Lecture 19: Simple Applications of Fourier Analysis & Convolution

Recall

- Let $f\colon \{0,1\}^n \to \mathbb{R}$ be a function
- Let $N = 2^n$
- Inner product of two functions is defined as follows

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

- For $S \in \{0,1\}^n$, define the function $\chi_S(x) = (-1)^{S \cdot x}$
- $\{\chi_S\}_{S \in \{0,1\}^n}$ forms an orthonormal basis
- We can write any function as follows

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

where $\widehat{f}(S) = \langle f, \chi_S \rangle$

- Parseval's Identity:

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

- The mapping $f \mapsto \widehat{f}$ is a linear bijection
- And, $\widehat{\left(\widehat{f}\right)} = \frac{1}{N} f$

Properties

- For a constant α, we have $\widehat{\alpha f} = \alpha \widehat{f}$
- For two functions f and g, we have $\widehat{(f+g)} = \widehat{f} + \widehat{g}$
- For a $c \in \{0,1\}^n$, suppose we have $f(x) = g(x+c)$

$$\begin{aligned}
\widehat{f}(S) &= \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x)\chi_S(x) \\
&= \frac{1}{N} \sum_{x \in \{0,1\}^n} g(x+c)\chi_S(x) \\
&= \frac{1}{N} \sum_{x \in \{0,1\}^n} g(x+c)\chi_S(x+c)\chi_S(c) \\
&= \chi_c(S)\widehat{g}(S)
\end{aligned}$$

So, we have $\widehat{f} = \chi_c \widehat{g}$

Binary Output Functions

- We will interpret binary functions as $f\colon \{0,1\}^n \to \{+1,-1\}$
- A Note: Traditionally, a binary function g is $g\colon \{0,1\}^n \to \{0,1\}$. We consider an equivalent function $f\colon \{0,1\}^n \to \{+1,-1\}$ defined by $f(x) = (-1)^{g(x)}$, or $f(x) = 1 - 2g(x)$. Intuitively, the traditional binary output is mapped as follows: $0 \mapsto +1$ and $1 \mapsto -1$

Claim

Let $f\colon \{0,1\}^n \to \{+1,-1\}$ be a binary function. We have

$$\sum_{S\in\{0,1\}^n} \widehat{f}(S)^2 = 1$$

Follows from Parseval's Identity

Distributions as Functions

- Let F be a distribution over the sample space $\{0,1\}^n$
- Let $f\colon \{0,1\}^n \to \mathbb{R}$ be the corresponding function defined by

$$f(x) = \mathbb{P}[F = x]$$

- When we say that f is a distribution, we mean that there exists an associated F as mentioned above such that F is a probability distribution

Claim

Let $f : \{0,1\}^n \to \mathbb{R}$ be a distribution. Then, we have $\widehat{f}(\emptyset) = \frac{1}{N}$.

Proof.

$$\widehat{f}(\emptyset) = \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x) \chi_\emptyset(x)$$
$$= \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x) \cdot 1 = \frac{1}{N}$$

□

Claim

Let $f = \mathbb{U}_{\{0,1\}^n}$, i.e. it is the uniform distribution over $\{0,1\}^n$. Then, we have $\widehat{f} = \delta_{0^n}/N$.

Proof.

$$\widehat{f}(S) = \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x)\chi_S(x)$$
$$= \frac{1}{N^2} \sum_{x \in \{0,1\}^n} \chi_S(x)$$
$$= \begin{cases} \frac{1}{N}, & \text{if } S = \emptyset \\ 0, & \text{if } S \neq \emptyset \end{cases}$$

□

Claim

Let $f = \delta_{0^n}$, it is the probability distribution that always outputs 0^n. Then, we have $\widehat{f} = \mathbb{U}_{\{0,1\}^n}$.

Use the previous result and the fact that $\widehat{(\widehat{f})} = f/N$

This result generalizes both the previous results.

Claim

Let $V \subseteq \{0,1\}^n$ be a vector space. Let $f = \mathbb{U}_V$ be the uniform distribution over the vector space V. Then, we have $\widehat{f} = 1_{V^\perp}/N$.

Proof.

Part 1: Let $S \in \mathbb{V}^\perp$.

$$\widehat{f}(S) = \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x)\chi_S(x) = \frac{1}{N} \sum_{x \in V} \frac{1}{|V|}(-1)^{S \cdot x}$$

$$= \frac{1}{N} \sum_{x \in V} \frac{1}{|V|} \cdot 1 = \frac{1}{N}$$

□

Proof.

Part 2: By Parseval's Identity, we have

$$\begin{aligned}
\sum_{S \notin V^\perp} \widehat{f}(S)^2 &= \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x)^2 - \sum_{S \in V^\perp} \widehat{f}(S)^2 \\
&= \frac{1}{N} \sum_{x \in V} f(x)^2 - \sum_{S \in V^\perp} \widehat{f}(S)^2 \\
&= \frac{1}{N} |V| \left(\frac{1}{|V|}\right)^2 - \left|V^\perp\right| \left(\frac{1}{N}\right)^2 = \frac{1}{|V|} - \frac{N}{|V|} \cdot \frac{1}{N^2} = 0
\end{aligned}$$

This implies that $\widehat{f}(S) = 0$ for all $S \notin V^\perp$. □

Exercise: Compute $\widehat{(c+f)}$, where $c \in \mathbb{R}$ is a constant and $f\colon \{0,1\}^n \to \mathbb{R}$

- A distribution X has min-entropy at least k, represented by $H_\infty(X) \geqslant k$, if $\mathbb{P}[X = x] \leqslant 2^{-k}$

Claim

Let f be a probability distribution with min-entropy at least k. Then, we have:

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

where $K = 2^k$.

Proof.

By Parseval's Identity we have

$$\begin{aligned}\sum_{S\in\{0,1\}^n} \widehat{f}(S)^2 &= \frac{1}{N}\sum_{x\in\{0,1\}^n} f(x)^2 \\ &\leqslant \frac{1}{N}\sum_{x\in\{0,1\}^n} f(x)\cdot\frac{1}{K} \\ &= \frac{1}{NK}\sum_{x\in\{0,1\}^n} f(x) = \frac{1}{NK}\end{aligned}$$

□

Claim

Let f and g be two distributions over $\{0,1\}^n$. Then, we have

$$2\mathrm{SD}(f,g) \leqslant N \left(\sum_{\emptyset \neq S \in \{0,1\}^n} \left(\widehat{f}(S) - \widehat{g}(S) \right)^2 \right)^{1/2}$$

$$
\begin{aligned}
2\mathrm{SD}(f,g) &= \sum_{x\in\{0,1\}^n} \left| f(x) - g(x) \right| \\
&\leqslant \left(\sum_{x\in\{0,1\}^n} \left(f(x) - g(x)\right)^2 \right)^{1/2} N^{1/2} \quad \text{By Cauchy-Schwarz} \\
&= N \left(\frac{1}{N} \sum_{x\in\{0,1\}^n} \left(f(x) - g(x)\right)^2 \right)^{1/2} \\
&= N \left(\frac{1}{N} \sum_{x\in\{0,1\}^n} (f-g)(x)^2 \right)^{1/2}
\end{aligned}
$$

$$2\mathrm{SD}(f,g) \leqslant N\left(\frac{1}{N}\sum_{x\in\{0,1\}^n}(f-g)(x)^2\right)^{1/2}$$

$$= N\left(\sum_{S\in\{0,1\}^n}\widehat{(f-g)}(S)^2\right)^{1/2} \quad \text{By Parseval's}$$

$$= N\left(\sum_{S\in\{0,1\}^n}\left(\widehat{f}(S)-\widehat{g}(S)\right)^2\right)^{1/2} \quad \text{By Parseval's}$$

$$= N\left(\sum_{\emptyset\neq S\in\{0,1\}^n}\left(\widehat{f}(S)-\widehat{g}(S)\right)^2\right)^{1/2} \quad \because \widehat{f}(\emptyset)=\widehat{g}(\emptyset)=1/N$$

Corollary

Let f be a distributions over $\{0,1\}^n$. Then, we have

$$2\mathrm{SD}\left(f, \mathbb{U}_{\{0,1\}^n}\right) \leqslant N \left(\sum_{\emptyset \neq S \in \{0,1\}^n} \widehat{f}(S)^2 \right)^{1/2}$$

Use the previous result and the fact that $\widehat{\mathbb{U}_{\{0,1\}^n}} = \delta_{0^n}/N$

Convolution

- Let $\mathbb{F}$ and $\mathbb{G}$ be two probability distributions over $\{0,1\}^n$
- Let $\mathbb{H}$ be a new distribution defined by the following sampling procedure:
  - Sample $a \sim \mathbb{F}$
  - Sample $b \sim \mathbb{G}$
  - Output $a + b$
- We will represent this as $\mathbb{H} = \mathbb{F} \oplus \mathbb{G}$
- Note that we have

$$\mathbb{P}[\mathbb{H} = x] = \sum_{y \in \{0,1\}^n} \mathbb{P}[\mathbb{F} = y] \cdot \mathbb{P}[\mathbb{G} = x - y]$$

- Let f, g, and h be the functions corresponding to the distributions $\mathbb{F}$, $\mathbb{G}$, and $\mathbb{H}$, respectively. That is,

$$h(x) = \sum_{y \in \{0,1\}^n} f(y) g(x - y)$$

Definition (Convolution)

Let $f, g\colon \{0,1\}^n \to \mathbb{R}$. The convolution of f and g, represented by $(f * g)$, is the function h such that

$$h(x) = \sum_{y \in \{0,1\}^n} f(y) g(x - y)$$

We emphasize that this definition is not specific to probability distributions f and g, but for all functions. When f and g happen to be probability distributions, then the function h corresponds to the probability distribution corresponding to the sampling procedure mentioned above

Claim

$$\widehat{(f * g)} = N \cdot \widehat{f}\,\widehat{g}$$

$$
\begin{aligned}
\widehat{(f * g)}(S) &= \frac{1}{N} \sum_{x \in \{0,1\}^n} h(x) \chi_S(x) \\
&= \frac{1}{N} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} f(y) g(x-y) \chi_S(x) \\
&= \frac{1}{N} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} f(y) g(x-y) \chi_S(y) \chi_S(x-y) \\
&= \frac{1}{N} \sum_{y \in \{0,1\}^n} \sum_{x-y \in \{0,1\}^n} f(y) g(x-y) \chi_S(y) \chi_S(x-y) \\
&= N \left(\frac{1}{N} \sum_{y \in \{0,1\}^n} f(y) \chi_S(y) \right) \left(\frac{1}{N} \sum_{z \in \{0,1\}^n} g(z) \chi_S(z) \right) \\
&= N \widehat{f}(S) \widehat{g}(S)
\end{aligned}
$$

An alternate proof for computing the Fourier Transform of a function that is the uniform distribution over a vector subspace V.

- Let V and W be two vector subspaces of $\{0,1\}^n$
- Let $Z = \mathrm{sp}(V, W)$
- Prove that: $\mathbb{U}_Z = \mathbb{U}_V \oplus \mathbb{U}_W$
- Prove that: $Z^\perp = V^\perp \cap W^\perp$
- Use induction on the dimension of V to prove that

$$\widehat{\mathbb{U}_V} = 1_{V^\perp}/N$$