Homework 4

1. **Fourier Analysis on Larger Domains.** (5+5+5+5 points) Recall that we apply discrete Fourier Analysis on the Boolean Hypercube to analyze functions with domain $\{0,1\}^n$. We will generalize this analysis to arbitrary domains.

   (a) Consider the space of all function $\mathbb{Z}_p \to \mathbb{C}$, where p is a prime number. Here $\mathbb{Z}_p$ is the set $\{0,1,\dots,p-1\}$. And addition and multiplication of two elements from this set is defined using integer addition and multiplication, respectively, $\mod p$. The set of complex numbers is represented by $\mathbb{C}$.

   Suppose $f, g\colon \mathbb{Z}_p \to \mathbb{C}$ be two functions. Recall that the *complex conjugate* of a complex number $z = a + \imath b$, represented by $\overline{z}$, is defined to be $a - \imath b$. The inner-product of these two functions is defined by

   $$\langle f, g \rangle := \frac{1}{p} \sum_{x \in \mathbb{Z}_p} f(x)\overline{g(x)}$$

   Let $\omega_p := \exp\left(2\pi\imath/p\right)$ and define $\chi_a(x) := \omega_p^{ax}$, for $a \in \mathbb{Z}_p$. Prove that $\{\chi_a \colon a \in \mathbb{Z}_p$ is an orthonormal basis for the space of all function $\mathbb{Z}_p \to \mathbb{C}$.

   (b) Consider the space of all functions $\mathbb{Z}_p^n \to \mathbb{C}$. Define the inner-product of functions, write the Fourier basis functions, and show their orthonormality.

   (c) Consider the space of all functions $\mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{C}$, for primes p and q. The primes p and q need not necessarily be distinct. Define the inner-product of functions, write the Fourier basis functions, and show their orthonormality.

   (d) Consider the space of all functions $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n} \to \mathbb{C}$. Note that the primes $p_1, \dots, p_n$ need not be distinct. Define the inner-product of functions, write the Fourier basis functions, and show their orthonormality.

   Solution.

2. **Majority Functions.** (5 + 15 points) Let n be an odd number, and $f(x)\colon \{0,1\}^n \to \{+1,-1\}$ be the majority function. That is, if the majority of the bits in x is 0, then $f(x) = +1$; otherwise $f(x) = -1$.

   (a) Compute the Fourier coefficients of f when $n = 3$.

   (b) For $x \in \{0,1\}^n$, define $\mathsf{flip}(x)$ to be the string where we flip every bit of x. For example, we have $\mathsf{flip}(00101) = 11010$.

   A function is *odd* if $f(\mathsf{flip}(x)) = -f(x)$, for all $x \in \{0,1\}^n$. Note that the majority function defined above is an odd function.

   A set $S \in \{0,1\}^n$ is *even* if the number of 1s in S is even. For example, when $n = 3$, the sets $S = 000, 011, 101, 110$ are even sets.

   Prove that if f is an odd function then $\widehat{f}(S) = 0$ for all even $S \in \{0,1\}^n$.

Solution.

3. **Generalized BLR.** (20 points) Recall that a function $f\colon \{0,1\}^n \to \{+1,-1\}$ is linear if $f(0^n) = +1$ and $f(x+y) = f(x)\cdot f(y)$, for all $x, y \in \{0,1\}^n$. Consider the following generalization of the BLR algorithm to test whether a function f or $-f$ is close to linear.

   > $\mathsf{BLR} - \mathsf{Gen}^f$:
   >
   > (a) Let $a, b, c \xleftarrow{\$} \{0,1\}^n$
   >
   > (b) Let $w = f(a)$, $x = f(b)$, $y = f(c)$, and $z = f(a+b+c)$
   >
   > (c) Return $(q \cdot x \cdot y == z)$

   State and prove a theorem that intuitively proves that "the algorithm returns true with high probability" if and only if "the function f or $-f$ is close to a linear function."

   Solution.

4. **An Alternative Proof.** (5+15 points) Recall that the convolution of two function $f, g\colon \{0,1\}^n \to \mathbb{R}$ is defined as follows

$$(f * g)(x) := \frac{1}{N} \sum_{y \in \{0,1\}^n} f(y) g(x-y)$$

In this problem we shall develop a new technique to prove that $\widehat{(f * g)} = \widehat{f}\widehat{g}$.

(a) Compute the function $(\chi_S * \chi_T)$

(b) Note that the convolution operator is a bilinear operator. That is, we have $\big((f_1 + f_2) * g\big) = (f_1 * g) + (f_2 * g)$ and $(cf) * g = c(f * g)$ from the definition of convolution. Similarly, we have $\big(f * (g_1 + g_2)\big) = (f * g_1) + (f * g_2)$ and $f * (cg) = c(f * g)$.

Recall that we have $f = \sum_{S \in \{0,1\}^n} \widehat{f}(S)\chi_S$ and $g = \sum_{S \in \{0,1\}^n} \widehat{g}(S)\chi_S$. Prove that

$$(f * g) = \sum_{S \in \{0,1\}^n} \widehat{f}(S)\widehat{g}(S)\chi_S$$

Solution.

5. **A Few Properties of Fourier Transformation.** (5+5+5+5 points) Let $f, g\colon \{0,1\}^n \to \mathbb{R}$ be two functions.

   (a) Express $\widehat{(fg)}$ using the functions $\widehat{f}$ and $\widehat{g}$. Here the function (fg) defined as $(fg)(x) = f(x) \cdot g(x)$, for all $x \in \{0,1\}^n$.

   (b) Let $\max\{f,g\}$ is the function that satisfies $\max\{f,g\}(x) = \max\{f(x), g(x)\}$, for all $x \in \{0,1\}^n$. Suppose the range of f and g is $\{+1,-1\}$. Express $\widehat{\max\{f,g\}}$ is terms of $\widehat{f}$ and $\widehat{g}$.

   (c) Recall that if $f(x) = g(x-c)$ for some $c \in \{0,1\}^n$ then we have $\widehat{f} = \chi_c \widehat{g}$. Find a function $h\colon \{0,1\}^n \to \mathbb{R}$ such that $f = (h * g)$.

   (d) For $1 \leqslant i < j \leqslant n$, define

$$\mathsf{swap}_{i,j}(x_1, \dots, x_n) = (x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_n).$$

   Suppose $f(x) = g(\mathsf{swap}_{i,j}(x))$, for all $x \in \{0,1\}^n$. Express $\widehat{f}$ as a function of $\widehat{g}$.

Solution.

Collaborators :