Q. Inf. Science 3 (8.372 / 18.S996) — Fall 2022

Assignment 9

Due: **Friday**, *Dec 2, 2022 at* ***5pm*** on gradescope.

1. **Entanglement distillation with CSS codes**

   (a) First we consider the problem of *information reconciliation*. Suppose that Alice has a string $x \in \mathbb{Z}_2^n$ and Bob has a string y such that x is uniformly distributed on $\mathbb{Z}_2^n$ and each y_i is equal to x_i with probability $1-p$ and equal to x_i+1 with probability p. In other words $y = x + e$ where each e_i is an independent Bernoulli random variable with expectation p. This is the output we would get from sending x through n uses of a binary symmetric channel.

   The goal of information reconciliation is to exchange messages such that Alice and Bob end with shared strings x', y' that are equal to each other with high probability *and* are secret to any eavesdropper. To this end, suppose that Alice chooses a random matrix $A \in \mathbb{Z}_2^{k\times n}$ for some $k < n$, subject to the constraint that the k rows are linearly independent. Then she sends A and Ax to Bob through a public channel. Show that conditioned on A and Ax, Alice's state has $n-k$ bits of entropy. (Hint: it should be uniformly distributed over a dimension-$n-k$ affine subspace of $\mathbb{Z}_2^n$. An affine space is a set of the form $x_0 + S = \{x_0 + x : x \in S\}$ where S is a linear subspace of $\mathbb{Z}_2^n$.) Next show that if $k = nR$ for some $R > H_2(p)$ then Bob can use this message to determine the exact value of e with high probability. Explain how this gives rise to a secrecy distillation protocol that can extract secret bits at rate asymptotically equal to $1 - H_2(p)$.

   (b) Now we turn to entanglement. Suppose that Alice generates n copies of $|\Phi_2\rangle$ and sends half of each copy through the channel $\mathcal{N}_X$, defined as

   $$\mathcal{N}_X(\rho) = (1-p)\rho + pX\rho X. \tag{1}$$

   Thus Alice and Bob share $\rho^{\otimes n}$ where $\rho = (\mathrm{id}\otimes\mathcal{N}_X)(\Phi_2)$. As in the classical case, Alice generates a random matrix $A \in \mathbb{Z}_2^{k\times n}$ (uniformly random subject to the constraint that rows are linearly independent) and sends this to Bob through a classical channel. For each row $A_i = (A_{i,1}, \ldots, A_{i,n})$ Alice measures the observable

   $$Z^{A_i} := Z_1^{A_{i,1}} Z_2^{A_{i,2}} \cdots Z_n^{A_{i,n}} \tag{2}$$

   obtaining outcome $(-1)^{s_i}$ for $s_i \in \{0,1\}$. She also sends the outcomes $s_1, \ldots, s_k$ to Bob. Then Bob also measures $Z^{A_1}, \ldots, Z^{A_k}$. Again assume $k = nR$ for $R > H_2(p)$. Show that the post-measurement state is close to a pure state of the form

   $$(I \otimes X^e)\,|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{x\in S} |x, x+e\rangle \tag{3}$$

   where S is a subspace of $\mathbb{Z}_2^n$. How many copies of $|\Phi_2\rangle$ can $(I\otimes X^e)\,|S\rangle$ be converted into using local unitaries?

(c) Now suppose that each of n copies of $|\Phi_2\rangle$ are sent first through $\mathcal{N}_X$ and then through $\mathcal{N}_Z$, defined as

$$\mathcal{N}_Z(\rho) = (1-p)\rho + pZ\rho Z. \tag{4}$$

Thus Alice and Bob share $\rho^{\otimes n}$ where $\rho = (\mathrm{id} \otimes \mathcal{N}_Z \circ \mathcal{N}_X)(\Phi_2)$. The combination $\mathcal{N}_Z \circ \mathcal{N}_X$ is not exactly the same as the depolarizing channel since it results in X with probability p, Z with probability p and Y with probability p^2 but it is a reasonable proxy for the depolarizing channel.

The entanglement distillation protocol from (b) is now modified as follows. First Alice follows the same steps as in (b). Then she chooses another random matrix $B \in \mathbb{Z}_2^{k\times n}$ that is uniformly distributed subject to its rows being linearly independent and the constraints $AB^T = 0$. Now for each $i = 1, \ldots, k$ Alice measures X^{B_i}, obtaining outcomes $(-1)^{t_1}, \ldots, (-1)^{t_k}$. She transmits B and t to Bob. Then Bob also measures $Z^{A_1}, \ldots, Z^{A_k}$ and $X^{B_1}, \ldots, X^{B_k}$. Again we assume $k = nR$ for $R > H_2(p)$. Show that the post-measurement state is close to a pure state of the form $(I \otimes Z^f X^e)\,|S\rangle$ where $e, f \in \mathbb{Z}_2^n$ and $|S\rangle$ is defined as in (3).

(d) Calculate $I_c = S(B) - S(E)$ for the states from (b) and (c), i.e. $(\mathrm{id} \otimes \mathcal{N}_X)(\Phi_2)$ and $(\mathrm{id} \otimes \mathcal{N}_Z \circ \mathcal{N}_X)(\Phi_2)$. How does this compare with the entanglement distillation rates achieved by the above protocols?

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

The Pinsker inequality is

$$D(\rho\|\sigma) \geq \frac{1}{2\ln 2}\|\rho - \sigma\|_1^2. \tag{5}$$

An important special case is for classical distributions over bits, where the Pinsker inequality implies

$$D\left(\begin{pmatrix} p+\epsilon \\ 1-p-\epsilon \end{pmatrix} \middle\| \begin{pmatrix} p \\ 1-p \end{pmatrix}\right) \geq \frac{2}{\ln 2}\epsilon^2. \tag{6}$$

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

$$\Pr\left(\frac{1}{n}\sum_{i=1}^n X_i \geq p + \epsilon\right) \leq e^{-2n\epsilon^2}. \tag{7}$$

Derivations of (6) and (7) (not needed for the rest of the problem) can be found on wikipedia, and you may take these equations as given.

(a) *[Optional:]* Prove (5). There are two possible routes. One is to use (7) and the quantum Stein's Lemma. Another is to use the monotonicity of relative entropy and (6). 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.

3. **Monogamy of entanglement**

(a) The principle of *monogamy of entanglement* is that entanglement cannot be shared without limit, unlike classical correlations. However, the larger the local dimension, the more systems can be be simultaneously entangled. We will start with an example of this phenomenon. Let

$$|\psi\rangle_{A_1,\ldots,A_n} = \frac{1}{\sqrt{n!}} \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \, |\pi_1\rangle \otimes |\pi_2\rangle \otimes \cdots |\pi_n\rangle \in (\mathbb{C}^n)^{\otimes n}. \tag{8}$$

Here S_n is the symmetric group, meaning the set of $n!$ permutations of n objects. The sign of a permutation $\operatorname{sgn}(\pi) = (-1)^m$ where m is the number of transpositions (swaps of two elements) in any decomposition of π. Let $\psi_{A_1A_2} := \operatorname{tr}_{A_3 \ldots A_n}[\psi]$. We will show that $\psi_{A_1A_2}$ is far from $\operatorname{Sep}(n,n)$. To show this, let $M = (I - F)/2$, where F is the SWAP operator on $\mathbb{C}^n \otimes \mathbb{C}^n$. Show that $\operatorname{tr}[M\psi_{A_1A_2}] = 1$ and $\operatorname{tr}[M\sigma] \leq 1/2$ for any $\sigma \in \operatorname{Sep}(n,n)$.

(b) Despite the above example, nontrivial statements about monogamy can be made when the number of systems is only logarithmic in the local dimension. This will follow from some information-theory tools that we now develop. Let $I(A:B|X)_\rho = \epsilon$ and suppose that X is classical while A, B are quantum. Show that there exists a separable state σ_{AB} such that $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_1 \leq \sqrt{\epsilon 2 \ln(2)}$. (Hint: you should review problem 2(b) from this pset.)

(c) Consider the state $\rho^{AB_1 \ldots B_k}$, where A has dimension d_A and each B_i has dimension d_B. Let $\{M, I - M\}$ be a 1-LOCC measurement on two systems A and B, meaning that it can be written as a measurement on system B followed by a two-outcome measurement on system A, i.e.

$$M = \sum_{y=1}^{m} Q_y \otimes R_y, \tag{9}$$

where each $R_y \geq 0$, $\sum_{y=1}^m R_y = I$ and $0 \leq Q_y \leq I$. It turns out that most of the ρ^{AB_i} are close to Sep when measured with M of this form. To see this, consider the state $\sigma^{AY_1 \ldots Y_k}$ where we measure each system B_i for $i = 1, \ldots, k$ using the

measurement $\{R_1, \ldots, R_m\}$ and we record the answer in a classical system Y_i. Let $Y_{<i} := Y_1 Y_2, \ldots, Y_{i-1}$. Show that

$$\sum_{i=1}^{k} I(A : Y_i | Y_{<i})_\sigma \leq \log(d_A). \tag{10}$$

(d) *[Optional:]* Given ρ and M as above, define $h_{\mathrm{Sep}}(M) = \max\{\operatorname{tr} M\sigma : \sigma \in \mathrm{Sep}(d_A, d_B)\}$. Show that

$$\mathop{\mathbb{E}}_{i \in [k]} \operatorname{tr}\left[M \rho^{AB_i}\right] \leq h_{\mathrm{Sep}}(M) + \sqrt{\frac{2\ln(d_A)}{k}}. \tag{11}$$

This shows a nontrivial monogamy relation when the number of systems is only logarithmic in the local dimension. On the other hand, it applies only to a restricted family of measurements. Hint: you may want to relate $I(A : Y_i|Y_{<i})$ to the states of ρ resulting from measuring some subsystems and conditioning on the outcomes, while leaving other systems unmeasured or traced out.

4. **Data hiding, continued**

(a) **Separable Werner states.** As in the last pset, define the symmetric/antisymmetric projectors $\Pi_\pm = (I \pm F)/2$ on $\mathbb{C}^d \otimes \mathbb{C}^d$ (with $F = \mathrm{SWAP}$) and the *Werner state*

$$W_\lambda := \lambda \frac{\Pi_+}{d(d+1)/2} + (1-\lambda)\frac{\Pi_-}{d(d-1)/2} \tag{12}$$

Previously we saw that W_λ is PPT for $\lambda \geq 1/2$, meaning that it is entangled for $\lambda < 1/2$. However, we need an additional argument to show that W_λ is separable for $\lambda \geq 1/2$. Prove this by giving explicit decompositions of W_λ into product states for all $\lambda \in [1/2, 1]$. As a hint, try computing $\mathbb{E}[(U \otimes U)(\alpha \otimes \beta)(U \otimes U)^\dagger]$ for pure states α, β.

(b) **Form of the optimal measurement.** Suppose that we would like to distinguish $\rho_0 := W_{\lambda_0}$ and $\rho_1 := W_{\lambda_1}$. (These λ_0, λ_1 could be $0, 1$ as in the last pset, or $1/2, 1$ if we want to consider the problem of distinguishing separable states.) Then we perform a a 2-outcome measurement $\{M_0, M_1\}$ and seek to maximize $p_0 := \operatorname{tr} M_0 \rho_0$ and $p_1 := \operatorname{tr} M_1 \rho_1$. This is a two-objective optimization; rather than a single optimal value, there is a feasible region of possible (p_0, p_1). Show that any feasible p_0, p_1 can be achieved by M_0, M_1 that are linear combinations of I and F. (*Hint: Do not try to determine which (p_0, p_1) are feasible.*)

(c) **Composability.** In the last part, if λ_0, λ_1 are not $0, 1$—say if we choose them to be $1/2, 1$—then ρ_0, ρ_1 are not orthogonal, so we cannot distinguish the states perfectly even with collective measurements. To remedy this, let $\rho_0 = W_{\lambda_0}^{\otimes n}$ and $\rho_1 = W_{\lambda_1}^{\otimes n}$ so that $F(\rho_0, \rho_1)$ decays exponentially with n. Show that now any feasible p_0, p_1 can be acheived by M_0, M_1 that are linear combinations of the 2^n operators $I \otimes I \otimes \cdots \otimes I$, $I \otimes I \otimes \cdots \otimes F$, $\ldots$ $F \otimes F \otimes \cdots \otimes F$.