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

Assignment 7

Due: **Friday**, *Oct 23, 2020 at* ***5pm*** on canvas.

1. **PPT test and 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 ρ is PPT if it has Positive [semi-definite] Partial Transpose, i.e. if $\rho^\Gamma \geq 0$.

(a) Show that Sep $\subseteq$ PPT, i.e. that for any separable σ we have $\sigma^\Gamma \geq 0$. Since the PPT condition can be checked efficiently, we can sometimes use the set PPT as an approximation for the set Sep.

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

(c) Show that for pure state $\psi = |\psi\rangle\langle\psi|$, $\psi \in$ PPT if and only if $\psi \in$ Sep, i.e. if $|\psi\rangle$ is a product state. (Hint: use (b) to rotate $|\psi\rangle$ into its Schmidt basis, then observe that ψ^Γ can be broken into 2×2 blocks. You may also want to use the definition of a PSD matrix where if M is PSD, then $\langle\psi| M |\psi\rangle > 0 \; \forall |\psi\rangle$.)

(d) Define the projectors $\Pi_\pm = (I \pm \mathrm{SWAP})/2$ 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 SWAP^Γ and W_λ^Γ. For which values of λ is $W_\lambda \in$ PPT?

(e) 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?

(f) Show that if ρ 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 $\mathrm{tr}[AB] \leq \|A\|_1 \|B\|_\infty$.

(g) [Optional] 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 SWAP commutes with $U \otimes U$ for all $U \in \mathcal{U}(d)$ and therefore that W_λ 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 SWAP, i.e. $M_0 = aI + b\,\text{SWAP}$ and $M_1 = (1-a)I - b\,\text{SWAP}$ 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

$$\delta := \frac{\operatorname{tr} M_0 W_0 + \operatorname{tr} M_1 W_1 - 1}{2}. \tag{3}$$

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. 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.

2. **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

$$\mathcal{N}_X(\rho) = (1 - p)\rho + pX\rho X. \tag{4}$$

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

$$Z^{A_i} := Z_1^{A_{i,1}} Z_2^{A_{i,2}} \cdots Z_n^{A_{i,n}} \tag{5}$$

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

$$(I \otimes X^e) |S\rangle := \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x, x + e\rangle \tag{6}$$

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

$$\mathcal{N}_Z(\rho) = (1 - p)\rho + pZ\rho Z. \tag{7}$$

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 (6).