Homework 4

1. (10 + 10 + 10 + 10 points) Recall that we apply discrete Fourier Analysis on the Boolean Hypercube to analyze functions when their domain is $\{0,1\}^n$. We will generalize this to arbitrary domain.

   (a) Consider the space of all functions $\mathbb{Z}_p \to \mathbb{C}$. Here $\mathbb{Z}_p$ is the set $\{0, 1, \ldots, p-1\}$, where p is a prime. And addition and multiplication is defined $\mod p$. 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:

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

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

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

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

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

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

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

   (b) Let us define odd and even functions. For $x \in \{0,1\}^n$, define $\mathsf{flip}(x)$ to be the string where you flip every bit of x. For example $\mathsf{flip}(0010) = 1101$.

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 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 $S \in \{0,1\}^n$.

(c) Similarly, a function f is *even* if $f(\mathsf{flip}(x)) = f(x)$, for all $x \in \{0,1\}^n$. A set $S \in \{0,1\}^n$ is *odd* if the number of 1s in S is odd. Prove that if f is an even function then $\widehat{f}(S) = 0$, for all odd $S \in \{0,1\}^n$.

3. (15 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 is close to linear or the function $-f$ is close to linear.

$\mathsf{BLR\text{-}Gen}^f$:
(a) Let $a, b, c \sim \mathbb{U}_{\{0,1\}^n}$
(b) Let $w = f(a)$, $x = f(b)$, $y = f(c)$, and $z = f(a+b+c)$
(c) Return $(w \cdot x \cdot y == z)$

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."