)$, then the set has $2^{6-4} = 4$ elements, $\{IIX, IXX, ZZX, ZYX\}$. (Hint available.)

(c) How many ways can we choose k independent commuting generators $G_1, G_2, \cdots, G_k$ in $\mathcal{P}_n$? (Hint: you can count the choices for G_1, then the remaining number of choices for G_2, etc.) (If you get a power of 2 for the answer, you forget to impose independence.)

(d) How many ways can we choose k independent commuting generators $G_1, G_2, \cdots, G_k$ in $\mathcal{P}_n$ such that each G_i commutes with a specific $E \in \mathcal{P}_n$, $E \neq I$?

(e) Given $E_s E_t \in \mathcal{P}_n$, if an $[[n, n-k]]$ stabilizer code is to be drawn at random, show that the probability (over the choice of the code) for E_s, E_t to have identical syndromes is no greater than 2^{-k}.

Let $\mathcal{N}(\rho) = q_I \rho + q_X X \rho X + q_Y Y \rho Y + q_Z Z \rho Z$, where $\vec{q} = (q_I, q_X, q_Y, q_Z)$ is a probability distribution on $\mathcal{P}_1$. Let $T_{n,\epsilon}$ denote the typical sequences for n iid draws of $\vec{q}$, and $\Pr(T_{n,\epsilon}) \geq 1 - \delta$. Let $\mathcal{T} \subset \mathcal{P}_n$ be the corresponding subset of typical Pauli operators in the Kraus decomposition of $\mathcal{N}^{\otimes n}$. Our goal is to correct the errors in $\mathcal{T}$.

(f) Use the union bound and part (e) to show that, given any $E_s \in \mathcal{P}_n$,

$$\Pr_{\mathcal{C}}(\exists E_t \in \mathcal{T} \text{ with same syndrome as } E_s) \leq 2^{n(H(\vec{q})+\epsilon)-k}.$$

(g) Conclude that the rate $\frac{n-k}{n} = 1 - H(\vec{q})$ is achievable for $\mathcal{N}$ using nondegenerate codes.

Each part carries 2 marks.

Hints:

For (1c) To show that there is an optimal ensemble of only d^2 pure states, start from any with minimal cardinality m, $\mathcal{E} = \{r_t, |\psi_t\rangle\langle\psi_t|\}$ with $r_t > 0$ for $t = 1, 2, \cdots, m$, and find a contradiction if $m > d^2$.

To do so, you will apply Caratheodory's theorem with $S = \{\mathcal{N}(|\psi_t\rangle\langle\psi_t|)\}$ at some point.

For (2b), associate X, Y, Z with $10, 11, 01$ respectively. Then every $P \in \mathcal{P}_n$ can be represented by a $2n$-bit string. Multiplication in $\mathcal{P}_n$ is associated with addition modulo 2 in $\mathbb{Z}_2^n$. You should check that commutation or anticommution relation of P with a fixed Pauli is a linear constraint in $\mathbb{Z}_2^n$.