Today:

Linearity Testing

Self-Correcting

Begin Fourier Analysis of Boolean Fctns

Linearity (homomorphism) testing:

$f: G \to G$

G is finite group

f "linear" (homomorphism) if

$\forall x,y \in G \quad f(x) + f(y) = f(x+y)$

e.g. $f(x) = x$

$f(x) = ax \mod p$ for $G = Z_p$

$f_{\bar{a}}(\bar{x}) = \sum a_i x_i \mod 2$

f "ε-linear" if $\exists$ linear g s.t. "distance of f to linear"

f & g agree on $\geq 1-\varepsilon$ inputs

i.e. $\Pr_{x \in G}[f(x) = g(x)] \geq 1-\varepsilon$

counting statement $= \dfrac{\# x \text{ s.t. } f(x)=g(x)}{\# x}$

Given query access to f, what is complexity of linearity testing?

How would you test it?

do not want to "learn" the linear fctn

in general could take $O(d)$ if $G = Z_p^d$

$(\sim \log |G|)$

Before, we see why "ε-linear" is a useful concept –

Useful observation :

G finite group

$\forall\, a, y \in G \qquad \Pr_x[\, y = a+x \,] = \frac{1}{|G|}$

since only $x = y-a$ satisfies it

$\therefore$ if pick $x \in_R G$

$\Rightarrow$ $a+x$ dist uniformly in G

i.e. $a+x \in_R G$

e.g. if $x \in_R \mathbb{Z}_{100}$

$\Rightarrow$ $15+x \in_R \mathbb{Z}$

even if $G = \mathbb{Z}_2^n$

under $(a_1 a_2 \cdots a_n) + (b_1 \cdots b_n) = (a_1 \oplus b_1 \;\cdots\; a_n \oplus b_n)$

$(0110) + (b_1 b_2 b_3 b_4) = (\underbrace{0 \oplus b_1, 1 \oplus b_2, 1 \oplus b_3, 0 \oplus b_4}_{\text{dist unif if } b_i\text{'s are}})$

why?

all coords are independent

each coord is uniform

Why do we want it?

Self-correcting (i.e. random self-reducibility)

Given f s.t. $\exists$ linear g s.t. $\Pr_x[f(x)=g(x)] \geq 7/8$.

To compute $g(x)$: (using calls to f <u>not</u> g)

For $i = 1 \ldots c \log \frac{1}{\beta}$

pick $y \in_R G$

$\text{answer}_i \leftarrow f(y) + f(x-y)$

↑ unif dist by observation

Output most common value for answer_i

<u>Claim</u> $\Pr[\text{output} = g(x)] \geq 1-\beta$

<u>pf</u>

$\Pr[f(y) \neq g(y)] \leq 1/8$

$\Pr[f(x-y) \neq g(x-y)] \leq 1/8$

$\therefore \Pr[\underbrace{f(y) + f(x-y)}_{\text{answer}_i} \neq \underbrace{g(y) + g(x-y)}_{=g(x)}] \leq 1/4$

rest is Chernoff.

How do we test when domain is Z_p?

Do $O(?)$ times
Pick random x, y
if $f(x) + f(y) \neq f(x+y)$ fail + halt

Does it work? Here is a "tough" fctn f:

$$\forall x \in Z_p, \quad f(x) \equiv \begin{cases} 1 & \text{if } x \equiv 1 \mod 3 \\ 0 & \text{if } x \equiv 0 \mod 3 \\ -1 & \text{if } x \equiv 2 \mod 3 \end{cases}$$

so $f(x)+f(y) = 2$
but $f(x+y) = -1$

f fails for $\left.\begin{array}{l} x \equiv y \equiv 1 \mod 3 \\ x \equiv y \equiv 2 \mod 3 \end{array}\right\}$ good! since this is the "right answer"

else passes ☹ bad! since this is the "wrong answer" + it happens a lot!!

$\delta_f \equiv \Pr[f(x) + f(y) \neq f(x+y)]$ "group failure probability of f"

here $\delta_f = 2/9$

closest linear fctn is $g \equiv 0$

$\therefore$ f is $2/3$ - far from linear

☹

but $\delta_f = 2/9$ is a threshold,
ie. if you know $\delta_f < 2/9$, it must be δ-close to linear.

(actually $\delta/2$ ...)

Will prove only for Boolean fctns.

Need some tools: Fourier analysis over Boolean cube

Over $\{0,1\}^n$ $f: \{0,1\}^n \to \{0,1\}$

inner product $x \cdot y = \sum_{i=1}^{n} x_i y_i \bmod 2$ (XOR)

linear fctns on $\{0,1\}^n$: $L_a(x) = a \cdot x$ for fixed $a \in \{0,1\}^n$

2^n linear fctns

can refer to specific one via set notation of 1's

i.e. $\underbrace{L_A(x) = \sum_{i \in A} x_i}_{\text{convenient}}$ $A \subseteq \{1..n\}$ is set of indices that are 1

<u>Notation change</u>: less natural but easier to work with

$f: \{\pm 1\}^n \to \{\pm 1\}$ $0 \rightsquigarrow +1$
$1 \rightsquigarrow -1$

+	0	1
0	0	1
1	1	0

$\to$

$\times$	1	-1
1	1	-1
-1	-1	1

i.e. $a \to (-1)^a$
$a+b \to (-1)^{a+b}$
$= (-1)^a (-1$

addition $\to$ multiplication

now linearity $\Leftrightarrow$ $f(\underbrace{a \cdot b}_{\text{coordinatewise mult}}) = f(a) f(b)$ $(a \cdot b)_i = a_i \cdot b_i$

Linear fctns are now!

def $S \subset \{1..n\}$

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

Parity functions

Now linearity test checks

$$f(x \odot y) = f(x) \cdot f(y)$$

coordwise mult

will just use $\odot$

Note: $f(x)\, f(y)\, f(x \odot y) = \begin{cases} 1 & \text{if test accepts} \\ -1 & \text{" " rejects} \end{cases}$

$$\Updownarrow$$

$$\frac{1 - f(x)\, f(y)\, f(x \odot y)}{2} = \begin{cases} 0 & \text{if accept} \\ 1 & \text{if reject} \end{cases}$$

Indicator var!

$$\underbrace{\delta_f}_{\text{rejection prob of } f} = E\left[\frac{1 - f(x) f(y)\, f(x \odot y)}{2} \right]$$

how to analyze?

Fourier Analysis on discrete binary hypercube

all n-bit fctns mapping to reals
vector space

$$G = \{g \mid g : \{\pm 1\}^n \to \mathbb{R}\}$$

$\dim(G) = 2^n$ i.e.

- all fctns can be written as lin comb of 2^n basis fctns
- which basis is convenient?

First basis: indicator fctns $e_a(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{o.w.} \end{cases}$

viewing g as 2^n-vector coords of g are values of $g(a)$ $\forall a$

$$g = \sum_a g(a)\, e_a(x)$$

2nd basis: (wrt what?)

don't write [χ_S $\forall S \subseteq [n]$ orthonormal basis as weighted sum of these guys
$\therefore f$ can be uniquely expressed]

define $\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \{\pm 1\}^n} f(x) g(x)$ inner product

$\uparrow$ 2 fctns

$\{\chi_S\}$ is orthonormal wrt inner product:

1) $\langle \chi_S, \chi_S \rangle = \frac{1}{2^n} \sum \underbrace{(\chi_S(x))}_{\pm 1}^2 = 1$ normal

2) $\langle \chi_S, \chi_T \rangle$ for $S \neq T$ orthogonal

$$= \frac{1}{2^n} \sum_{x \in \{\pm 1\}^n} \chi_S(x) \chi_T(x)$$

$$= \frac{1}{2^n} \sum_{x \in \{\pm 1\}^n} \prod_{i \in S} x_i \prod_{i \in T} x_i$$ if $i \in S \cap T$ $x_i^2 = 1$ so drops out

$$= \frac{1}{2^n} \sum_{x \in \{\pm 1\}^n} \prod_{i \in S \Delta T} x_i$$

$S \Delta T$ nonempty since $S \neq T$, assume $j \in S \Delta T$

$$= \frac{1}{2^n} \sum_{\substack{\text{pairs} \\ x, \underbrace{x^{\oplus j}}_{= x'}}} \underbrace{\left(\prod_{i \in S \Delta T} x_i + \prod_{i \in S \Delta T} x_i' \right)}_{\underbrace{x_j \left(\prod_{i \in S \Delta T \setminus \{j\}} x_i \right) + \bar{x}_j \left(\prod_{i \in S \Delta T \setminus \{j\}} x_i \right)}_{= 0}}$$

$x^{\oplus j}$ = x with jth bit flipped $\rightarrow$ $(x_1 \cdots x_j (+1) x_{j+1} \cdots x_n)$, $(x_1 \cdots x_j (-1) x_{j+1} \cdots x_n)$

$\Leftarrow$ one is +1 and other is −1

$= 0$ ■

$\therefore \chi_S, \chi_T$ orthogonal

f uniquely expressible as lin comb of χ_S since $\{\chi_S\}$ is orthonormal basis

define $\hat{f}(S) \equiv \langle f, \chi_S \rangle = \frac{1}{2^n} \sum_{x \in \{\pm 1\}^n} f(x)\chi_S(x)$ "Fourier coeffs of f"

<u>Thm</u> $\forall f$ $\quad f(x) = \sum_S \hat{f}(S)\chi_S(x)$

Fourier coeffs of linear fctns:

<u>Fact</u> [Fourier coeffs of linear fctn.]

f linear $\iff \exists S \subseteq [n]$ $\hat{f}(S) = 1$ ← one Fourier coeff is big

$+ \forall T \neq S$ $\hat{f}(T) = 0$ ← others 0

Fourier coeff <u>characterize</u> distance to linear!

<u>Lemma</u> $\forall S \subseteq [n]$

$$\hat{f}(S) = 1 - 2\,\mathrm{dist}(f, \chi_S)$$
$$= 1 - 2 \Pr_{x \in \{\pm 1\}^n}[f(x) \neq \chi_S(x)]$$

<u>Pf</u> $2^n \hat{f}(S) = \sum_x f(x)\chi_S(x)$

$$= \sum_{\substack{x \text{ s.t.} \\ f(x) = \chi_S(x)}} 1 + \sum_{\substack{x \text{ s.t.} \\ f(x) \neq \chi_S(x)}} -1$$

$$= 2^n(1 - \mathrm{dist}(f, \chi_S)) + 2^n \cdot (-1)(\mathrm{dist}(f, \chi_S))$$
$$= 2^n(1 - 2\,\mathrm{dist}(f, \chi_S)) \quad \blacksquare$$

<u>example</u> $f =$ all -1's

$\forall S \neq \emptyset$ $\text{dist}(f, \chi_S) = \frac{1}{2}$

so $\hat{f}(S) = 0$

For $S = \emptyset$ $\text{dist}(f, \chi_S) = 1$

so $\hat{f}(S) = -1$

<u>Observation</u> 2 distinct linear fctns differ on exactly $\frac{1}{2}$ of pts $\Rightarrow$

<u>Pf</u> $f = \chi_T$ so
$g = \chi_S$
$T \neq S$

$\hat{f}(S) = \langle f, \chi_S \rangle = \langle f, g \rangle$

but $\underset{\substack{\uparrow \\ \text{since orthonormal}}}{0 =} \langle \overset{f}{\chi_T}, \overset{g}{\chi_S} \rangle \underset{\text{lemma}}{=} 1 - 2 \, \text{dist}[\overset{f}{\chi_T(x)}, \overset{g}{\chi_S}(x)]$

$\Downarrow \leftarrow$ algebra

$\text{dist}[\chi_T, \chi_S] = \frac{1}{2}$

Very Useful Tool: Plancherel / Parseval's Identity

$$\langle f, g \rangle = \Big\langle \sum_{S \subseteq [n]} \hat{f}(S) \chi_S, \sum_{T \subseteq [n]} \hat{g}(T) \chi_T \Big\rangle = \sum_{S,T} \hat{f}(S) \hat{g}(T) \langle \chi_S, \chi_T \rangle$$

$$= \sum_{S \subseteq [n]} \hat{f}(S) \hat{g}(S) \underbrace{\langle \chi_S, \chi_S \rangle}_{=1}$$

since $\langle \chi_S, \chi_T \rangle = 0$ for $S \neq T$

so Parseval $\langle f, f \rangle = \sum \hat{f}(S)^2$, $\langle f, g \rangle = \sum \hat{f}(S) \hat{g}(S)$ "Plancherel"

when f is <u>boolean</u> $\langle f, f \rangle = \frac{1}{2^n} \sum \underbrace{f(x) f(x)}_{\substack{1 \cdot 1 = 1 \\ -1 \cdot -1 = 1}} = 1$

so "Boolean Parseval's" is $1 = \sum \hat{f}(S)^2$

Useful tools:

Plancherel's Identity

$$\langle f, g\rangle = \left\langle \sum_{S\subseteq[n]} \hat{f}(S)\chi_S, \sum_{T\subseteq[n]} \hat{\hat{g}}(T)\chi_T \right\rangle$$

$$= \sum_{S,T} \hat{f}(S)\hat{\hat{g}}(T)\langle\chi_S, \chi_T\rangle \quad \text{bilinearity of } \langle\cdot;\cdot\rangle$$

$$= \sum_S \hat{f}(S)\hat{g}(S) \quad \text{since } \langle\chi_S, \chi_T\rangle = \begin{cases} 0 & \text{if } S\neq T \\ 1 & \text{if } S=T \end{cases}$$

Parseval's

$$\forall f \quad \langle f, f\rangle = \sum_S \hat{f}(S)^2$$

Boolean Parseval's

$$\forall f \text{ boolean } \langle f, f\rangle = \frac{1}{2^n}\sum_x f(x)f(x) = 1$$

(ie. range is ± 1)

<u>so</u> $\sum_S \hat{f}(S)^2 = 1$

Now we are ready for a quick linearity test proof!

Recall $\delta_f \equiv \Pr[f(x \oplus y) \neq f(x) f(y)] \iff \delta_f = E\left[\frac{1 - f(x) f(y) f(x \oplus y)}{2}\right]$

Thm f is δ_f - close to some linear fctn

(note: Coppersmith's example doesn't work over $\{\pm 1\}^n$)

Pf

$$E_{x,y}[f(x)f(y)\,f(x \oplus y)] = E_{xy}\left[\sum_S \hat{f}(S)\chi_S(x) \sum_T \hat{f}(T)\,\chi_T(y) \sum_U \hat{f}(U)\chi_U(x \oplus y)\right]$$

$$= E_{xy}\left[\sum_{S,T,U} \hat{f}(S)\hat{f}(T)\hat{f}(U)\,\chi_S(x)\chi_T(y)\,\chi_U(x \oplus y)\right]$$

$$= \sum_{S,T,U} \hat{f}(S)\,\hat{f}(T)\,\hat{f}(U)\;E_{x,y}\left[\chi_S(x)\chi_T(y)\,\chi_U(x \oplus y)\right]$$

note: 1) if $S = T = U$ $\quad \chi_S(x)\,\chi_{\underset{S}{T}}(y)\,\chi_{\underset{S}{U}}(x \oplus y) = \prod_{i \in S} x_i \cdot y_i \cdot (x_i \cdot y_i) = \prod_{i \in S} \underbrace{x_i^2}_{1}\, \underbrace{y_i^2}_{1} =$

2) if $\neg(S = T = U)$ $\quad E_{x,y}[\chi_S(x)\,\chi_T(y)\,\chi_U(x \oplus y)] = $

$$= E_{xy}\left[\prod_{i \in S} x_i \prod_{j \in T} y_j \prod_{k \in U} x_k \prod_{l \in U} y_l\right]$$

$$= E_{xy}\left[\prod_{i \in S \Delta U} x_i \prod_{j \in T \Delta U} y_j\right]$$

$$= \underbrace{E_x\left[\prod_{i \in S \Delta U} x_i\right]}_{=0}\; \underbrace{E_y\left[\prod_{j \in T \Delta U} y_j\right]}_{=0}$$ since indep

if $S \neq U$, $\qquad$ if $T \neq U$

$\therefore \quad = 0$

$$E_{xy}[f(x) f(y) f(x \odot y)]$$

$$= \sum_{S=T=U} \hat{f}(S)^3$$

$$\leq \max_S \hat{f}(S) \underbrace{\sum_S \hat{f}(S)^2}_{=1} \quad \text{by Parseval's (Boolean)}$$

$$= \max_S \hat{f}(S)$$

$$= 1 - 2 \min_S \mathrm{dist}(f, \chi_S)$$

$$\text{so} \quad \delta_f = \frac{\cancel{1} - \cancel{1} + \cancel{2} \min_S \mathrm{dist}(f, \chi_S)}{\cancel{2}}$$

∎