Q. Inf. Science 3 (8.S372 / 18.S996) — Fall 2020

Assignment 6

Due: **Friday**, *Oct 16, 2020 at* ***5pm*** on canvas.

1. **Chernoff bound and Pinsker inequality.** In this problem you will derive the quantum Pinsker inequality and explore some applications.

   The Pinsker inequality is
   $$D(\rho\|\sigma) \geq \frac{1}{2\ln 2}\|\rho-\sigma\|_1^2. \tag{1}$$
   An important special case is for classical distributions over bits, where the Pinsker inequality implies
   $$D\left(\begin{pmatrix} p+\epsilon \\ 1-p-\epsilon \end{pmatrix} \middle\| \begin{pmatrix} p \\ 1-p \end{pmatrix}\right) \geq \frac{2}{\ln 2}\epsilon^2. \tag{2}$$
   As you saw on an earlier pset, the Pinsker inequality can also be related to the Chernoff bound, which is a way of showing that sums of many independent random variables are exponentially unlikely to be far from their mean. One version of this bound states that if $X_1, \ldots, X_n$ are i.i.d. random variables such that $\Pr[X_i = 1] = p$ and $\Pr[X_i = 0] = 1-p$, then
   $$\Pr\left(\frac{1}{n}\sum_{i=1}^n X_i \geq p+\epsilon\right) \leq e^{-2n\epsilon^2}. \tag{3}$$
   Derivations of (2) and (3) (not needed for the rest of the problem) can be found on wikipedia, and you may take these equations as given.

   (a) Prove (1). There are two possible routes. One is to use (3) and the quantum Stein's Lemma. Another is to use the monotonicity of relative entropy and (2). Pick one of these, or come up with another.

   (b) The Pinsker inequality can be used to derive approximate versions of various entropic conditions. Prove the following:

      i. If $S(\rho) \leq \epsilon$ then ρ is close in trace distance to a pure state, where "close" means the distance goes to 0 as $\epsilon \to 0$. [Hint: let $\rho = \sum_i \lambda_i \psi_i$ for $\lambda_1 \geq \lambda_2 \geq \cdots$ and show $D(\psi_1\|\rho) \leq S(\rho)$.]

      ii. If $I(A;B)_\rho \leq \epsilon$ then $\rho_{AB} \approx \rho_A \otimes \rho_B$ where again $\approx$ means close in trace distance. [Hint: show $I(A;B) = D(\rho_{AB}\|\rho_A \otimes \rho_B)$.]

      iii. For this last part, there is nothing to turn in. If $|H(A|B)| \leq \epsilon$ then there is no simple structural statement we can make (in the quantum case). Think about why this is true. We will later see that $I(A;B|C) \leq \epsilon$ implies a structural property about quantum states but this is very far from obvious.

2. **Remote state preparation** In remote state preparation (RSP), Alice has a classical description of a state $|\psi\rangle$ (denoted "ψ") and by using classical communication and entanglement, they end with Bob holding $|\psi\rangle$. This can be achieved by teleportation using 2 cbits and 1 ebit per qubit of $|\psi\rangle$ but asympototically this communication cost can be reduced nearly by a factor of 2.

   (a) *Equatorial states.* We say that a single-qubit state $|\psi\rangle$ is "equatorial" if it lies on the equator of the Bloch sphere, i.e. if there exists ϕ such that

   $$|\psi\rangle = \frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}. \tag{4}$$

   Show that $\psi + Z\psi Z = I$. Use this to construct a protocol in which

   - Alice and Bob begin with the state $|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (1 ebit).
   - Alice performs a two-outcome measurement with outcomes $\{M_0, M_1\}$ and obtains outcome $b \in \{0, 1\}$.
   - Alice transmits b to Bob using 1 cbit.
   - Bob performs the correction U_b and obtains the state $|\psi\rangle$.

   Find M_0, M_1, U_0, U_1. M_0, M_1 should depend on ψ but U_0, U_1 shouldn't; explain why this is true. (Hint: $M_0 = \psi, M_1 = Z\psi Z$ is not quite right but it is close.)

   (b) Now suppose $|\psi\rangle$ is an n-qubit state. Suppose that

   $$|\langle z|\psi\rangle|^2 = 2^{-n} \qquad \forall z \in \{0, 1\}^n. \tag{5}$$

   Show how a modification of the above protocol can be used to perform RSP for all states satisfying (5). This should be a single protocol in which Alice knows the identity of a state $|\psi\rangle$ satisfying (5) but Bob does not. It should use n cbits and n ebits.

   (c) It turns out there exist large subspaces containing only states that approximately satisfy (5), and that this can be used to construct an RSP protocol for an arbitrary high-dimensional state. However, there is a more direct argument that can yield RSP for arbitrary states. Let $S(\mathbb{C}^d)$ denote the unit vectors in $\mathbb{C}^d$. If $U_1, \ldots, U_n$ are $d \times d$ unitaries then we say they have the ϵ-randomizing property if,

   $$\forall |\psi\rangle \in S(\mathbb{C}^d), \qquad \left\| \frac{1}{n}\sum_{i=1}^{n} U_i \psi U_i^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\epsilon}{d}. \tag{6}$$

   We saw earlier that the generalized Paulis are a set of size $n = d^2$ that are $\epsilon = 0$-randomizing. It turns out that for $\epsilon > 0$, ϵ-randomizing sets exist of size $n = O(d/\epsilon^2)$.

   Show that given an ϵ-randomizing set of size n in d dimensions, there exists an RSP protocol for d dimensional states that consumes one copy of the state $|\Phi_d\rangle := \frac{1}{\sqrt{d}}\sum_{i=1}^{d} |i\rangle_A \otimes |i\rangle_B$, uses $\log(n)$ cbits, and incurs (trace distance) error $O(\epsilon)$. What is the asymptotic cbit cost per qubit if we use (a) the generalized Paulis; or (b) a set with $n = O(d/\epsilon^2)$?