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

BLR Linearity Testing

- "BLR" = Blum, Luby, Rubinfeld
- Problem: Given an oracle access to a function $f\colon \{0,1\}^n \to \{+1,-1\}$, 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

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

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

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

Proof

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

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

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

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

$$A = \max_{S \subseteq [n]} \left| \widehat{f}(S) \right| \qquad B = \left| \sum_{S \subseteq [n]} \widehat{f}(S)^3 \right|$$

Proof

Lemma

First Direction: $A \geqslant B$

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

$$\begin{aligned} B'_+ + B'_- &= B' \\ \implies \qquad B'_+ &\geqslant B' \\ \implies \qquad A'\cdot C_+ \geqslant B'_+ &\geqslant B' \\ \implies \qquad A \geqslant A' &\geqslant B'/C_+ \geqslant B' \end{aligned}$$

- Now perform the same analysis with $-\widehat{f}(S)$ instead if $\widehat{f}(S)$ and get $A \geqslant -B'$ and, hence, the result follows

Proof

Lemma

Other Direction: If $A \geqslant (1-\varepsilon)$ *implies* $B \geqslant (1-4\varepsilon)$, *for* $0 \leqslant \varepsilon \leqslant 1/4$

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

Finding S

- Suppose f is close to χ_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: $S \to H(S) := \chi_S$
- 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 $f \colon \{0,1\}^n \to \{-1,+1\}$ and outputs the nearest χ_S

Lemma

Let $\Delta(f, \chi_S)$ be the distance between f and χ_S. Then $\widehat{f}(S) = 1 - 2\delta(f, \chi_S)$, where $\delta(\cdot,\cdot) = \Delta(\cdot,\cdot)/N$.

- If $\delta(f, \chi_S) = \frac{1}{2} - \varepsilon$, then: $\widehat{f}(S) = 2\varepsilon$

Unique Decoding

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 $\widehat{f}(S) = 2\varepsilon > 1/2$
- There cannot exist $T \neq S$ such that $\widehat{f}(T) > 1/2$. Reason: If possible there exists $T \neq S$ such that $\widehat{f}(T) = 2\varepsilon' > 1/2$. Then, we have:

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

But we have:

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

A Contradiction.

List Decoding

List Decoding up to "Error rate $< 1/2$":

- Suppose "Error rate $\leqslant \frac{1}{2} - \varepsilon$"
- Then $\widehat{f}(S) \geqslant 2\varepsilon$
- Note that:

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

- There can be at most $1/4\varepsilon^2$ subsets S with $\widehat{f}(S)^2 \geqslant 4\varepsilon^2$

Error Function

- Consider a distribution p over $\{0,1\}^n$ that sets each bit independently to 1 with probability ε, and sets it to 0 with probability $(1-\varepsilon)$
- Therefore $p(x) = (1-\varepsilon)^{n-\mathrm{wt}(x)} \cdot \varepsilon^{\mathrm{wt}(x)}$
- Let $\rho = (1-2\varepsilon)$

Lemma

$$N\widehat{p}(S) = \rho^{|S|}$$

Proof of Lemma

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

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

$$= (1-\varepsilon)^n \sum_{0\leqslant w\leqslant n} \lambda^w \sum_{0\leqslant i\leqslant w} \binom{|S|}{i}\binom{n-|S|}{w-i}(-1)^i$$

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

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

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

$$= (1-\varepsilon)^n(1+\lambda)^n \left(\frac{1-\lambda}{1+\lambda}\right)^{|S|} = (1-2\varepsilon)^{|S|}$$

Noisy Version of a Function

- $\widetilde{f}(x)$ is computed by sampling $r \sim p$ and then outputting $f(x+r)$
- Let T_ρ be a mapping that maps the function f to $\widetilde{f}$
- Note that:

$$\widetilde{f}(x) = \sum_{r \in \{0,1\}^n} p(r) f(x+r) = (p * f)(x)$$

- Think: T_ρ is a linear map

Lemma

$$\widehat{\widetilde{f}}(S) = \rho^{|S|} \widehat{f}(S)$$

- Proof: $\widehat{\widetilde{f}}(S) = N\widehat{p}(S)\widehat{f}(S) = \rho^{|S|}\widehat{f}(S)$
- Intuition: T_ρ smoothes f by attenuating the higher Fourier coefficients in f more