Q. Inf. Science 3 (8.372) — Fall 2024

Assignment 8

Due: **Tuesday**, *Nov 5, 2024 at* ***9pm***

Turning in your solutions: Upload a single pdf file to gradescope.

1. **Separable data hiding using Werner states.** In class we argued that random unitaries could yield data-hiding states. In this problem you will derive an explicit, although less efficient, construction of data hiding.

   For a bipartite state $\rho_{AB} = \sum_{ijkl} (\rho_{AB})_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l|$ define the *partial transpose*

   $$\rho^\Gamma := (\mathrm{id} \otimes T)(\rho) = \sum_{ijkl} (\rho_{AB})_{ijkl} |i\rangle\langle j| \otimes |l\rangle\langle k| \tag{1}$$

   We say that a state ρ is PPT if $\rho^\Gamma \geq 0$.

   Let $F = \mathrm{SWAP}$ act on $\mathbb{C}^d \otimes \mathbb{C}^d$ and define the projectors $\Pi_\pm = (I \pm F)/2$. These are called the symmetric and antisymmetric projectors respectively. Define the *Werner state*

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

   (a) **Separable Werner states.** On an 8.371 pset you may have seen that W_λ is PPT for $\lambda \geq 1/2$, meaning that it is entangled for $\lambda < 1/2$. (If you haven't seen this before, then don't worry.) Here you will argue that W_λ is separable for $\lambda \geq 1/2$. A state is "separable" if it is a convex combination of product states.

   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 $\rho_1 := W_{\lambda_1}$. (Later we will take λ_0, λ_1 to be $0, 1$ or $1/2, 1$, but this part will not depend on that.) Then we perform a a 2-outcome measurement $\{M_0, M_1\}$ and seek to maximize $p_0 := \mathrm{tr}\, M_0 \rho_0$ and $p_1 := \mathrm{tr}\, M_1 \rho_1$. 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) **Data hiding.** For this part we will take $\lambda_0 = 0$ and $\lambda_1 = 1$. Define the *bias* of the measurement to be

   $$\delta := \mathrm{tr}\, M_0 W_0 + \mathrm{tr}\, M_1 W_1 - 1. \tag{3}$$

   Show that $\delta \leq O(1/d)$ for LOCC measurements but $\delta = 1$ is possible for unrestricted measurements. Show also that $\delta = O(1/d)$ is achievable by measuring both systems in the basis $\{|1\rangle, \ldots, |d\rangle\}$ and checking whether the answers agree.

(d) **Composability.** Now take $\lambda_0 = 1/2$ and $\lambda_1 = 1$. This way we are dealing with entirely separable states. However, now $W_{1/2}$ and W_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 $I \otimes I \otimes \cdots \otimes I$, $I \otimes I \otimes \cdots \otimes F$, ... $F \otimes F \otimes \cdots \otimes F$.

2. **Monogamy of entanglement** Let $\mathcal{D}_d$ denote the set of d-dimensional density matrices and define the separable states to be

$$\mathrm{Sep}(d_A, d_B) = \mathrm{conv}\left\{\alpha \otimes \beta : \alpha \in \mathcal{D}_{d_A}, \beta \in \mathcal{D}_{d_B}\right\} \tag{4}$$

where $\mathrm{conv}\, S$ denotes the convex hull of a set S, meaning

$$\mathrm{conv}\, S = \left\{\sum_i p_i x_i : x_i \in S, p \text{ a probability distribution}\right\} \tag{5}$$

(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 simultaneously entangled. We will start with an example of this phenomenon. Let

$$|\psi\rangle_{A_1,\ldots,A_n} = \frac{1}{\sqrt{n!}} \sum_{\pi \in S_n} \mathrm{sgn}(\pi)\, |\pi_1\rangle \otimes |\pi_2\rangle \otimes \cdots |\pi_n\rangle \in (\mathbb{C}^n)^{\otimes n}. \tag{6}$$

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

(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 $\|\rho_{AB} - \sigma_{AB}\|_1 \leq \sqrt{\epsilon 2 \ln(2)}$. (Hint: you should review problem 2(b) from pset 6.)

(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.

$$M = \sum_{y=1}^{m} Q_y \otimes R_y, \tag{7}$$

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

$$\sum_{i=1}^{k} I(A : Y_i | Y_{<i})_\sigma \leq \log(d_A). \tag{8}$$

(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

$$\mathop{\mathbb{E}}_{i \in [k]} \operatorname{tr}\left[M \rho^{AB_i}\right] \leq h_{\mathrm{Sep}}(M) + \sqrt{\frac{2 \ln(d_A)}{k}}. \tag{9}$$

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.