COMS E6998-9: Algorithmic Techniques for Massive Data — Nov 19, 2015

Lecture 21: Linearity Testing

Instructor: *Alex Andoni* — Scribe: *Nikita Nataraj*

1 Linear Testing

Given a function f, in linear testing we determine whether it is a linear function: i.e., $f(x+y) = f(x)+f(y)$ for all x, y. Assume that we have the following function:

$$f : \{0,1\}^n \to R$$
$$x \xrightarrow{f} f(x)$$

We can think of $f(x)$ is being describe as a complete truth table, as we can sample $f(x)$. To make this proof easier we map the boolean onto +1 and -1.

$$0 \to +1$$
$$1 \to -1$$

From now on, we will consider the function

$$f : \{+1,-1\}^n \to \{+1,-1\}$$

Definition 1. *f is linear if* $\forall x, y \in \{+1,-1\}^n$

$$f(x \oplus y) = f(x) \cdot f(y)$$
$$x \oplus y = (x_1y_1, x_2y_2 ... x_ny_n)$$

The modulus addition is equivalent to a dot product. This is also termed **Homomorphism** (for general groups).

Problem 2. *The problem at hand is to distinguish between:*

- f is linear
- f is ϵ far from linear, which means the following:

$$\forall g \text{ that is linear}$$
$$f(x) \neq g(x) \text{ on } \geq \epsilon 2^n \text{ inputs } x.$$

Goal 3. *How many queries do we need to solve the above goal with 90% success probability.*

Motivation [Blum-Luby-Rubinfield '90]

- self testing
- self correction

- PCP Theorem (probabilistically checkable proof): informally it is as follows. For a given formula φ, we can transform it into φ', where φ' is satisfiable if and only if φ is satisfiable. For any proof (satisfyable assignment) of φ', we can check whether it is indeed satisfyable in $O(1)$ places.
- PCP is often used to prove non-approximability: even approximating max clique upto a factor of $\sqrt{n}$ is a NP hard problem.

Algorithm for testing linearity is fairly basic.

- pick x, y randomly
- check the given property $f(x \oplus y) = f(x) \oplus f(y)$. Lets call this T_{xy} (a test for x,y)
- repeat the $T_{x,y}$ test for $O(1/\epsilon)$ times and fail if at least one of them fails.

Analysis of Algorithm

- If the function f is linear, then T_{xy} will pass.
- If the function f is ϵ far from linear, we need to find the Pr[T_{xy} fails]:

$$\begin{aligned} \Pr[T_{xy} \text{ fails}] &= 1 - \Pr[T_{xy} \text{ passes}] \\ &\geq \epsilon \end{aligned}$$

Example [Coppersmith]

$$f\colon\ Z_{3^k} \to Z_{3^{k-1}}$$
$$f(3h+d) = h \text{ (where } d \in \{-1, 0, +1\})$$

We have that $Pr[T_{xy}\ fails] = 2/9$, but f is 2/3 far from linear.

2 Fourier Analysis

We will show how Fourier analysis can be used to determine linearity. It is given that

$$f : \{+1, -1\}^n \to R, \text{ can be seen as a vector } F \in R^d \text{ where } d = 2^n$$
$$\mathcal{F} = \{\text{set of all } f\}$$

We define $f(x)$ as a summation of the multiplication of a basis vector and a scalar.

$$\text{Define: } f_i(x) = 1 \text{ for } i = x, \text{ and } 0 \text{ for } i \neq x$$
$$\text{Then, } f = \sum f(i) f_i, \text{ i.e., } f(x) = \sum f(i) f_i(x) \text{ for all } x.$$

This is equivalent to: a natural basis e_i (where $i \in \{+1, -1\}^n$), $F = \sum x_i e_i$ where x_i is a scalar and e_i is a basis vector.

We now introduce the Fourier basis. Fix $S \subseteq [n]$, then we define $\chi_S(x)$ as:

$$\chi_s(x) = \Pi x_i \text{ where } i \in S$$
$$\text{Define } \chi_\emptyset(x) = 1.$$

Fact χ_S for $S \subseteq [n]$ are a basis for $\mathcal{F}$.

- There are 2^n of them.

- $||\chi_S||^2 = \sum_x (\chi_S(x))^2 = 2^n$.
- Dot product: $\sum_x \chi_S(x)\chi_T(x) = \sum \prod_{i\in S} x_i \prod_{i\in T} x_i = \sum \prod_{i\in S\Delta T} x_i$
  $= \sum_x \chi_{S\Delta T}(x) = \frac{1}{2^n} E[\prod_{i\in S\Delta T} x_i] = \frac{1}{2^n} \prod_{i\in S\Delta T} E[x_i] = 0$ if $S \neq T$.

Hence these basis functions χ_S form a basis for $\mathcal{F}$.

Definition 4. $< f, g > \triangleq \frac{1}{2^n} \sum_x f(x)g(x)$ *which is essentially a dot product.*

In this definition, we get that $< \chi_S, \chi_S >= 1$ (norm of a basis vector is one).

Corollary 5. $\forall f$

$$f(x) = \sum_{S\subseteq[n]} \hat{f}(S)\chi_S(x)$$

where $\hat{f}(S)$ *is given by* $\hat{f}_S =< f, \chi_S >$*.*

Examples of Fourier transform

$f(x)$	Fourier
1	1
X_i	X_i
AND(X_2,X_1) = -1 if X_2=X_1=-1, 1 otherwise	$\frac{1}{2} + \frac{1}{2}X_1 + \frac{1}{2}X_2 - \frac{1}{2}X_1X_2$
$f = \chi_S$	$\hat{f}_S = 1$ and $\hat{f}_T = 0$ for $T \neq S$

Theorem 6 (Plancherel's)**.** *shows that*

$$< f, g >= \sum_{S\subseteq[n]} \hat{f}_S \hat{g}_S$$

Proof $< f, g >= E_x[f(x)g(x)]$
$= E[\sum_{S\subseteq[n]} \hat{f}(S)\chi_S(x) \sum_{T\subseteq[n]} \hat{g}(T)\chi_T(x)]$
$= \sum_{S,T} \hat{f}_S \hat{g}_T E[\chi_S(x)\chi_T(x)]$
The only terms that survive are those in which $S = T$ which makes the expectation value equal 1. Therefore,
$< f, g >= \sum_S \hat{f}_S \hat{g}_S$.

Theorem 7 (Parseval's)**.** $< f, f >= \sum_{S\subseteq[n]} \hat{f}_S^2$

If $f_i\{+, -1\}^n \rightarrow \{+1, -1\}$, then, $< f, f >= 1$ or can be written as $\sum \hat{f}_S^2 = 1$ by Plancherel's.

3 Proof of Linearity with Fourier Analysis

Lemma 8. χ_S *are exactly all the linear functions* $f : \{+1, -1\}^n \rightarrow \{+1, -1\}$*.*

Proof.
- First we prove χ_S is linear

  $\forall x, y$

  $\chi_S(x \oplus y) = \prod_{i\in S} x_i y_i = \prod_{i\in S} x_i \prod_{i\in S} y_i = \chi_S(x)\chi_S(y)$

- if f is linear then it is some χ_S (in problem set 5).

□

$\hat{f}_S$ relates distance to basis function χ_S. In particular, if f is ϵ-far from linearity, then we have:
$\hat{f}_S =< f, \chi_S >= E_x f(x)\chi_S(x)$
$= \Pr[f(x) = \chi_S(x)] - \Pr[f(x) \neq \chi_S(x)]$
$= 1 - dist(f, \chi_S) - dist(f, \chi_S) = 1 - 2dist(f, \chi_S)$
$\leq 1 - 2\epsilon$
Hence, none of the $\hat{f}_S$ coefficients are close to 1, and this will cause the test to fail.

Theorem 9 (Main theorem)**.** *Define:* $T_{xy} = 1$ *if* $f(x) \cdot f(y) = f(x \oplus y)$ *and it is 0 otherwise.*
If f *is* ϵ *far then we prove that the* $\Pr[T_{xy} = 1] \leq 1 - \epsilon$.

Proof Let $\delta = \Pr[T_{xy} = 0]$.

Lemma 10. $\Pr[T_{xy} = 1] = 1 - \delta = \frac{1}{2} + \frac{1}{2}\sum_S \hat{f}_S^3$.

We prove that this lemma proves the above theorem.
$\delta = 1 - (\frac{1}{2} + \frac{1}{2}\sum_S \hat{f}_S^3) = \frac{1}{2} - \frac{1}{2}\sum_S \hat{f}_S^3$
Since $\hat{f}_S$ is upper bounded by $1 - 2\epsilon$
$\geq \frac{1}{2} - \frac{1}{2}(1 - 2\epsilon)\sum_S \hat{f}_S^2$
As proved above, we have $\sum_S \hat{f}_S^2 = 1$. Therefore,
$\geq \frac{1}{2} - \frac{1}{2} + \epsilon = \epsilon$.
Hence proven. We will prove the above lemma in the next lecture.