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: $(f \oplus g) = (f * g)$

Fourier Coefficients of a Convolution

Lemma

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

$$\begin{aligned}
\widehat{(f * g)}(S) &= \mathop{\mathbb{E}}_{x \sim U_n} [(f * g)(x), \chi_S(x)] \\
&= \frac{1}{N} \sum_{x \in \{0,1\}^n} \sum_{r \in \{0,1\}^n} f(r) g(x + r) \cdot \chi_S(x) \\
&= \frac{1}{N} \sum_{x \in \{0,1\}^n} \sum_{r \in \{0,1\}^n} f(r) g(x + r) \cdot \chi_S(r) \chi_S(x + r) \\
&= \frac{1}{N} \left(\sum_{r \in \{0,1\}^n} f(r) \chi_S(r) \right) \cdot \left(\sum_{x \in \{0,1\}^n} g(x + r) \chi_S(x + r) \right) \\
&= N \cdot \widehat{f}(S) \cdot \widehat{g}(S)
\end{aligned}$$

Example

Lemma

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

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

- 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 $V = \mathrm{span}(v_1, \dots, v_t)$ and $V_i = \mathrm{span}(v_i)$, for $i \in [t]$
- By base case, we have: $\widehat{U_{V_i}}(S) = 1/N$ if and only if $S \in V_i^{\perp}$, otherwise $\widehat{U_{V_i}}(S) = 0$
- Note that $U_V = U_{V_1} \oplus \cdots \oplus U_{V_t}$
- $\widehat{U_V}(S) = N^{t-1} \prod_{i=1}^{t} \widehat{U_{V_i}}(S)$

Example continued

- So, $\widehat{U_V}(S) = 0$, if there exists $i \in [t]$ such that $S \notin V_i^{\perp}$. That is, $\widehat{U_V}(S) = 0$, if $S \notin \cap_{i=1}^{t} V_i^{\perp} = V^{\perp}$
- If $S \in \cap_{i=1}^{t} V_i^{\perp} = V^{\perp}$, then it is easy to see that $\widehat{U_V}(S) = N^{t-1} \cdot \frac{1}{N^t} = \frac{1}{N}$ from the base case

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

Min-Entropy

- A distribution f has min-entropy k if $f(x) \leqslant 2^{-k}$, 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 $\text{coll}(f) \leqslant 2^{-k}$

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

Collision Probability and Fourier Coefficients

Lemma

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

$$2^{-k} \geqslant \mathrm{coll}(f) = N \|f\|_2^2 = N \sum_{S \subseteq [n]} \widehat{f}(S)^2$$

Min-entropy Extraction via Masking with Small-bias Distribution

Lemma

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

$$\mathrm{SD}\left(f \oplus g, U_n\right) \leqslant \dots$$

What is given:

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

What we need to prove:

- $\mathrm{SD}\left(f \oplus g, U_n\right) \leqslant \frac{N}{2} \left(\sum_{S \neq \emptyset} \widehat{(f * g)}(S)^2\right)^{1/2}$ is small

Proof

$$
\begin{aligned}
\mathrm{SD}\left(f \oplus g, U_n\right) &\leqslant \frac{N}{2}\left(\sum_{S \neq \emptyset} \widehat{(f * g)}(S)^2\right)^{1/2} \\
&= \frac{N}{2}\left(\sum_{S \neq \emptyset} N^2 \widehat{f}(S)^2 \widehat{g}(S)^2\right)^{1/2} \\
&\leqslant \frac{N}{2} \cdot \frac{1}{TN}\left(N^2 \sum_{S \subseteq [n]} \widehat{f}(S)^2\right)^{1/2} \\
&\leqslant \frac{1}{2} \cdot \frac{1}{T}\left(\frac{N}{K}\right)^{1/2}
\end{aligned}
$$