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 $= \frac{\#\, x \text{ s.t. } f(x)=g(x)}{\#\, x}$

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 $\Theta(d)$ 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

ie. $a+x \in_R G$

even if $G = Z_2^n$

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

$(0110) + (b_1 b_2 b_3 b_4) = (0 \oplus b_1,\ 1 \oplus b_2,\ 1 \oplus b_3,\ 0 \oplus b_4)$

dist unif if b_i's are

Why do we want it?

Self-correcting (ie. 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 not 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

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

pf

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

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

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

rest is Chernoff.

Will prove only for Boolean fctns. lin test.s

Need some tools: Fourier analysis over Boolean cube

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

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

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

2^n linear fctns

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

ie. $L_A(x) = \sum_{i \in A} x_i$ $\quad A \subseteq \{1..n\}$ is set of indices that are 1

Convenient

Notation change: less natural but easier to work with

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

+	0	1
0	0	1
1	1	0

$\to$

×	1	−1
1	1	−1
−1	−1	1

ie. $a \to (-1)^a$

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

addition $\to$ multiplication

now linearity $\iff$ $f(a \circ b) = f(a) f(b)$ coordinatwise mult $(a \cdot b)_i = a_i \cdot b_i$

Linear fctns are now!

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

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

Parity functions

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?

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

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

f fails for $x \equiv y \equiv 1 \mod 3$, $x \equiv y \equiv 2 \mod 3$ } looks good!

else passes ☹

$\delta_f \equiv Pr[f(x) + f(y) \neq f(x+y)]$ "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 $\delta/2$ ...)

Now linearity test checks

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

↑ coordwise mult
will just use $\circledcirc$

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

$$\Updownarrow$$

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

$$\delta_f = E\left[\frac{1 - f(x) f(y)\, f(x \circledcirc y)}{2}\right]$$

δ_f ~ rejection prob of f

how to analyze?

Fourier Analysis on discrete binary hypercube

$G = \{g \mid g : \{\pm 1\}^n \to \mathbb{R}\}$ all n-bit fctns mapping to reals

vector space

$\dim(G) = 2^n$ 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 of g are values coords of $g(a)$ wrt

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

2nd basis:

don't write $\begin{bmatrix} \chi_S \\ \vdots \\ f \end{bmatrix}$ $\forall S \subseteq [n]$ orthonormal basis (wrt what?)

can be uniquely expressed as weighted sum of these guys

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

(f, g: 2 fctns)

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

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

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

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

$$= \frac{1}{2^n} \sum_{\text{pairs } x, x^{\oplus j}} \left(\prod_{i \in S \Delta T} x_i + \prod_{i \in S \Delta T} x_i' \right)$$

$x^{\oplus j}$ = x with jth bit flipped → $(x_1 \cdots x_j (\mp 1) x_{j+1} \cdots x_n) + (x_1 \cdots x_j (\pm 1) x_{j+1} \cdots x_n)$

$$= x_j \left(\prod_{i \in S \Delta T \setminus \{j\}} x_i \right) + \bar{x}_j \left(\prod_{i \in S \Delta T \setminus \{j\}} x_i \right)$$

⇐ one is $+1$ and other is -1

$= 0$

$= 0$ ∎

$\therefore \chi_S, \chi_T$ 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"

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

Fourier coeffs of linear fctns:

Fact [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 characterize distance to linear!

Lemma $\forall\, S \subseteq [n]$

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

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

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

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

∎

example $f =$ all -1's

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

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

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

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

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

Pf $f = \chi_T$ so

$g = \chi_S$

$T \neq S$

but $0 = \langle \overset{f}{\chi_T}, \overset{g}{\chi_S} \rangle \overset{\text{Lemma}}{=} 1 - 2 \operatorname{dist}[\overset{f}{\chi_T}(x), \overset{g}{\chi_S}(x)]$

↑ since orthonormal ↓ ← algebra

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

Very Useful Tool: Plancherel / Parseval's Identity

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

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

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 boolean $\langle f, f \rangle = \frac{1}{2^n} \sum \underbrace{f(x)f(x)}_{1 \cdot 1 = 1,\ -1 \cdot -1 = 1} = 1$ so "Boolean Parseval's" is $1 = \sum \hat{f}(S)^2$

Useful tools:

Plancherel's Identity

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

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

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

Parseval's

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

Boolean Parseval's

$\forall f$ boolean (ie. range is ± 1) $\quad \langle f, f \rangle = \frac{1}{2^n} \sum_x f(x) f(x) = 1$

so $\quad \sum_S \hat{f}(S)^2 = 1$

Now we are ready for a quick linearity test proof!

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

Thm f is δ_f-close to some linear fctn

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

pf

$$\mathbb{E}_{x,y}[f(x) f(y) f(x \circledast y)] = \mathbb{E}_{x,y}\left[\sum_S \hat{f}(S)\chi_S(x) \sum_T \hat{f}(T)\chi_T(y) \sum_U \hat{f}(U)\chi_U(x \circledast y)\right]$$

$$= \mathbb{E}_{x,y}\left[\sum_{S,T,U} \hat{f}(S)\hat{f}(T)\hat{f}(U)\chi_S(x)\chi_T(y)\chi_U(x \circledast y)\right]$$

$$= \sum_{S,T,U} \hat{f}(S)\hat{f}(T)\hat{f}(U)\, \mathbb{E}_{x,y}[\chi_S(x)\chi_T(y)\chi_U(x \circledast y)]$$

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

2) if $\neg(S = T = U)$ $\quad \mathbb{E}_{x,y}[\chi_S(x)\chi_T(y)\chi_U(x \circledast y)] = ?$

$$= \mathbb{E}_{x,y}\left[\prod_{i \in S} x_i \prod_{j \in T} y_j \prod_{k \in U} x_k \prod_{l \in U} y_l\right]$$

$$= \mathbb{E}_{x,y}\left[\prod_{i \in S \Delta U} x_i \prod_{j \in T \Delta U} y_j\right]$$

$$= \mathbb{E}_x\left[\prod_{i \in S \Delta U} x_i\right] \mathbb{E}_y\left[\prod_{j \in T \Delta U} y_j\right] \quad \text{since independent}$$

if $S \neq U$, $\mathbb{E}_x[\prod_{i \in S \Delta U} x_i] = 0$; if $T \neq U$, $\mathbb{E}_y[\prod_{j \in T \Delta U} y_j] = 0$

$\therefore \quad = 0$

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

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

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

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

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

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

▨