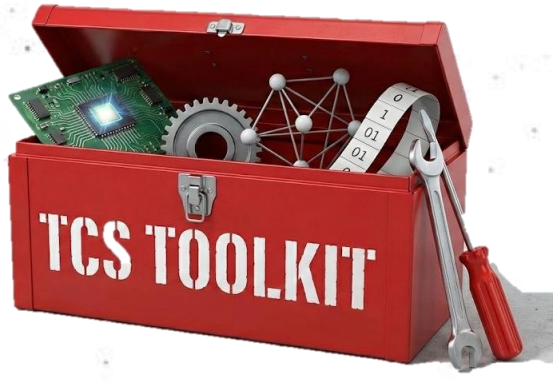
CS 58500 – Theoretical Computer Science Toolkit

Lecture 17 (04/09)

Boolean Function Analysis (II)



https://ruizhezhang.com/course_spring_2026.html

Today's Lecture

- Linearity Testing
- Random Restriction

Linearity Testing

A function $f:\{0,1\}^n \to \{-1,1\}$ is said to be linear if for any $x, y \in \{0,1\}^n$, it holds that

$$f(x)f(y) = f(x+y)$$

Suppose you are given query access to an unknown function $f:\{0,1\}^n \to \{-1,1\}$ and your goal is to test whether f is a linear function or not

- This is a question from a field known as Property Testing
- The current setting has an issue: if f agrees with some linear function on all but one input x^*, then it will be hard to test f

The objective of property testing is to distinguish:

1. YES: f is linear
2. NO: f is far from all linear functions

Linearity Testing

For two Boolean functions $f, g: \{0,1\}^n \to \{-1,1\}$, define the distance

$$\Delta(f,g) \coloneqq \frac{1}{N}|\{x \in \{0,1\}^n : f(x) \neq g(x)\}|$$

We want to use as few queries as possible to test the distance between f and the set of linear functions

Blum-Luby-Rubinfeld (BLR) Test

- Uniformly sample $x, y \in \{0,1\}^n$
- "Accept" if $f(x+y) = f(x)f(y)$

Blum-Luby-Rubinfeld '90: If the BLR test accepts with probability $1-\epsilon$, then f is ϵ-close to some linear function

Linearity Testing

Blum-Luby-Rubinfeld (BLR) Test

- Uniformly sample $x, y \in \{0,1\}^n$
- "Accept" if $f(x+y) = f(x)f(y)$

- If $f(x) = \pm 1$ uniformly at random, then the accept probability is $1/2$
- Suppose $f(x+y) = f(x)f(y)$ holds with probability $1/2 + \delta$, what can we say about f?
  - Large δ, i.e. $\delta = 1/2 - \epsilon$
  - Small $\delta > 0$

Linearity Testing

Theorem. Suppose $f:\{0,1\}^n \to \{-1,1\}$ is a function such that $\Pr[f(x+y) = f(x)f(y)] \geq \frac{1}{2} + \delta$. Then there exists $S \subseteq [n]$ such that $\hat{f}(S) \geq 2\delta$

Proof.

- Note that if f passes the BLR test, then $f(x+y)f(x)f(y) = 1$; otherwise $f(x+y)f(x)f(y) = -1$
- Thus,

$$\mathbb{E}[f(x+y)f(x)f(y)] = \Pr[f(x+y) = f(x)f(y)] - \Pr[f(x+y) \neq f(x)f(y)]$$
$$= 2\Pr[f(x+y) = f(x)f(y)] - 1 \geq 2\delta$$

- Recall the convolution: $(f \star g)(x) = \mathbb{E}_y[f(y)g(x+y)]$

$$\mathbb{E}_{x,y}[f(x+y)f(x)f(y)] = \mathbb{E}_x\left[f(x)\mathbb{E}_y[f(y)f(x+y)]\right] = \mathbb{E}_x[f(x)(f \star f)(x)] = \langle f, f \star f \rangle$$
$$= \sum_S \hat{f}(S)\widehat{(f \star f)}(S) = \sum_S \hat{f}(S)^3 \leq \max_S \hat{f}(S) \sum_T \hat{f}(T)^2 = \max_S \hat{f}(S)\,\|f\|_2^2 = \max_S \hat{f}(S)$$

■

Linearity Testing

Theorem. Suppose $f:\{0,1\}^n \to \{-1,1\}$ is a function such that $\Pr[f(x+y) = f(x)f(y)] \geq \frac{1}{2} + \delta$. Then there exists $S \subseteq [n]$ such that $\hat{f}(S) \geq 2\delta$

- $\hat{f}(S) = \langle f, \chi_S \rangle = \mathbb{E}[f(x)\chi_S(x)] = 2\Pr[f(x) = \chi_S(x)] - 1 \geq 2\delta$
- Therefore, $\Delta(f, \chi_S) = \Pr[f(x) = \chi_S(x)] \geq \frac{1}{2} + \delta$
- For $\delta = \frac{1}{2} - \epsilon$, we obtain that if f passes the BLR test with probability $1 - \epsilon$, then f is ϵ-close to χ_S for some $S \subseteq [n]$

Linearity Testing

A property $\mathcal{P}$ of Boolean functions is testable with $q(\epsilon)$ queries if there exists a randomized algorithm $\mathcal{A}$ (which gets ϵ as input) such that for all $\epsilon > 0$ it makes $q(\epsilon)$ queries and satisfies:

- If $f \in \mathcal{P}$, then $\Pr[\mathcal{A} \text{ accepts}] \geq 2/3$
- If f is ϵ-far from $\mathcal{P}$, then $\Pr[\mathcal{A} \text{ accepts}] \leq 1/3$

Corollary. The property of being a linear function is testable with $\mathcal{O}(1/\epsilon)$ queries.

Linearity Testing

- BLR test does not reveal which linear function χ_S is close to

Proposition (Local Correctability of Linear Functions**).** Suppose $f:\{0,1\}^n \to \{-1,1\}$ is ϵ-close to the linear function χ_S. Then for every $x \in \{0,1\}^n$, the following algorithm outputs $\chi_S(x)$ with probability at least $1-2\epsilon$:

- Uniformly sample $y \in \{0,1\}^n$
- Output $f(y)f(x+y)$

Proof.

- Since y and $x+y$ are uniformly distributed over $\{0,1\}^n$ (though not independent), we have
$$\Pr[f(y) \neq \chi_S(y)] \leq \epsilon, \qquad \Pr[f(x+y) \neq \chi_S(x+y)] \leq \epsilon$$
- By union bound, $\Pr[f(y) = \chi_S(y) \wedge f(x+y) = \chi_S(x+y)] \geq 1-2\epsilon$
- In this case, $f(y)f(x+y) = \chi_S(y+x+y) = \chi_S(x)$

Linearity Testing

BLR test has many important applications in TCS:

- Local tester for the Hadamard code
- Probabilistic checkable proofs (PCPs)
- Hardness of approximations
- Additive combinatorics (Roth's theorem: every dense subset of $[N]$ contains a 3-term arithmetic progression)
- …

Today's Lecture

- Linearity Testing
- Random Restriction

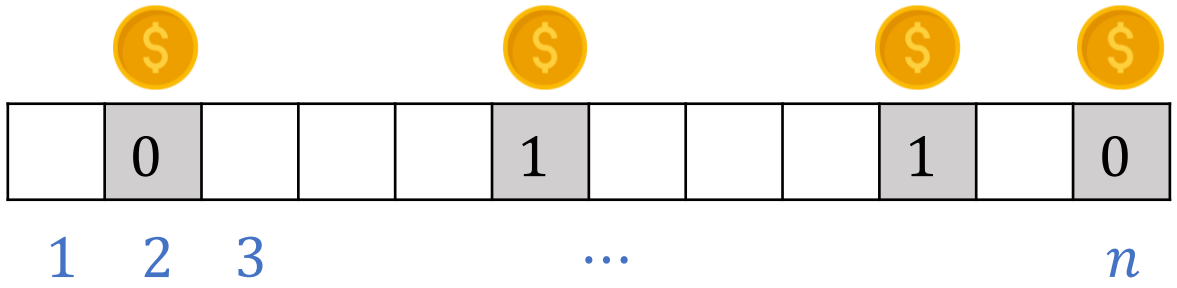
Random Restriction

Random Restriction is a very powerful tool in Boolean function analysis

- It is convenient to identify the index $S \in \{0,1\}^n$ of a Fourier coefficient $\hat{f}(S)$ as a subset of $[n]$
- Suppose we have a function $f: \{0,1\}^n \to \mathbb{R}$, a set of coordinates $J \subseteq [n]$, and an assignment $z \in \{0,1\}^{\bar{J}}$. The restricted function $f_{\bar{J}\to z}: \{0,1\}^n \to \{-1,1\}$ is defined by

$$f_{\bar{J}\to z}(y) \coloneqq f\left(x_J = y, x_{\bar{J}} = z\right)$$

- Given $f: \{0,1\}^n \to \mathbb{R}$ and $J \subseteq [n]$, a random restriction of f on J is a function $f_{\bar{J}\to z}$ wherein $z \in \{0,1\}^{\bar{J}}$ is sampled uniformly at random



Random Restriction

Lemma. Let $f:\{0,1\}^n \to \mathbb{R}$, $J \subseteq [n]$, $z \in \{0,1\}^{\bar{J}}$. We have

$$\widehat{f_{\bar{J}\to z}}(S) = \sum_{T\subseteq \bar{J}} \hat{f}(S \cup T)\chi_T(z) \qquad \forall S \subseteq J \ (\Leftrightarrow S \in \{0,1\}^J)$$

Proof.

- We can decompose the Fourier transform into the J part and the $\bar{J}$ part:

$$f(x) = \sum_{S\subseteq J, T\subseteq \bar{J}} \hat{f}(S \cup T)\chi_S\left(x_J\right)\chi_T\left(x_{\bar{J}}\right)$$

- Thus, we have

$$f_{\bar{J}\to z}(y) = \sum_{S\subseteq J, T\subseteq \bar{J}} \hat{f}(S \cup T)\chi_S(y)\chi_T(z) = \sum_{S\subseteq J}\left(\sum_{T\subseteq \bar{J}} \hat{f}(S \cup T)\chi_T(z)\right)\chi_S(y)$$

■

Random Restriction

Lemma. Let $f:\{0,1\}^n \to \mathbb{R}$, $J \subseteq [n]$, $z \in \{0,1\}^{\bar{J}}$. We have

$$\widehat{f_{\bar{J}\to z}}(S) = \sum_{T\subseteq \bar{J}} \hat{f}(S \cup T)\chi_T(z) \qquad \forall S \subseteq J \ (\Leftrightarrow S \in \{0,1\}^J)$$

Claim. Let $f:\{0,1\}^n \to \mathbb{R}$, $J \subseteq [n]$, $z \in \{0,1\}^{\bar{J}}$, and $S \subseteq J$. We have

$$\mathbb{E}_z\left[\widehat{f_{\bar{J}\to z}}(S)^2\right] = \sum_{T\subseteq \bar{J}} \hat{f}(S \cup T)^2$$

Proof.

- Define $g(z) \coloneqq \widehat{f_{\bar{J}\to z}}(S)$. Then the lemma gives that $\hat{g}(T) = \hat{f}(S \cup T)$
- The claim then follows from Parseval

■

Random Restriction

In some applications, it is useful to consider p-random restrictions

- Given a function $f:\{0,1\}^n \to \mathbb{R}$ and a parameter $p \in [0,1]$, a p-random restriction is sampled by taking $J \subseteq [n]$ randomly by including each $i \in [n]$ in J with probability p, and then taking $z \in \{0,1\}^{\bar{J}}$

Examples:

- Monomial/Fourier basis $\chi_S(x) = (-1)^{\langle S,x \rangle}$: if we take (J,z) a p-random restriction, then we expect $f_{\bar{J}\to z}$ is a (signed) monomial of degree $p|S|$

  → Random restriction "reduces" the degree of monomials

Random Restriction

In some applications, it is useful to consider p-random restrictions

- Given a function $f:\{0,1\}^n \to \mathbb{R}$ and a parameter $p \in [0,1]$, a p-random restriction is sampled by taking $J \subseteq [n]$ randomly by including each $i \in [n]$ in J with probability p, and then taking $z \in \{0,1\}^{\bar{J}}$

Examples:

- OR function $f(x) = \bigvee_{i \in I} x_i$: under the p-random restriction (J, z),
  - $f_{\bar{J} \to z} \equiv 1$ if there is a variable I_i in J receiving value 1 (What is the probability of this case?)
  - $f_{\bar{J} \to z}$ is an OR function on roughly $p|I|$ variables

Random Restriction

In some applications, it is useful to consider p-random restrictions

- Given a function $f:\{0,1\}^n \to \mathbb{R}$ and a parameter $p \in [0,1]$, a p-random restriction is sampled by taking $J \subseteq [n]$ randomly by including each $i \in [n]$ in J with probability p, and then taking $z \in \{0,1\}^{\bar{J}}$

Examples:

- CNF formula $f(x) = \bigwedge_{i\in[m]} \bigvee_{j\in I_i} x_j$: under the p-random restriction (J, z),
  - If a term $\bigvee_{j\in I_i} x_j$ becomes completely 0, then $f_{\bar{J}\to z} \equiv 0$
  - Terms that become 1 disappear
  - The rest considerably shrink in width
  - The Håstad switching lemma

Random Restriction

Recall that the Fourier weight of $f:\{0,1\}^n \to \mathbb{R}$ at level d is defined as

$$\mathbf{W}^d[f] = \sum_{|S|=d} \hat{f}(S)^2$$

We also define $\mathbf{W}^{\leq d}[f] \coloneqq \sum_{k=0}^{d} \mathbf{W}^k[f]$ and $\mathbf{W}^{\geq d}[f] \coloneqq \sum_{k=d}^{n} \mathbf{W}^k[f]$

Lemma. Let $f:\{0,1\}^n \to \mathbb{R}$, $d \in \mathbb{N}$, and let (J,z) be a p-random restriction. Then

$$\mathbb{E}_{J,z}\left[\mathbf{W}^d\left[f_{\overline{J}\to z}\right]\right] = \sum_{Q\in\{0,1\}^n} \hat{f}(Q)^2 \Pr[\mathrm{Bin}(|Q|,p) = d]$$

Random Restriction

Lemma. Let $f:\{0,1\}^n \to \mathbb{R}$, $d \in \mathbb{N}$, and let (J,z) be a p-random restriction. Then

$$\mathbb{E}_{J,z}\left[\mathbf{W}^d\left[f_{\overline{J}\to z}\right]\right] = \sum_{Q\in\{0,1\}^n} \hat{f}(Q)^2 \Pr[\mathrm{Bin}(|Q|,p) = d]$$

Proof.

$$\mathbb{E}_{J,z}\left[\mathbf{W}^d\left[f_{\overline{J}\to z}\right]\right] = \mathbb{E}_{J,z}\left[\sum_{S\subseteq J:|S|=d} \widehat{f_{\overline{J}\to z}}(S)^2\right] = \mathbb{E}_J\left[\sum_{|S|=d} \mathbf{1}_{S\subseteq J}\mathbb{E}_z\left[\widehat{f_{\overline{J}\to z}}(S)^2\right]\right]$$

$$= \mathbb{E}_J\left[\sum_{|S|=d} 1_{S\subseteq J}\sum_{T\subseteq\overline{J}} \hat{f}(S\cup T)^2\right] = \sum_Q \mathbb{E}_J\left[1_{|Q\cap J|=d}\right]\hat{f}(Q)^2$$

$$= \sum_Q \hat{f}(Q)^2 \Pr[\mathrm{Bin}(|Q|,p) = d]$$

■

Random Restriction

If f has most of its Fourier mass below level d, then $f_{\overline{J}\to z}$ has most of its Fourier mass below level $\approx pd$

Corollary. Suppose that $f:\{0,1\}^n \to \{-1,1\}$ satisfies $\mathbf{W}^{\geq d}[f] \leq \epsilon$, and let (J,z) be a p-random restriction. Then

$$\mathbb{E}_{J,z}\left[\mathbf{W}^{\geq 2pd}\left[f_{\overline{J}\to z}\right]\right] \leq \epsilon + e^{-\Theta(pd)}$$

Proof.

- The previous lemma implies that

$$\mathbb{E}_{J,z}\left[\mathbf{W}^{\geq 2pd}\left[f_{\overline{J}\to z}\right]\right] = \sum_Q \hat{f}(Q)^2 \Pr[\mathrm{Bin}(|Q|,p) \geq 2pd] = \sum_{k\geq 0} \mathbf{W}^k[f] \Pr[\mathrm{Bin}(k,p) \geq 2pd]$$

$$= \underbrace{\sum_{k\geq d} \mathbf{W}^k[f] \Pr[\mathrm{Bin}(k,p) \geq 2pd]}_{\leq \mathbf{W}^{\geq d}[f] \leq \epsilon} + \sum_{k<d} \mathbf{W}^k[f] \Pr[\mathrm{Bin}(k,p) \geq 2pd]$$

Random Restriction

If f has most of its Fourier mass below level d, then $f_{\overline{J}\to z}$ has most of its Fourier mass below level $\approx pd$

Corollary. Suppose that $f:\{0,1\}^n \to \{-1,1\}$ satisfies $\mathbf{W}^{\geq d}[f] \leq \epsilon$, and let (J,z) be a p-random restriction. Then

$$\mathbb{E}_{J,z}\left[\mathbf{W}^{\geq 2pd}\left[f_{\overline{J}\to z}\right]\right] \leq \epsilon + e^{-\Theta(pd)}$$

Proof.

- For $k < d$, we have

$$\Pr[\mathrm{Bin}(k,p) \geq 2pd] \leq \Pr[\mathrm{Bin}(d,p) \geq 2pd] \leq \exp\left(-\Theta(pd)\right)$$

$$\sum_{k<d} \mathbf{W}^k[f] \Pr[\mathrm{Bin}(k,p) \geq 2pd] \leq \sum_{k\geq 0} \mathbf{W}^k[f] \exp\left(-\Theta(pd)\right) = \|f\|_2^2 \exp\left(-\Theta(pd)\right)$$

■

Random Restriction

If f has sizable mass around level d, then $f_{\overline{J}\to z}$ has sizable weight around level pd

Corollary. Let $d \in \mathbb{N}$ and $p \in [0,1]$ be such that $pd \geq 10$. Suppose that $f: \{0,1\}^n \to \{-1,1\}$, and let (J, z) be a p-random restriction. Define the weight around level d to be

$$\mathbf{W}^{\approx d}[f] \coloneqq \sum_{d \leq k \leq 2d} \mathbf{W}^k[f]$$

Then

$$\mathbb{E}_{J,z}\left[\mathbf{W}^{\approx pd}\left[f_{\overline{J}\to z}\right]\right] \geq \Omega\left(\mathbf{W}^{\approx d}[f]\right)$$