Lecture 20: Basic Applications

- Objective: Study function $f\colon \{0,1\}^n \to \mathbb{R}$
- Interpret function $\{0,1\}^n \to \mathbb{R}$ as vectors in $\mathbb{R}^N$, where $N = 2^n$
- Fourier Basis: A basis for the space $\mathbb{R}^N$ with appropriate properties
- Character Functions: For $S \in \{0,1\}^n$, we define

  $$\chi_S(x) := (-1)^{S_1x_1+\cdots+S_nx_n},$$

  where $x = x_1x_2\ldots x_n$ and $S = S_1S_2\ldots S_n$.
- We define the inner product of two functions as

  $$\langle f, g\rangle = \frac{1}{N}\sum_{x\in\{0,1\}^n} f(x)g(x)$$

- With respect to this inner-product the Fourier basis $\{\chi_0, \chi_1, \ldots, \chi_{N-1}\}$ is orthonormal

- Now, every function f can be written as

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

- The mapping $f \mapsto \widehat{f}$ is the Fourier transformation
- There exists an $N \times N$ matrix $\mathcal{F}$ such that $f \cdot \mathcal{F} = \widehat{f}$, for all f
- This result proves that the Fourier transformation is linear, that is, $\widehat{(f+g)} = \widehat{f} + \widehat{g}$ and $\widehat{(cf)} = c\widehat{f}$
- We saw that $\mathcal{F} \cdot \mathcal{F} = \frac{1}{N} \cdot I_{N \times N}$. This result implies that $\mathcal{F}$ is full rank and $\widehat{f} = \widehat{g}$ if and only if $f = g$. So, for any function f, we have

$$\widehat{\left(\widehat{f}\right)} = \frac{1}{N} f$$

Recall

- We saw two identities
  1. Plancherel's Theorem: $\langle f, g\rangle = \sum_{S\in\{0,1\}^n} \widehat{f}(S)\widehat{g}(S)$, and
  2. Parseval's Identity: $\langle f, f\rangle = \sum_{S\in\{0,1\}^n} \widehat{f}(S)^2$.

Objective

- The objective of this lecture is to associate "properties of a function f" to "properties of the function $\widehat{f}$"
- In the sequel, we shall consider a few such properties

- Let $\mathbb{X}$ be a random variable over the sample space $\{0,1\}^n$
- We shall use $\mathbb{X}$ to represent the corresponding function $\{0,1\}^n \to \mathbb{R}$ defined as follows

$$\mathbb{X}(x) := \mathbb{P}\left[\mathbb{X} = x\right]$$

- **Collision Probability.** The probability that when we draw two independent samples according to the distribution $\mathbb{X}$, the two samples turn out to be identical. Note that this probability is $\mathrm{col}(\mathbb{X}) := \sum_{x\in\{0,1\}^n} \mathbb{X}(x)^2 = N\langle\mathbb{X},\mathbb{X}\rangle$

- We can translate "collision probability" as a property of f into an alternate property of $\widehat{f}$ as follows

Lemma

$$\mathrm{col}(\mathbb{X}) = N \sum_{S \in \{0,1\}^n} \widehat{\mathbb{X}}(S)^2$$

This lemma is a direct consequence of Parseval's identity

- Note that if we say that "$\mathbb{X}$ has *low* collision probability" then it is equivalent to saying that "$\sum_{S \in \{0,1\}^n} \widehat{\mathbb{X}}(S)^2$ is *small*"
- So, we can use "$\sum_{S \in \{0,1\}^n} \widehat{\mathbb{X}}(S)^2$ is *small*" as a proxy for the guarantee that "$\mathbb{X}$ has *low* collision probability"
- **Min Entropy.** We say that the min-entropy of $\mathbb{X}$ is $\geqslant k$, if $\mathbb{P}[\mathbb{X} = x] \leqslant 2^{-k} = \frac{1}{K}$, for all $x \in \{0,1\}^n$

- We can similarly get a property of a *high min-entropy distribution* $\mathbb{X}$

Lemma

If the min-entropy of $\mathbb{X}$ is $\geqslant k$, then we have

$$\sum_{S \in \{0,1\}^n} \widehat{\mathbb{X}}(S)^2 \leqslant \frac{1}{NK}$$

The proof follows from the observation that if the min-entropy of $\mathbb{X}$ is $\geqslant k$, then we have

$$\mathrm{col}(\mathbb{X}) = \sum_{x \in \{0,1\}^n} \mathbb{X}(x)^2 \leqslant \sum_{x \in \{0,1\}^n} \mathbb{X}(x) \cdot 2^{-k} = \frac{1}{K}$$

- Intuitively, if a distribution $\mathbb{X}$ has "high min-entropy" then it has "low collision probability," which, in turn, implies that "$\sum_{S \in \{0,1\}^n} \widehat{\mathbb{X}}(S)^2$ is small" (i.e., the function $\widehat{\mathbb{X}}$ lies inside a small sphere)

Vector Spaces over Finite Fields I

- We need to understand vector spaces over finite fields to understand the next result
- In this document, we shall restrict our attention to finite fields of size p, where p is a prime. In general, finite fields can have size q, where q is a prime-power
- A finite field is defined by three objects $(\mathbb{Z}_p, +, \times)$
  - The set $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$
  - The addition operator $+$. This operator is integer addition mod p.
  - The multiplication operator $\times$. This operator is integer multiplication mod p.
- For example, consider the finite field $(\mathbb{Z}_5, +, \times)$. We have $3 + 4 = 2$ and $2 \times 4 = 3$
- Every element $x \in \mathbb{Z}_p$ has an additive inverse, represented by $-x$ such that $x + (-x) = 0$. For example, $-3 = 2$

- Every element $x \in \mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$ has a multiplicative inverse, represented by $1/x$, such that $x \times (1/x) = 1$. For example, $1/3 = 2$.
- We can interpret $\mathbb{Z}_p^n$ as a vector space over the finite field $(\mathbb{Z}_p, +, \times)$
- We shall consider vector subspace V of $\mathbb{Z}_p^n$ that is spanned by the rows of the matrix G of the following form.

$$G = \left[I_{k \times k} \middle| P_{k \times (n-k)} \right]$$

- We consider the corresponding subspace $V^\perp$ of $\mathbb{Z}_p^n$ that is spanned by the rows of the matrix H of the form

$$H = \left[-P^\intercal \middle| I_{(n-k) \times (n-k)} \right]$$

- We define the dot-product of two vectors $u, v \in \mathbb{Z}_p^n$ as $u_1 v_1 + \cdots + u_n v_n$, where $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$
- Note that the dot-product of any row of G with any row of H is 0. This result follows from the fact that $G \cdot H^\intercal = 0_{k \times n-k}$. This observation implies that the dot-product of any vector in V with any vector in $V^\perp$ is 0
- Note that V has dimension k and $V^\perp$ has dimension $(n-k)$
- The vector space $V^\perp$ is referred to as the *dual vector space* of V
- Note that the size of the vector space V is p^k and the size of the vector space $V^\perp$ is p^{n-k}

- Let us consider an example. We shall work over the finite field $(\mathbb{Z}_2, +, \times)$. Consider the following matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

The corresponding matrix H is defined as follows

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Note that the dot-product of any row of G with any row of H is 0. Consequently, the dot-product of any vector in the span of the rows-of-G with any vector in the span of the rows-of-H is always 0

- Actually, any vector space $V \subseteq \mathbb{Z}_p^n$ has an associated $V^\perp \subseteq \mathbb{Z}_p^n$ such that the dot-product of their vectors is 0. (Think how to prove this result)

- Let V be a vector sub-space of $\{0,1\}^n$ of dimension k. Let $V^\perp$ be the dual vector sub-space of $\{0,1\}^n$ of dimension $(n-k)$.
- Let $f = \frac{1}{|V|}1_{\{V\}}$. That is, the function f is the following probability distribution

$$f(x) = \begin{cases} \frac{1}{K}, & \text{if } x \in V \\ 0, & \text{if } x \notin V \end{cases}$$

- Then, we have the following result.

Lemma

$$\widehat{f}(S) = \begin{cases} \frac{1}{N}, & \textit{if } S \in V^\perp \\ 0, & \textit{if } S \notin V^\perp \end{cases}$$

- **Proof Outline.** Suppose $S \in V^{\perp}$.

$$\begin{aligned}\widehat{f}(S) = \langle f, \chi_S \rangle &= \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x)\chi_S(x) \\ &= \frac{1}{N} \sum_{x \in V} f(x)\chi_S(x) \\ &= \frac{1}{NK} \sum_{x \in V} (-1)^{S \cdot x} \\ &= \frac{1}{NK} \sum_{x \in V} 1 \\ &= \frac{1}{NK} \cdot K = \frac{1}{N}\end{aligned}$$

Now, note that

$$\langle f, f\rangle = \frac{1}{N}\sum_{x\in\{0,1\}^n} f(x)^2 = \frac{1}{N}\sum_{x\in V}\frac{1}{K^2} = \frac{1}{NK}$$

Next note that

$$\begin{aligned}\sum_{S\in\{0,1\}^n}\widehat{f}(S)^2 &= \sum_{S\in V^\perp}\widehat{f}(S)^2 + \sum_{S\notin V^\perp}\widehat{f}(S)^2\\ &= (N/K)\frac{1}{N^2} + \sum_{S\notin V^\perp}\widehat{f}(S)^2\\ &= \frac{1}{NK} + \sum_{S\notin V^\perp}\widehat{f}(S)^2\end{aligned}$$

By Parseval's identity, we have $\langle f, f\rangle = \sum_{S\in\{0,1\}^n} \widehat{f}(S)^2$. So, we get that

$$\sum_{S\notin V^\perp} \widehat{f}(S)^2 = 0$$

That is, for every $S \in V^\perp$, we have $\widehat{f}(S) = 0$

- We can write the entire result tersely as follows

$$\widehat{\left(\frac{1_{\{V\}}}{|V|}\right)} = \frac{1}{N} 1_{\{V^\perp\}}$$

- As a corollary of this result, we can conclude that

$$\widehat{\delta_0} = \frac{1}{N} 1_{\{\{0,1\}^n\}}$$

Recall that δ_0 is the delta function that is 1 only at $x = 0$; 0 elsewhere. Furthermore, the function $1_{\{\{0,1\}^n\}}$ is the constant function that evaluates to 1 at every x

- Recursively use this result and the fact that $(V^{\perp})^{\perp} = V$ to verify that $\widehat{\left(\widehat{f}\right)} = \frac{1}{N} f$