Quantum Information Theory, Spring 2020

Practice problem set #5

You do **not** have to hand in these exercises, they are for your practice only.

1. **Fidelity and trace distance:** For any ρ, $\sigma \in D(\mathcal{H})$, prove that $T(\rho, \sigma) \leqslant \sqrt{1 - F(\rho, \sigma)^2}$. This is one of the Fuchs-van de Graaf inequalities.

   Hint: Use Uhlmann's theorem and the monotonicity property of the trace distance.

2. **Classical-quantum states:** Let $\mathcal{H}_X = \mathbb{C}^\Sigma$. We say that a state ρ_{XB} is *classical on subsystem* X or a *classical-quantum state* if it can be written in the form

   $$\rho_{XB} = \sum_{x \in \Sigma} p(x) \, |x\rangle\langle x| \otimes \rho_{B,x}$$

   for a probability distribution p on Σ and states $\rho_{B,x}$. By convention, we will always denote subsystems by $X, Y, \ldots$ if we know them to be classical (and $A, B, \ldots$ otherwise).

   (a) Discuss how this generalizes the notion of classical states.
   (b) Show that ρ_{XB} is classical on subsystem X if and only if $(\Delta_X \otimes \mathcal{I}_B)[\rho_{XB}] = \rho_{XB}$, where $\Delta_X[M] = \sum_{x \in \Sigma} |x\rangle\langle x|M|x\rangle\langle x|$ is the completely dephasing channel on the X-system.
   (c) Let $\Phi_{A \to X}$ be the channel corresponding to a measurement μ_A, as on the previous homework. Show that, for any system B and any state ρ_{AB}, the state $\rho_{XB} = (\Phi_{A \to X} \otimes \mathcal{I}_B)\,[\rho_{AB}]$ is a classical-quantum state and compute the probabilities $p(x)$ and the states $\rho_{B,x}$.

3. **How to compress it?** Suppose you would like compress an IID source. In class we showed how such a source can in principle be compressed by using typical sets. Discuss how this can be applied in practice. What parameters have to be fixed? How do the encoder and decoder work? What if you don't know the distribution of symbols emitted by the source? Is this a *practical* way of compressing?

4. **Lossy vs. lossless compression:** In class, we mostly discussed *lossy* compression protocols which compress any input sequence into a fixed number of bits but may fail with some small probability. In practice, it is also interesting to consider *lossless* compression protocols that use a variable number of bits (depending on the input sequence) and never fail.

   Given an (n, R, δ)-code, which achieves lossy compression, can you construct a lossless compression protocol with average rate $\approx R$ (for large n and small δ)?

5. **Lexicographic order (for the bonus problem):** The lexicographic order $\leqslant_{\text{lex}}$ on $\{0, 1\}^n$ is defined as follows: Given bitstrings x^n and y^n, we let $x^n \leqslant_{\text{lex}} y^n$ if either $x^n = y^n$ or $x_i < y_i$ for the smallest i such that $x_i \neq y_i$. For example, `001` $\leqslant_{\text{lex}}$ `010`. The lexicographic order defines a total order on $\{0, 1\}^n$, hence also on the bitstrings of length n with k ones, which we denote by $B(n, k)$.

   (a) Write down $B(5, 2)$ in lexicographic order (smallest element first).

(b) How can you recursively compute the m-th element of $B(n, k)$?

(c) How can you recursively compute the index of a given element in $B(n, k)$?

Hint: $|B(n, k)| = \binom{n}{k}$. *Moreover,* $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ *for all* $1 \leqslant k \leqslant n - 1$.