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

Assignment 8

Due: **Friday**, *Nov 13, 2020 at* ***5pm*** on canvas.

1. **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 $F = \text{SWAP}$) and the *Werner state*

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

   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 $I \otimes I \otimes \cdots \otimes I$, $I \otimes I \otimes \cdots \otimes F$, $\ldots$ $F \otimes F \otimes \cdots \otimes F$.

2. **Measure concentration**

(a) Let $z \in N_{\mathbb{C}}(0,1)$, meaning $z = x + iy$ with $x, y \in N(0, 1/2)$. For $\gamma \geq 0$, calculate $\Pr[|z|^2 \geq t]$ and the associated density $p(t) = -\frac{\mathrm{d}}{\mathrm{d}t}\Pr[|z|^2 \geq t]$. Use this to calculate $\mathbb{E}[e^{\lambda |z|^2}]$. Note that this becomes ∞ for large enough λ. Think about why this is but you don't need to write your answer.

(b) Let $|\gamma\rangle \in \mathbb{C}^{d_A d_B}$ be a complex Gaussian vector with mean zero and variance such that $\mathbb{E}[|\gamma\rangle\langle\gamma|] = I/d_A d_B$. Let $|\alpha\rangle \in \mathbb{C}^{d_A}$ be a unit vector. Compute $\mathbb{E}[\exp(\lambda \operatorname{tr}[\alpha\gamma_A])]$. Show that for $0 < \epsilon \leq 1$,

$$\Pr\left[\operatorname{tr}[\alpha\gamma_A] \geq \frac{1+\epsilon}{d_A}\right] \leq e^{-c_1 d_B \epsilon^2} \tag{2}$$

for some constant $c_1 > 0$. As a hint, you should find that the optimal λ is $d_A d_B(1 - (1+\epsilon)^{-1})$. You may use without proof the fact that $\epsilon - \ln(1+\epsilon) \geq \epsilon^2/6$.

(c) Let $|\psi\rangle \in \mathbb{C}^{d_A d_B}$ be a random unit vector. Show that ψ satisfies the same bound as (2), i.e. that

$$\Pr\left[\operatorname{tr}[\alpha\psi_A] \geq \frac{1+\epsilon}{d_A}\right] \leq e^{-c_1 d_B \epsilon^2} \tag{3}$$

(d) Assume that $d_A \leq d_B$. We know from random matrix theory that $\|\gamma_A\|_\infty \approx (1 + \sqrt{d_A/d_B})^2/d_A$. We will use simpler arguments to achieve this bound up to the constant factor in front of $\sqrt{d_A/d_B}$. Suppose $d_B = c_2 d_A/\epsilon^2$ for some $c_2 > 0$. Show that $\|\psi_A\|_\infty \leq (1+\epsilon)/d_A$ with high probability. Do this by first showing that with high probability $\operatorname{tr}\hat{\alpha}\psi_A \leq (1+\epsilon)/d_A$ for all $\hat{\alpha}$ in a δ-net on $\mathbb{C}^d$, with $\delta = 1/2$. You may want to use the fact that if $\operatorname{tr} X = 0$ then $\operatorname{tr} X\psi_A = \operatorname{tr} X(\psi_A - I/d) \leq \|X\|_1 \|\psi_A - I/d\|_\infty$. If you don't see how to prove this, show the bound for $d_B = c_2 d_A \log(d_A/\epsilon)/\epsilon^2$ using a $O(\epsilon/d_A)$-net for partial credit.