CS 538: Complexity of Computation Fall 2022

Homework 1: Toolkit for Complexity Theory

Instructor: Karthik C. S. Grader: Surya Teja Gavva

Due Date: *October 10, 2022*

1.1 Finite Fields

For every prime q, the field $\mathbb{F}_q$ may be thought of as the set $\{0, 1, \ldots, q-1\}$, where arithmetic operations like addition and multiplication are performed modulo q. A polynomial of degree d over a field $\mathbb{F}_q$ is an expression of the form: $a_0 + a_1 x + a_2 x^2 + \cdots a_d x^d$, where each of the a_i is an element of $\mathbb{F}_q$, with $a_d \neq 0$.

Euclid's Division algorithm asserts that for any two polynomials $f(x)$ and $g(x)$ over $\mathbb{F}_q$, there exists unique polynomials $t(x)$ (referred to as quotient polynomial) and $r(x)$ (referred to as remainder polynomial) such that $f(x) = g(x) \cdot t(x) + r(x)$ and $\deg(r) < \deg(g)$.

Question 1.1. *Let p be a polynomial over $\mathbb{F}_q$. Using Euclid's Division algorithm, prove that if α is a root of $p(x)$, that is $p(\alpha) = 0$, then $(x - \alpha)$ is a factor of $p(x)$. In other words, show that $p(x) = (x - \alpha)t(x)$, for some polynomial $t(x)$ over $\mathbb{F}_q$.*

Question 1.2. *Assuming the assertion of the above question, show that a non-zero polynomial of degree d over $\mathbb{F}_q$ has at most d roots.*

1.2 Fourier Analysis

The Fourier decomposition of a function $f : \{-1, 1\}^n \to \mathbb{R}$ is its expression as a multilinear polynomial (on n variables) given below.

$$f(\boldsymbol{x}) = \sum_{S \subseteq [n]} \widehat{f}(S) \cdot \chi_S(\boldsymbol{x}),$$

where for every subset $S \subseteq [n]$, $\widehat{f}(S)$ are the coefficients which take values in $\mathbb{R}$, and $\chi_S(\boldsymbol{x})$ is the monomial

$$\chi_S(\boldsymbol{x}) = \prod_{i \in S} x_i.$$

Given a function $f : \{-1, 1\}^n \to \mathbb{R}$, the Fourier coefficients of f can be computed using

$$\widehat{f}(S) = \mathop{\mathbb{E}}_{\boldsymbol{x} \sim \{-1,1\}^n} \left[f(\boldsymbol{x}) \cdot \chi_S(\boldsymbol{x}) \right]. \tag{1.1}$$

Question 1.3. *Prove that for every two subsets $S, T \subseteq [n]$, we have the following orthogonality:*

$$\mathop{\mathbb{E}}_{\boldsymbol{x}\sim\{-1,1\}^n}[\chi_S(\boldsymbol{x})\chi_T(\boldsymbol{x})] = \begin{cases} 1 \text{ if } S = T \\ 0 \text{ otherwise} \end{cases}.$$

Use the above orthogonality to verify the Fourier expansion formula given in (1.1).

Question 1.4. *Use the above orthogonality to prove the following Parseval's identity: For any $f : \{-1,1\}^n \to \mathbb{R}$, we have:*

$$\mathop{\mathbb{E}}_{\boldsymbol{x}\sim\{-1,1\}^n}\left[(f(\boldsymbol{x}))^2\right] = \sum_{S\subseteq[n]} \widehat{f}(S)^2.$$

1.3 Probability

Linearity of Expectation says that the expected value of a sum of random variables is the sum of the expected values of the variables. Use linearity of expectation to answer the below question.

Question 1.5. *Let $n \in \mathbb{N}$. Pick uniformly and independently random vectors $y_1, y_2, \ldots y_k$ in $\{0,1\}^n$ and consider the set $Y = \{y_1, \ldots, y_k\}$. For any $x \in \{0,1\}^n$, consider the random variable $U_x = \sum_{j=1}^{k} \langle x, y_j\rangle$ (where the dot product is modulo 2 and the sum is not). Compute $\mathop{\mathbb{E}}_{Y}[U_x]$.*

Chernoff bounds give the concentration of the sum of independent and identically distributed random variables. Use Chernoff bound and the answer to the above question to show the following.

Question 1.6. *For every $n \in \mathbb{N}$ and $\varepsilon > 0$, show that there exists a set $S \subset \{0,1\}^n$ of size $O\left(n/\varepsilon^2\right)$ such that $\forall x \in \{0,1\}^n \backslash \{0\}$ the following holds:*

$$\left|\mathop{\mathbb{E}}_{y\sim S}\left[(-1)^{<x,y>}\right]\right| \leq \varepsilon.$$

1.4 Error Correcting Codes

Let Σ be a finite set of cardinality greater than 1. Let $\ell \in \mathbb{N}$. An error correcting C code of block length ℓ over alphabet set Σ is simply a collection of vectors $\mathsf{C} \subseteq \Sigma^\ell$. Each vector in C is referred to as a codeword. The relative distance between any two codewords is the fraction of coordinates on which they are different. The relative distance of the code C is defined to be the smallest relative distance between any pair of distinct codewords in C. The message length of C is defined to be $\lfloor \log_{|\Sigma|} |\mathsf{C}| \rfloor$. The rate of C is defined as the ratio of its message length and block length.

Question 1.7. *For every Σ of cardinality greater than 1, and for every large enough $\ell \in \mathbb{N}$, show that there is a code $\mathsf{C} \subseteq \Sigma^\ell$ of relative distance 0.25 and rate greater than 0.01.*

Question 1.8. *Let q be a prime number and let $\Sigma = \mathbb{F}_q$. We simultaneously associate Σ with $[q]$. Let d be a non-negative integer less than q. For every polynomial p over $\mathbb{F}_q$ of degree d, we associate a vector c_p in Σ^q as follows: the i^{th} coordinate of c_p is the evaluation of p at the field element $i-1$. Then we construct the code $\mathsf{C} := \{c_p \mid p \text{ is degree } d \text{ polynomial over } \mathbb{F}_q\}$. What is the rate and relative distance of C?*

1.5 Expanders

Let $n, d \in \mathbb{N}$. Given a simple undirected graph G on vertex set $[n]$ and edge set E, we say that G is d-regular if every vertex in G has exactly d neighbors. Given a family $\mathcal{F}$ of graphs $\{G_i\}_{i\in\mathbb{N}}$, where G_i is a graph on i vertices, we say that $\mathcal{F}$ is d-regular graph family, if there exists some $i_0 \in \mathbb{N}$ such that for every $i \geq i_0$, we have that G_i is a d-regular graph.

We say that a d-regular graph family $\mathcal{F} = \{G_i\}_{i\in\mathbb{N}}$ is an expander family, if there exists some $i_0 \in \mathbb{N}$ and $\delta > 0$, such that for every $i \geq i_0$, and for every subset of vertices S in G_i of cardinality at most $i/2$, we have that the number of edges in G_i with one end point in S and another end point *not* in S is at least $\delta \cdot |S| \cdot d$.

Question 1.9. *Show that there is no 2-regular graph family $\mathcal{F} = \{G_i\}_{i\in\mathbb{N}}$ which is an expander family.*

Question 1.10. *Show that there is a 3-regular graph family $\mathcal{F} = \{G_i\}_{i\in\mathbb{N}}$ which is an expander family.*[*]

[*]Hint: Consider any large even $n \in \mathbb{N}$. One can then build a d-regular random balanced bipartite graph with $n/2$ vertices on each side, by uniformly and independently sampling d permutations of $[n/2]$. Show that with probability $1/2$, in this random graph, every subset of vertices S of cardinality at most $n/2$, have at least $0.01 \cdot |S| \cdot d$ edges with one end point in S and another end point not in S.