Quantum Information Theory
Series 13

HS 14
Dr. J.M. Renes

Exercise 13.1 Quantum One-time Pad

The quantum one-time pad encrypts a one qubit message ρ with two bits of key k_1, k_2 as

$$\mathcal{E}_{k_1,k_2}(\rho) = X^{k_1} Z^{k_2} \rho Z^{k_2} X^{k_1}.$$

For any purification $|\psi\rangle_{AB}$ of ρ_A, the mixture over all possible keys is then

$$\frac{1}{4}\sum_{k_1,k_2} \mathcal{E}_A \otimes \mathcal{I}_B \left(|\psi\rangle\langle\psi|_{AB}\right) = \tau_A \otimes \rho_B, \tag{1}$$

where τ_A is the fully mixed state and $\rho_B = \mathrm{tr}_A \left(|\psi\rangle\langle\psi|_{AB}\right).$
Show that using two bits of key per qubit of message is optimal, i.e., for any alternative (but reversible) definition of the encryption operation $\mathcal{E}_k$, (1) can only be satisfied for any state $|\psi\rangle$ if the key k is at least 2 bits.

Exercise 13.2 Data hiding

Suppose you have two agents, Alice and Bond, at your service. You want them to deliver a secret (classical) message to your ally Charlie. You will give Alice and Bond two different states (i.e. an encryption of your message), so that they cannot extract the secret message unless they are physically together. Specifically, data hiding is what you want: states that are easily distinguishable by doing a certain class of operations, such as a global measurement on Alice and Bond's systems together, but they are nearly indistinguishable under a different, restricted class of operations, such as local operations and classical communication (LOCC). Formally, we say that a family of states $\left\{\rho^i\right\}_i$ is ε-secure under a set of operations $\mathbb{E}$ if

$$\delta(\mathcal{E}(\rho^i), \mathcal{E}(\rho^j)) < \varepsilon, \quad \forall i, j, \quad \forall \mathcal{E} \in \mathbb{E}.$$

In this exercise we will consider a data hiding scheme which is secure under LOCC and so the original message can only be recovered if global measurements on the joint system are allowed. Consider a $2d$-qubit Hilbert space, $\mathcal{H}_A \otimes \mathcal{H}_B$, and the computational basis of both spaces. Consider the projectors onto the symmetric and antisymmetric subspaces of $\mathcal{H}_A \otimes \mathcal{H}_B$,

$$\begin{aligned}\Pi^S &= \frac{1}{2}\sum_{i<j}\Big(|i\rangle_A|j\rangle_B + |j\rangle_A|i\rangle_B\Big)\Big(\langle i|_A\langle j|_B + \langle j|_A\langle i|_B\Big) + \sum_i |i\rangle_A|i\rangle_B\langle i|_A\langle i|_B,\\ \Pi^A &= \frac{1}{2}\sum_{i<j}\Big(|i\rangle_A|j\rangle_B - |j\rangle_A|i\rangle_B\Big)\Big(\langle i|_A\langle j|_B - \langle j|_A\langle i|_B\Big).\end{aligned}$$

You will encode only one bit of information, b, giving Alice and Bond each their $d-$qubit part of ρ^b_{AB}, with

$$\rho^{b=0} = \frac{2}{d(d+1)}\Pi^S, \qquad \rho^{b=1} = \frac{2}{d(d-1)}\Pi^A.$$

a) Show that $\rho^{b=0}$ and $\rho^{b=1}$ are valid density operators and explain how you would proceed to recover b if you had access to Alice and Bond's systems (together).

b) Consider the flip operator in basis $\{|i\rangle_A|j\rangle_B\}_{ij}$,

$$F = \Pi^S - \Pi^A = \sum_{i,j} |i\rangle_A|j\rangle_B\langle j|_A\langle i|_B.$$

Show that, for all operators $M_A \in \mathrm{End}(\mathcal{H}_A), N_B \in \mathrm{End}(\mathcal{H}_B)$, $\mathrm{Tr}[F(M_A \otimes N_B)] = \mathrm{Tr}(M_A N_B)$. In particular, for all pure states $|x\rangle_A, |y\rangle_B$, $\mathrm{Tr}[F|xy\rangle\langle xy|] = |\langle x|y\rangle|^2$.

c) Suppose that Alice and Bond perform local projective measurements in arbitrary bases, $\{|x\rangle_A\}$ and $\{|y\rangle_B\}$ respectively. We denote the joint probability distribution of the outcomes P_{XY} when they measure state $\rho^{b=0}$ and Q_{XY} when they measure $\rho^{b=1}$. We want them to be unable to distinguish the two distributions, so we want to show that $\delta(P_{XY}, Q_{XY})$ is small. Remember that

$$P_{XY}(x, y) = \mathrm{Tr}(|xy\rangle\langle xy|\rho^{b=0}), \quad Q_{XY}(x, y) = \mathrm{Tr}(|xy\rangle\langle xy|\rho^{b=1}).$$

Use the results from *b)* to show that $\delta(P_{XY}, Q_{XY}) \leq \frac{2}{d+1}$.

Hint: Start from the trace distance as $\delta(P_{XY}, Q_{XY}) = \sum_{x,y\in\mathcal{S}} P_{XY}(x, y) - Q_{XY}(x, y)$, with $\mathcal{S} = \{(x, y) : P_{XY}(x, y) > Q_{XY}(x, y)\}$.