Lecture 19: BLR Linearity Testing

Paper of interest

- Manuel Blum, Michael Luby, Ronitt Rubinfeld: Self-Testing/Correcting with Applications to Numerical Problems. J. Comput. Syst. Sci. 47(3): 549-595 (1993)
- Manuel Blum, Michael Luby, Ronitt Rubinfeld: Self-Testing/Correcting with Applications to Numerical Problems. STOC 1990: 73-83

Setting

- Our objective is to study functions with boolean output $f : \{0,1\}^n \to \{+1,-1\}$
- Consider the following definition of linear functions

Definition (Linear Function)

A function $f : \{0,1\}^n \to \{+1,-1\}$ is a linear function if, for all $x, y \in \{0,1\}^n$, we have $f(x+y) = f(x) \cdot f(y)$.

- Note that the function χ_S is linear, for any $S \in \{0,1\}^n$. In fact, we can prove (by induction) that these are the only linear functions. That is, if f is a linear function then f is identical to χ_S, for some $S \in \{0,1\}^n$
- **Objective.** We want to test, given an oracle access to a function f, whether f is close to a linear function or not. That is, we want to test whether a given function f agrees with χ_S, for some $S \in \{0,1\}^n$, at a large fraction of inputs

BLR Linearity Testing Algorithm

- Blum-Luby-Rubinfeld algorithm is presented below

BLR^f

1. Pick random $x, y \xleftarrow{\$} \{0,1\}^n$
2. Return $f(x) \cdot f(x) == f(x+y)$

- We emphasize that this algorithm has an oracle access to the function f. That is, it can only study the function f's input-output behavior
- Our objective is to prove that "f is close to linear" if and only if "the probability of BLR^f outputting true is close to 1"
- Note that observing one output of the BLR^f algorithm to be true does not certify that the function f is linear (or, close to linear)!

Proof Overview

- We shall state a few useful results (without proof) and prove our main theorem based on these results
- Finally, to complete the proof, we shall prove these (unproven) results

Useful Results

- Result 1: Characterization of Boolean Functions

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

- Result 2: Characterization of "close-to-linear functions"

Lemma

A function $f : \{0,1\}^n \to \{+1,-1\}$ *agrees with some linear function at* $\geqslant (1-\varepsilon)$ *fraction of the inputs, if and only if there exists* $S \in \{0,1\}^n$ *such that* $\widehat{f}(S) \geqslant (1-2\varepsilon)$.

- Result 3: Characterization of "$\mathbb{P}\left[\mathrm{BLR}^f = \mathrm{true}\right]$"

Lemma

$$\mathbb{P}\left[\mathrm{BLR}^f = \mathit{true}\right] = \frac{1 + \sum_{T \in \{0,1\}^n} \widehat{f}(T)^3}{2}$$

- We shall show the following theorem

Theorem

If f agrees with a linear function at $\geqslant (1-\varepsilon)$ fraction of the inputs, then $\mathbb{P}\left[\text{BLR}^f = \textit{true}\right] \geqslant 1 - 6\varepsilon$.

- Let us start the proof. Note that f agrees with a linear function at $\geqslant (1-\varepsilon)$ fraction of the inputs. So, there exists $S \in \{0,1\}^n$ such that $\widehat{f}(S) \geqslant 1 - 2\varepsilon$ (By Result 2)
- By Result 1, we have $\sum_{T \in \{0,1\}^n} \widehat{f}(T)^2 = 1$. So, we conclude that

$$\sum_{T \in \{0,1\}^n :\ T \neq S} \widehat{f}(T)^2 = 1 - \widehat{f}(S)^2 \leqslant 1 - (1-2\varepsilon)^2 \leqslant 4\varepsilon$$

That is, we conclude that $\sum_{T \in \{0,1\}^n :\ T \neq S} \widehat{f}(T)^2$ is small

- Note that $\sum_{T \in \{0,1\}^n:\ T \neq S} \widehat{f}(T)^3$ can be negative. However, we want to show that its magnitude cannot be too large. To prove this inequality, we need the following mathematical inequality, which is easy to prove using Jensen's inequality.

Claim

Let $a_1, \ldots, a_K$ be non-negative numbers such that $\sum_{i=1}^{K} a_i \leqslant 4\varepsilon$. Then, the following bound holds

$$\sum_{i=1}^{K} a_i^{3/2} \leqslant 8\varepsilon^{3/2}$$

From this inequality, we conclude that

$$\sum_{T \in \{0,1\}^n:\ T \neq S} \left|\widehat{f}(T)^3\right| \leqslant 8\varepsilon^{3/2}$$

That is, we conclude that

$$\sum_{T \in \{0,1\}^n :\ T \neq S} \widehat{f}(T)^3 \geqslant -8\varepsilon^{3/2}$$

- By adding $\widehat{f}(S)^3$ to this expression above, we get

$$\sum_{T \in \{0,1\}^n} \widehat{f}(T)^3 \geqslant 1 - 4\varepsilon - 8\varepsilon^{3/2}$$

- By Result 3, we get

$$\mathbb{P}\left[\mathrm{BLR}^f = \mathrm{true}\right] \geqslant 1 - 2\varepsilon - 4\varepsilon^{3/2} \geqslant 1 - 6\varepsilon$$

- We shall show the following theorem

Theorem

If $\mathbb{P}\left[\text{BLR}^f = \textit{true}\right] \geqslant 1-\varepsilon$ *then* f *agrees with a linear function at* $\geqslant (1-\varepsilon)$ *fraction of the inputs*

- Let us start the proof. If $\mathbb{P}\left[\text{BLR}^f = \text{true}\right] \geqslant 1-\varepsilon$ then by Result 3 we have

$$\sum_{T \in \{0,1\}^n} \widehat{f}(T)^3 \geqslant 1 - 2\varepsilon$$

- Note that

$$\begin{aligned}\sum_{T\in\{0,1\}^n} \widehat{f}(T)^3 &\leqslant \sum_{T\in\{0,1\}^n} \widehat{f}(T)^2 \max_{R\in\{0,1\}^n} \widehat{f}(R) \\ &= \max_{R\in\{0,1\}^n} \widehat{f}(R) \sum_{T\in\{0,1\}^n} \widehat{f}(T)^2 \\ &= \max_{R\in\{0,1\}^n} \widehat{f}(R)\end{aligned}$$

  The last equality uses Result 1.

- We know that $\sum_{T\in\{0,1\}^n} \widehat{f}(T)^3 \geqslant 1-2\varepsilon$. So, we conclude that

$$\max_{R\in\{0,1\}^n} \widehat{f}(R) \geqslant 1-2\varepsilon$$

  That is, there exists $S \in \{0,1\}^n$, such that $\widehat{f}(S) \geqslant 1-2\varepsilon$.

- By Result 2, f agrees with χ_S at $\geqslant (1-\varepsilon)$ fraction of the inputs

Proof of Result 1

- Note that $\langle f, f \rangle = 1$, when $f : \{0,1\}^n \to \{+1,-1\}$
- By Parseval's identity, we have $1 = \langle f, f \rangle = \sum_{T \in \{0,1\}^n} \widehat{f}(T)^2$

Proof of Result 2

- Suppose f agrees with some linear function at ρ fraction of the inputs. We can conclude that f disagrees with that linear function at $(1-\rho)$ fraction of the inputs
- Since the Fourier basis is the set of all linear functions, we get that f agrees with χ_S at ρ fraction of the inputs, for some $S \in \{0,1\}^n$
- So, we conclude that

$$\widehat{f}(S) = \langle f, \chi_S \rangle = \frac{1}{N}\left(\rho N \cdot 1 + (1-\rho)N \cdot (-1)\right) = 2\rho - 1$$

- Note that $\rho \geqslant 1-\varepsilon$ if and only if $\widehat{f}(S) \geqslant 1-2\varepsilon$

- Suppose that $p := \mathbb{P}\left[\mathrm{BLR}^f = \text{true}\right]$
- Let us consider the sum

$$\frac{1}{N^2} \sum_{x,y \in \{0,1\}^n} f(x)f(y)f(x+y)$$

Note that $f(x)f(y)f(x+y) = 1$ if $f(x)f(y) = f(x+y)$; otherwise $f(x)f(y)f(x+y) = -1$.
Equivalently, $f(x)f(y)f(x+y) = 1$ if $\mathrm{BLR}^f = \text{true}$ for this choice of x and y; otherwise $f(x)f(y)f(x+y) = -1$. So, we conclude that

$$\frac{1}{N^2} \sum_{x,y \in \{0,1\}^n} f(x)f(y)f(x+y) = p \cdot 1 + (1-p) \cdot (-1) = 2p - 1$$

That is

$$p = \frac{1 + \frac{1}{N^2} \sum_{x,y \in \{0,1\}^n} f(x) f(y) f(x+y)}{2}$$

- So, to prove Result 3, it suffices to prove that

$$\frac{1}{N^2} \sum_{x,y \in \{0,1\}^n} f(x) f(y) f(x+y) = \sum_{T \in \{0,1\}^n} \widehat{f}(T)^3$$

- To prove this statement, consider a new function $h \colon \{0,1\}^n \to \mathbb{R}$.

$$h(z) = \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x) f(z-x)$$

- First, observe that $h = (f * f)$, and

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

- By Plancherel identity, we have

$$\langle h, f \rangle = \sum_{T \in \{0,1\}^n} \widehat{h}(T) \cdot \widehat{f}(T) = \sum_{T \in \{0,1\}^n} \widehat{f}(T)^2 \cdot \widehat{f}(T) = \sum_{T \in \{0,1\}^n} \widehat{f}(T)^3$$

Here we use the fact that $\widehat{h}(S) = \widehat{f}(S)^2$ by properties of convolution.