ECE 4950 Fall 2023
Quantum Information Science: Communication and Computation
Homework 1

Due Monday 11 September 2023, by 8:40am in class (no late homeworks accepted)

(You are allowed to work with 1-2 other classmates as long as you write down who your collaborators are.)

1. Concentration inequalities:

   (a) Prove the Markov inequality. That is, for a random variable X whose realizations are non-negative, prove that

   $$\Pr\{X \geq \varepsilon\} \leq \frac{\mathbb{E}\{X\}}{\varepsilon}.$$

   (b) Prove the Chebyshev inequality. That is, for any random variable with finite second moment, show that the following inequality holds:

   $$\Pr\{|X - \mathbb{E}\{X\}| \geq \varepsilon\} \leq \frac{\operatorname{Var}\{X\}}{\varepsilon^2},$$

   where $\operatorname{Var}\{X\} = \mathbb{E}\{|X - \mathbb{E}\{X\}|^2\}$.

   (c) Prove the following law of large numbers. For a large number of pairwise independent and identically distributed random variables $X_1, \ldots, X_n$, (such that $\mathbb{E}\{X_i\} = \mu$ and $\mathbb{E}\{|X_i - \mu|^2\} = \sigma^2$ for all $i \in \{1, \ldots, n\}$) the probability that the sample mean deviates from the true mean has a power law decay:

   $$\Pr\left\{\left|\frac{1}{n}\sum_{i=1}^{n} X_i - \mu\right| \geq \varepsilon\right\} \leq \frac{\sigma^2}{\varepsilon^2 n}.$$

   (d) Prove the Hoeffding inequality (feel free to consult Wikipedia). That is, for a large number of bounded independent and identically distributed random variables X_1, $\ldots$, X_n taking values in $[a, b]$, show that the probability that their sum $S_n = \sum_{i=1}^{n} X_i$ deviates from the expected sum $\mathbb{E}[S_n]$ by an additive constant (one-sided) decays exponentially with the number of samples taken:

   $$\Pr\{S - \mathbb{E}[S_n] \geq t\} \leq \exp\left(-2t^2/nM^2\right),$$

   where $M = b - a$.

   (e) Under the same assumptions as (d), prove also that

   $$\Pr\{S - \mathbb{E}[S_n] \leq -t\} \leq \exp\left(-2t^2/nM^2\right). \tag{1}$$

   (f) Under the same assumptions as (d), use the union bound to conclude that

   $$\Pr\{|S - \mathbb{E}[S_n]| \geq t\} \leq 2\exp\left(-2t^2/nM^2\right). \tag{2}$$

(g) Under the same assumptions as (d), for the sample mean $\overline{X^n} = \frac{1}{n}\sum_{i=1}^{n} X_i$ with expectation μ, prove that

$$\Pr\left\{\left|\overline{X^n} - \mu\right| \geq \varepsilon\right\} \leq 2\exp\left(-2n\varepsilon^2/M^2\right). \tag{3}$$

(h) Under the same assumptions as (d), rewrite the result from (g) to conclude the claim from class, that, to have a desired accuracy $\varepsilon > 0$ and success probability at least $1 - \delta$, i.e.,

$$\Pr\left\{\left|\overline{X^n} - \mu\right| \leq \varepsilon\right\} \geq 1 - \delta, \tag{4}$$

the Hoeffding inequality guarantees that the following number n of samples suffices:

$$n \geq \frac{M^2}{\varepsilon^2}\ln\left(\frac{2}{\delta}\right). \tag{5}$$

(i) Under the same assumptions as (d), suppose that there is a probabilistic algorithm that takes $p(m)$ steps to output an independent sample of the random variable X, where m is the size of the computational problem and $p(m)$ is a polynomial in m. What are the smallest values of the accuracy ε and success probability $1 - \delta$ such that, by taking independent samples of X and forming the sample mean, the resulting algorithm can be considered efficient? That is, can we take ε to be exponentially small in m / polynomially small? Can we take δ to be exponentially small in m / polynomially small?

2. Given is a random variable X with probability distribution $p(x)$ and a random variable Y with probability distribution $q(x)$.

   (a) Devise a probabilistic algorithm to estimate $\sum_x p^2(x)$. Use the Hoeffding inequality to give guarantees on the accuracy and success probability of the algorithm. (Hint: Use the fact that $\sum_x p^2(x) = \sum_{x,x'} \delta_{x,x'} p(x)p(x')$ and observe that this rewriting allows for understanding the quantity of interest as the expected value of a random variable that takes values $\delta_{x,x'}$ with probability $p(x)p(x')$.)

   (b) Devise a probabilistic algorithm to estimate $\sum_x p^k(x)$, where $k \in \mathbb{N}$.

   (c) Devise a probabilistic algorithm to estimate $\sum_x p(x)q(x)$.

   (d) Devise a probabilistic algorithm to estimate the squared Euclidean distance between the distributions p and q:

   $$\sum_x |p(x) - q(x)|^2$$

   Use the union bound, the triangle inequality, and the Hoeffding inequality to give precise guarantees on the accuracy and success probability of the algorithm. Conclude that $O(\varepsilon^{-2}\ln\delta^{-1})$ samples from p and q suffice.

3. In class, we considered an abstract algorithm $\mathcal{A}$ for primality testing of an integer N, which outputs "prime" with probability $p_1 \geq 2/3$ when N is prime and outputs "not prime" with probability $p_0 \geq 2/3$ when N is not prime. We then considered a majority vote algorithm $\mathcal{A}'$ and analyzed its failure probability when N is prime, by

making use of the Chernoff bound $\Pr[S \leq (1-\delta)\mathbb{E}[S]] \leq \exp(-\delta^2\mathbb{E}[S]/2)$. Analyze the failure probability of $\mathcal{A}'$ when N is not prime, by making use of the Chernoff bound $\Pr[S \geq (1+\delta)\mathbb{E}[S]] \leq \exp(-\delta^2\mathbb{E}[S]/(2+\delta))$.

4. Pauli matrices:

   (a) Show that the Pauli matrices are all Hermitian, unitary, they square to the identity, and their eigenvalues are ± 1.

   (b) Represent the eigenstates of the Y Pauli matrix in the standard basis.

   (c) Show that the Pauli matrices either commute or anticommute.

   (d) Let us label the Pauli matrices as $\sigma_0 \equiv I$, $\sigma_1 \equiv X$, $\sigma_2 \equiv Y$, and $\sigma_3 \equiv Z$.

   (e) Show that $\mathrm{Tr}[\sigma_i \sigma_j] = 2\delta_{ij}$ for all $i, j \in \{0, \ldots, 3\}$, where Tr denotes the trace of a matrix, defined as the sum of the entries along the diagonal.