Q. Inf. Science 3 (8.372) — Fall 2024

Assignment 2

Due: **Tuesday**, *Sep 24, 2024 at* ***9pm***

Turning in your solutions: Upload a single pdf file (typed or neatly handwritten) to gradescope.

Collaboration policy: You may work individually or together in small groups but should write up your solutions individually. You can use psetpartners.mit.edu to find partners if you don't already know people in the class.

1. **Gentle measurement.** Suppose we perform a two-outcome measurement $\{M, I-M\}$ with $0 \leq M \leq I$. This does not uniquely define the post-measurement states, but we will assume that when the first outcome occurs, ρ is mapped to

$$\sigma := \frac{\sqrt{M}\rho\sqrt{M}}{\mathrm{tr}[M\rho]}. \tag{1}$$

(This happens with probability $\mathrm{tr}[M\rho]$.) Quantum measurements can sometimes cause significant disturbance, so it is possible that σ is far from ρ, but this turns out not to happen when $\mathrm{tr}[M\rho]$ is close to 1.

(a) Prove that

$$F(\rho, \sigma) \geq \sqrt{\mathrm{tr}\, M\rho}. \tag{2}$$

Hint: Can you show that $\sqrt{M} \geq M$?

(b) Suppose that $M = \Pi^n_{\rho,\delta}$ satisfies $\mathrm{tr}[M\rho^{\otimes n}] \geq 1 - \epsilon$. In Schumacher compression we apply the measurement $\{M, I - M\}$ to one half of $|\phi_\rho\rangle^{\otimes n}$ and we say that we have succeeded if we obtain outcome M. (The other details of the protocol do not matter for this problem.) What can you say about the trace distance between the initial state and the post-measurement state, assuming the measurement outcome is M?

2. **Types.** Given a sequence $x^n = x_1, x_2, \ldots, x_n \in [d]^n$ and a symbol $a \in [d]$, let $N(a|x^n)$ be the number of occurrences of a in x^n. The *type* (or empirical probability distribution) of x^n is the distribution that results from choosing a random letter from x^n, i.e. $P_{x^n}(a) = \frac{1}{n}N(a|x^n)$. Here we use P_{x^n} to denote the type of x^n. Let $\mathcal{P}_n$ denote the set of all possible types of sequences in $[d]^n$; equivalently $\mathcal{P}_n$ is the set of probability distributions on $[d]$ whose entries are integer multiples of $1/n$. Let $\mathcal{T}_p^n := \{x^n : P_{x^n} = p\}$. Note that

$$|\mathcal{T}_p^n| = \binom{n}{np} := \frac{n!}{np_1!np_2!\cdots np_d!}. \tag{3}$$

(a) List the elements of $\mathcal{P}_3$ when $d = 3$.

(b) Prove the upper bound

$$|\mathcal{P}_n| \le (n+1)^{d-1}. \tag{4}$$

(c) Prove that for $x^n \in \mathcal{T}_p^n$,

$$p^n(x^n) := p(x_1)\cdots p(x_n) = 2^{-nH(p)}, \tag{5}$$

where $H(p) := \sum_x p(x)\log(1/p(x))$.

(d) Compute $p^n(\mathcal{T}_q^n)$ where we use the notation $p^n(S)$ to mean $\sum_{x^n\in S} p^n(x^n)$. Express your answer in terms of $H(q)$ and $D(q\|p) = \sum_x q(x)\log\frac{q(x)}{p(x)}$.

(e) If $p \in \mathcal{P}_n$ then it turns out that $\max_{q\in\mathcal{P}_n} p^n(\mathcal{T}_q^n)$ is achieved by $q = p$. You do not need to prove this. Use this fact, along with the previous parts, to prove that

$$\frac{2^{nH(p)}}{(n+1)^{d-1}} \le |\mathcal{T}_p^n| \le 2^{nH(p)}. \tag{6}$$

(f) Pinsker's inequality (which you can use without proof) states that

$$D(q\|p) \ge \frac{1}{2\ln 2}\|p-q\|_1^2. \tag{7}$$

Combine this with the last two parts to prove that

$$p^n(\mathcal{T}_q^n) \le e^{-n\frac{\|p-q\|_1^2}{2}}. \tag{8}$$

(g) One consequence of (8) is a weak version of a Chernoff bound. Suppose that we have a coin with probability a of heads and probability $1-a$ of tails. If we flip it n times show that the probability of $\ge nb$ heads for $b > a$ decreases exponentially with n.

(h) We can also use types to define a sharper version of typical sets. Define

$$\mathcal{T}_{p,\delta}^n = \bigcup_{q:\|p-q\|_1\le\delta} \mathcal{T}_q^n. \tag{9}$$

Prove that $1 - p^n(\mathcal{T}_{p,\delta}^n)$ is exponentially small for fixed p and fixed $\delta > 0$.