Lecture 20: Fourier Analysis on the Boolean Hypercube
Convolution

**Definition (Convolution)**

\[(f * g)(x) = \sum_{r \in \{0,1\}^n} f(r)g(x + r)\]

- For two distributions \(f\) and \(g\), the distribution \((f \oplus g)\) is the distribution that samples \(a \sim f\) and \(b \sim g\) and outputs \((a \oplus b)\)
- Note: \((f \oplus g) = (f * g)\)
Lemma

\[(f \ast g)(S) = N \cdot \hat{f}(S) \cdot \hat{g}(S)\]

\[(f \ast g)(S) = \mathbb{E}_{x \sim U_n} [(f \ast g)(x), \chi_S(x)]\]

\[= \frac{1}{N} \sum_{x \in \{0,1\}^n} \sum_{r \in \{0,1\}^n} f(r)g(x + r) \cdot \chi_S(x)\]

\[= \frac{1}{N} \sum_{x \in \{0,1\}^n} \sum_{r \in \{0,1\}^n} f(r)g(x + r) \cdot \chi_S(r) \chi_S(x + r)\]

\[= \frac{1}{N} \left( \sum_{r \in \{0,1\}^n} f(r) \chi_S(r) \right) \cdot \left( \sum_{x \in \{0,1\}^n} g(x + r) \chi_S(x + r) \right)\]

\[= N \cdot \hat{f}(S) \cdot \hat{g}(S)\]
Example

Lemma

Let $V \subseteq \{0, 1\}^n$ be a vector space of dimension $t$. Then

$$\hat{U}_V(S) = \begin{cases} \frac{1}{N}, & \text{if } S \in V^\perp \\ 0, & \text{otherwise} \end{cases}$$

- If $\dim(V) = 0$ we know that the result is true (by Fourier transform of a delta-function)
- Let $\dim(V) = 1$ be the base case
- For $\dim(V) > 1$, we reduce the result to the base case
- Let $V = \text{span}(v_1, \ldots, v_t)$ and $V_i = \text{span}(v_i)$, for $i \in [t]$
- By base case, we have: $\hat{U}_{V_i}(S) = 1/N$ if and only if $S \in V_i^\perp$, otherwise $\hat{U}_{V_i}(S) = 0$
- Note that $U_V = U_{V_1} \oplus \cdots \oplus U_{V_t}$
- $\hat{U}_V(S) = N^{t-1} \prod_{i=1}^{t} \hat{U}_{V_i}(S)$
Example continued

- So, \( \hat{U}_V(S) = 0 \), if there exists \( i \in [t] \) such that \( S \not\in V_i^\perp \). That is, \( \hat{U}_V(S) = 0 \), if \( S \not\in \bigcap_{i=1}^t V_i^\perp = V^\perp \)

- If \( S \in \bigcap_{i=1}^t V_i^\perp = V^\perp \), then it is easy to see that \( \hat{U}_V(S) = N^{t-1} \cdot \frac{1}{N^t} = \frac{1}{N} \) from the base case

- Think: How to prove the result for \( \dim(V) = 1 \)?
Min-Entropy

- A distribution $f$ has min-entropy $k$ if $f(x) \leq 2^{-k}$, for all $x \in \{0, 1\}^n$.
- The collision probability of $f$ is defined as:

$$\text{coll}(f) = \sum_{x \in \{0, 1\}^n} f(x)^2$$

**Lemma**

*If $f$ has min-entropy $k$, then $\text{coll}(f) \leq 2^{-k}$*

- $\text{coll}(f) = \sum_{x \in \{0, 1\}^n} f(x)^2 \leq \sum_{x \in \{0, 1\}^n} f(x) \cdot 2^{-k} = 2^{-k}$
Lemma

Let $f$ be a probability distribution with min-entropy $k$. Then:

$$2^{-k} \geq \text{coll}(f) = N \| f \|_2^2 = N \sum_{S \subseteq [n]} \hat{f}(S)^2$$
Lemma

Let \( f \) be a probability distribution with min-entropy \( k \). Let \( g \) be a small-bias distribution, i.e. \( \text{bias}_S(g) \leq 2^{-t} \), for \( S \neq \emptyset \). Then:

\[
\SD(f \oplus g, U_n) \leq \ldots
\]

What is given:

- \( \sum_{S \subseteq [n]} \hat{f}(S)^2 \leq 1/KN \), where \( K = 2^k \)
- For all \( S \neq \emptyset \), we have \( |\hat{g}(S)| \leq 1/TN \), where \( T = 2^t \)

What we need to prove:

- \( \SD(f \oplus g, U_n) \leq \frac{N}{2} \left( \sum_{S \neq \emptyset} \widehat{(f \ast g)}(S)^2 \right)^{1/2} \) is small
Proof

\[ \text{SD}(f \oplus g, U_n) \leq \frac{N}{2} \left( \sum_{S \neq \emptyset} (\hat{f} \ast \hat{g})(S)^2 \right)^{1/2} \]

\[ = \frac{N}{2} \left( \sum_{S \neq \emptyset} N^2 \hat{f}(S)^2 \hat{g}(S)^2 \right)^{1/2} \]

\[ \leq \frac{N}{2} \cdot \frac{1}{TN} \left( N^2 \sum_{S \subseteq [n]} \hat{f}(S)^2 \right)^{1/2} \]

\[ \leq \frac{1}{2} \cdot \frac{1}{T} \left( \frac{N}{K} \right)^{1/2} \]