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

## Assignment 8

*Due:* **Friday**, *Nov 4, 2022 at* ***5pm*** *on gradescope.*

1. **PPT test and Werner states** 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 $\rho$ is PPT if it has Positive [semi-definite] Partial Transpose, i.e. if $\rho^\Gamma \geq 0$. We saw in lecture that all separable states are PPT.

(a) The transpose is a basis-dependent operation. However, show that the set PPT is invariant under local unitaries, i.e. if $\rho \in \mathrm{PPT}$ then $(U \otimes V)\rho(U \otimes V)^\dagger \in \mathrm{PPT}$ as well. (You will not need it here but your proof should work even if $U, V$ are not unitary.)

(b) Let $F$ denote the SWAP operator, i.e. $F = \sum_{i,j} |i,j\rangle \langle j,i|$. Define the projectors $\Pi_\pm = (I \pm F)/2$ on $\mathbb{C}^d \otimes \mathbb{C}^d$. These are called the symmetric and antisymmetric projectors respectively. Verify that $\mathrm{tr}\, \Pi_\pm = d(d \pm 1)/2$. Define the *Werner state*

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

Calculate $F^\Gamma$ and $W_\lambda^\Gamma$. For which values of $\lambda$ is $W_\lambda \in \mathrm{PPT}$?

(c) We say a channel $\mathcal{N}_{A' \to B}$ is PPT if its Jamiolkowski state $\omega(\mathcal{N})$ is in PPT. For what values of $p, d$ is the depolarizing channel $\mathcal{D}_p^d(\rho) = (1-p)\rho + p\frac{I}{d}$ PPT?

(d) Show that if $\rho$ is a PPT state and $|\Phi_d\rangle = d^{-1/2} \sum_{i=1}^d |i\rangle \otimes |i\rangle$ then $\mathrm{tr}[\Phi_d \rho] \leq 1/d$. Along the way you may find it helpful to show that $\mathrm{tr}\left[A^\Gamma B^\Gamma\right] = \mathrm{tr}[AB]$. Recall also the bound $\mathrm{tr}[AB] \leq \|A\|_1 \|B\|_\infty$.

(e) Consider now the problem of distinguishing the Werner states $W_0$ and $W_1$ using LOCC (local operations and classical communication). The measurement consists of operators $\{M_0, M_1\}$ such that $0 \leq M_0$, $0 \leq M_1$ and $M_0 + M_1 = I$. It turns out that if $\{M_0, M_1\}$ can be implemented using LOCC then it should additionally satisfy $M_0^\Gamma \geq 0$ and $M_1^\Gamma \geq 0$.

We can further restrict the form of $M_0, M_1$ using symmetry. Show that $F$ commutes with $U \otimes U$ for all $U \in \mathcal{U}(d)$ and therefore that $W_\lambda$ does as well. It turns out that this allows us to show that $M_0, M_1$ are (without loss of generality) linear combinations of $I$ and $F$, i.e.

$$M_0 = aI + bF \quad \text{and} \quad M_1 = (1-a)I - bF \tag{3}$$

for $a, b \in \mathbb{R}$. (Both "it turns out" facts in this problem are non-trivial but will be discussed in lecture.) Define the *bias* of the measurement to be

$$\delta := \operatorname{tr} M_0 W_0 + \operatorname{tr} M_1 W_1 - 1. \tag{4}$$

(If the probability of guessing the state correctly is $p$ then $\delta = 2p - 1$.)

Show that $\delta \leq O(1/d)$ for LOCC measurements but $\delta = 1$ is possible for unrestricted measurements. Along the way you should give conditions for which values of $a, b$ yield valid measurements (i.e. satisfy $M_0 \geq 0$ and $M_1 \geq 0$) as well as satisfying the additional LOCC condition: $M_0^\Gamma \geq 0$ and $M_1^\Gamma \geq 0$. 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.

As a result we call the Werner states *data hiding* states since they can be used to hide a bit in a way that is concealed from LOCC measurements but accessible to general measurements.