CS6845 - Pseudorandomness
Assignment 5

Due date: April 23, in class

Instructions

- For each day's delay in submission, you will lose 25% marks.
- Discussing the questions on the assignment with your classmates is allowed, but **no** collaboration is allowed while writing up the solution. If you discuss an assignment problem with someone, please acknowledge that while writing the solution. This will **not** affect your grade.
- Checking online sources for answers is **strongly discouraged**. If you need any clarification, you are welcome to discuss with me or Dinesh. Any academic dishonesty will result in zero marks for the assignment.
- Include all the steps/arguments in your answer/proof.

---

1. (3 points) Let $\mathcal{C}_1$ be a code with an encoding function $\mathrm{Enc}_1 : \Sigma^k \to \Sigma^n$ and $\mathcal{C}_2$ be a code with an encoding function $\mathrm{Enc}_2 : \Sigma \to \{0,1\}^m$. A *concatenated code* of $\mathcal{C}_1$ and $\mathcal{C}_2$ is a code with an encoding function $\mathrm{Enc} : \Sigma^k \to \{0,1\}^{mn}$ defined as follows: For $x \in \Sigma^k$, obtain $y = y_1 y_2 \ldots y_n \in \Sigma^n$ such that $y = \mathrm{Enc}_1(x)$. For each $y_i \in \Sigma$, obtain $z_i = \mathrm{Enc}_2(y_i)$. Now $\mathrm{Enc}(x) = z_1 z_2 \ldots z_n$ where $z_i \in \{0,1\}^m$.

   Suppose that $\mathcal{C}_1$ and $\mathcal{C}_2$ has local decoding algorithms $\mathcal{A}_1$ and $\mathcal{A}_2$ that can decode up to ρ_1 and ρ_2 fraction of errors respectively. Give a local decoding algorithm for the concatenated code using $\mathcal{A}_1$ and $\mathcal{A}_2$ that can decode up to $\rho_1 \cdot \rho_2$ fraction of errors.

   (**Hint:** Simulate the local decoder for $\mathcal{C}_1$, and use the local decoder for $\mathcal{C}_2$ whenever it queries a position.)

2. (2 points) Let $f : \{\pm 1\}^n \to \{\pm 1\}$ be a random function, i.e. $f(x) = \pm 1$ with probability $1/2$ for all $x \in \{\pm 1\}^n$. Show that for each $S \subseteq [n]$, the random variable $\hat{f}(S)$ has mean 0, and variance 2^{-n}.

3. (2 points) Suppose an algorithm is given query access to a linear function $f : \{\pm 1\}^n \to \{\pm 1\}$ and its task is to determine which linear function f is. Show that querying f on n inputs is necessary and sufficient.

4. (3 points) Let f be a Boolean function. Given a set $S \subseteq [n]$, define $f^{\leq S} : \{\pm 1\}^n \to \mathbb{R}$ by $f^{\leq S} = \sum_{T, T \subseteq S} \hat{f}(T)\chi_T$. Show that $f^{\leq S}(x) = \mathbb{E}_{y \in \{\pm 1\}^n}[f(y) | y_S = x_S]$, where x_S denote the bits of x in S.

5. (2 points) Let $A \subseteq \mathbb{F}_2^n$, and let $\alpha = |A|/2^n$ and write $1_A : \mathbb{F}_2^n \to \{0,1\}$ for the indicator function of A. Show that $\sum_{S \neq \emptyset} \widehat{1_A}(S)^2 = \alpha(1-\alpha)$.

6. In this question, we will design and analyze a tester for affine functions. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is an affine function if $f(x) = a \cdot x + b$ for some $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$.
   (a) (2 points) Show that f is affine iff $f(x+y+z) = f(x) + f(y) + f(z)$ for all $x, y, z \in \mathbb{F}_2^n$.
   (b) (3 points) Let $f : \mathbb{F}_2^n \to \mathbb{R}$. Suppose we choose $x, y, z \in_r \mathbb{F}_2^n$ independently and uniformly at random, show that $\mathbb{E}[f(x)f(y)f(z)f(x+y+z)] = \sum_S \hat{f}(S)^4$.
   (c) (2 points) Give a 4-query test for a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with the following property: if the test accepts with probability $1 - \epsilon$ then f is ϵ-close to being affine. All four query inputs should have the uniform distribution on $\mathbb{F}_2^n$, but need not be independent.
   (d) (2 points) Give an alternate 4-query test for being affine in which three of the query inputs are uniformy distributed and the fourth is not random.
   (**Hint:** Show that f is affine if and only if $f(x) + f(y) + f(0) = f(x+y)$ for all $x, y \in \mathbb{F}_2^n$.)