Lecture 21: Basic Applications of Fourier Analysis
(BLR-Test, List-Decoding Hadamard Codes, Smoothening Functions)
“BLR” = Blum, Luby, Rubinfeld

Problem: Given an oracle access to a function $f : \{0, 1\}^n \rightarrow \{+1, -1\}$, test whether it is (close to) a linear function

Algorithm (BLR Test):
- Pick random $x$ and $y$
- Output: “Linear” if $f(x) \cdot f(y) = f(x + y)$; otherwise, output “Not Linear”
Proof

- We want to understand the relation between the following two quantities

\[ A = \max_{S \subseteq [n]} |\hat{f}(S)| \quad B = \left| \mathbb{E}_{x,y}[f(x)f(y)f(x + y)] \right| \]

- We want to show that: \( A \approx 1 \) if and only if \( B \approx 1 \)
- Let us expand \( B \):

\[
\frac{1}{N^2} \sum_{x,y} \left( \sum_{Q \subseteq [n]} \hat{f}(Q) \chi_Q(x) \right) \times \left( \sum_{R \subseteq [n]} \hat{f}(R) \chi_R(y) \right) \\
\times \left( \sum_{T \subseteq [n]} \hat{f}(T) \chi_T(x + y) \right)
\]

\[
= \frac{1}{N^2} \sum_{x,y} \sum_{Q,R,T \subseteq [n]} \hat{f}(Q) \hat{f}(R) \hat{f}(T) \chi_Q(x) \chi_R(y) \chi_T(x + y)
\]
\[ \frac{1}{N^2} \sum_{x,y} \sum_{Q,R,T \subseteq [n]} \hat{f}(Q) \hat{f}(R) \hat{f}(T) \chi_{Q+T}(x) \chi_{R+T}(y) \]

\[ = \frac{1}{N^2} \sum_{x,y} \sum_{Q=R=T \subseteq [n]} \hat{f}(Q) \hat{f}(R) \hat{f}(T) \]

\[ = \frac{1}{N^2} \sum_{x,y} \sum_{Q \subseteq [n]} \hat{f}(Q)^3 = \sum_{Q \subseteq [n]} \hat{f}(Q)^3 \]

So, under the constraint that \( \sum_{S \subseteq [n]} \hat{f}(S)^2 = 1 \), we want to show that \( A \approx 1 \) if and only if \( B \approx 1 \), where:

\[ A = \max_{S \subseteq [n]} \left| \hat{f}(S) \right| \quad B = \left| \sum_{S \subseteq [n]} \hat{f}(S)^3 \right| \]
Proof

Lemma

*First Direction: \( A \geq B \)*

- Let \( B' := \sum_{S \subseteq [n]} \hat{f}(S)^3 \)
- Let \( B'_+ = \sum_{S \subseteq [n]: \hat{f}(S) \geq 0} \hat{f}(S)^3 \) and \( B'_- = \sum_{S \subseteq [n]: \hat{f}(S) < 0} \hat{f}(S)^3 \)
- Let \( C_+ = \sum_{S \subseteq [n]: \hat{f}(S) \geq 0} \hat{f}(S)^2 \) and \( C_- = \sum_{S \subseteq [n]: \hat{f}(S) < 0} \hat{f}(S)^2 \)
- Let \( A' = \max_{S \subseteq [n]: \hat{f}(S) \geq 0} \hat{f}(S) \)
- Note that:

\[
B'_+ + B'_- = B' \\
\implies B'_+ \geq B' \\
\implies A' \cdot C_+ \geq B'_+ \geq B' \\
\implies A \geq A' \geq B'/C_+ \geq B'
\]

- Now perform the same analysis with \(-\hat{f}(S)\) instead if \( \hat{f}(S) \)
  and get \( A \geq -B' \) and, hence, the result follows
**Lemma**

*Other Direction:* If \( A \geq (1 - \varepsilon) \) implies \( B \geq (1 - 4\varepsilon) \), for \( 0 \leq \varepsilon \leq 1/4 \)

- Suppose \( A' \geq (1 - \varepsilon) \), then \( B'_+ \geq (1 - \varepsilon)^3 \)
- Then \( C_- = 1 - C_+ \leq 1 - (1 - \varepsilon)^2 = \varepsilon(2 - \varepsilon) \)
- Then \( B'_- \geq -[\varepsilon(2 - \varepsilon)]^{3/2} \)
- Now, we have \( B' = B'_+ + B'_- \geq (1 - \varepsilon)^3 - [\varepsilon(2 - \varepsilon)]^{3/2} \)
- We can show that: \( B' \geq (1 - 4\varepsilon) \)
- If \( \min_{S \subseteq [n]: \hat{f}(S) < 0} \hat{f}(S) \leq -(1 - \varepsilon) \), we perform the above analysis with \( -\hat{f}(S) \) instead of \( f(S) \) and get \( B' \leq -(1 - 4\varepsilon) \)
- Hence we get the result
Finding $S$

- Suppose $f$ is close to $\chi_S$, then how do we recover $S$?
- Closely related to the problem of “Decoding Hadamard code”
List Decoding of Hadamard Code

- Hadamard Code establishes the following mapping:
  \[ S \rightarrow H(S) := \chi_S \]
- Note that \( H(S) \) and \( H(T) \), where \( T \neq S \), differs in exactly \( N/2 \) positions
- Hadamard code has distance \( N/2 \)
- Decoding takes as input a function \( f : \{0, 1\}^n \rightarrow \{-1, +1\} \) and outputs the nearest \( \chi_S \)

**Lemma**

Let \( \Delta(f, \chi_S) \) be the distance between \( f \) and \( \chi_S \). Then
\[
\hat{f}(S) = 1 - 2\delta(f, \chi_S), \text{ where } \delta(\cdot, \cdot) = \Delta(\cdot, \cdot)/N.
\]

- If \( \delta(f, \chi_S) = \frac{1}{2} - \varepsilon \), then: \( \hat{f}(S) = 2\varepsilon \)
Unique Decoding up to “Error rate < 1/4”:

- “Error rate $\frac{1}{2} - \varepsilon < 1/4$” is equivalent to “$\varepsilon > 1/4$”
- Then there exists $S$ such that $\hat{f}(S) = 2\varepsilon > 1/2$
- There cannot exist $T \neq S$ such that $\hat{f}(T) > 1/2$. Reason: If possible there exists $T \neq S$ such that $\hat{f}(T) = 2\varepsilon' > 1/2$. Then, we have:

$$\delta(f, \chi_S) + \delta(f, \chi_T) = 1 - (\varepsilon + \varepsilon') < 1/2$$

But we have:

$$1/2 = \delta(\chi_S, \chi_T) \leq \delta(f, \chi_S) + \delta(f, \chi_T)$$

A Contradiction.
Suppose “Error rate $\leq \frac{1}{2} - \varepsilon$”

Then $\hat{f}(S) \geq 2\varepsilon$

Note that:

$$1 = \|f\|_2^2 = \sum_{S \subseteq [n]} \hat{f}(S)$$

There can be at most $1/4\varepsilon^2$ subsets $S$ with $\hat{f}(S)^2 \geq 4\varepsilon^2$
Consider a distribution $\rho$ over $\{0,1\}^n$ that sets each bit independently to 1 with probability $\epsilon$, and sets it to 0 with probability $(1 - \epsilon)$

Therefore $\rho(x) = (1 - \epsilon)^{n - \text{wt}(x)} \cdot \epsilon^{\text{wt}(x)}$

Let $\rho = (1 - 2\epsilon)$

Lemma

$$N\hat{\rho}(S) = \rho^{|S|}$$
Proof of Lemma

\[
\sum_{x \in \{0,1\}^n} p(x) \chi_S(x) = \sum_{x \in \{0,1\}^n} (1 - \varepsilon)^{n - \text{wt}(x)} \cdot \varepsilon^{\text{wt}(x)} \cdot (-1)^{S \cdot x}
\]

\[
= (1 - \varepsilon)^n \sum_{x \in \{0,1\}^n} \left( \frac{\varepsilon}{1 - \varepsilon} \right)^{\text{wt}(x)} (-1)^{S \cdot x}
\]

\[
= (1 - \varepsilon)^n \sum_{0 \leq w \leq n} \lambda^w \sum_{0 \leq i \leq w} \binom{|S|}{i} \left( n - |S| \right)^{w - i} (-1)^i
\]

where \( \lambda = \varepsilon / (1 - \varepsilon) \)

\[
= (1 - \varepsilon)^n \sum_{0 \leq w \leq n} [X^w](1 - \lambda X)^{|S|}(1 + \lambda X)^{(n - |S|)}
\]

\[
= (1 - \varepsilon)^n \left[ (1 - \lambda X)^{|S|}(1 + \lambda X)^{(n - |S|)} \right]_{X=1}
\]

\[
= (1 - \varepsilon)^n(1 + \lambda)^n \left( \frac{1 - \lambda}{1 + \lambda} \right)^{|S|} = (1 - 2\varepsilon)^{|S|}
\]
Noisy Version of a Function

- \( \tilde{f}(x) \) is computed by sampling \( r \sim p \) and then outputting \( f(x + r) \)
- Let \( T_\rho \) be a mapping that maps the function \( f \) to \( \tilde{f} \)
- Note that:
  \[
  \tilde{f}(x) = \sum_{r \in \{0,1\}^n} p(r)f(x + r) = (p \ast f)(x)
  \]
- Think: \( T_\rho \) is a linear map

**Lemma**

\[
\hat{\tilde{f}}(S) = \rho^{|S|} \hat{f}(S)
\]

- Proof: \( \hat{\tilde{f}}(S) = N\hat{p}(S)\hat{f}(S) = \rho^{|S|} \hat{f}(S) \)
- Intuition: \( T_\rho \) smoothes \( f \) by attenuating the higher Fourier coefficients in \( f \) more

Lecture 21: Basic Applications of Fourier Analysis (BLR-Test, List-Decoding Hadamard Codes, Smoothening Functions)