Today:

Linearity Testing

Self- Correcting

Begin Fourier Analysis of Boolean fctns.

Given:

$f : G \to \cancel{G}$ H

G is finite group
H is " "

def: f is "linear" (homomorphism) if

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

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

$f(x) = ax \bmod p$ for $G = \mathbb{Z}_p = H$

$f_{\bar{a}}(\bar{x}) = \sum a_i x_i \bmod 2$ for $G = \mathbb{Z}_2^d$, $H = \mathbb{Z}_2$

$+_G \equiv$ bitwise xor

$+_H =$ xor

def: f "ε-linear" if $\exists$ linear fctn g

"distance" of f to linear $\left\{ \begin{array}{l} \text{s.t. } f \text{ + } g \text{ agree on } \geq 1-\varepsilon \text{ inputs} \\ \text{ie. } \underbrace{\Pr_{x \in G}[f(x) = g(x)]}_{\text{counting statement}} \geq 1 - \varepsilon \end{array} \right.$

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

Complexity of linearity testing?

First: A useful observation

G finite group

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

since only $x = y - a$ satisfies

$\Rightarrow$ if pick $x \in_R G$

$\Rightarrow$ $a + x \in_u G$ even though a fixed or from arbitrary distribution

notation: $\in_u$ uniformly distributed in G

e.g. if $G = Z_2^d$

$$\underset{\substack{\uparrow\\ \text{fixed}}}{(a_1 \ldots a_d)} + \underset{\substack{\uparrow\\ \text{dist uniformly}}}{(b_1 \ldots b_d)} = \underbrace{(a_1 \oplus b_1, \ldots, a_d \oplus b_d)}$$

$\Rightarrow$ dist uniformly
(1) coords are indep
(2) each coord unif by above

Why are fctns that are ε-close to linear useful? Can fix them!

Self-correcting (AKA random self-reducibility)

Given f $\frac{1}{8}$-close to linear

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

must be unique

To compute $g(x)$:

(use calls to f <u>not</u> g)

For $i = 1 \ldots c \log 1/\beta$

pick $y \in_R G$

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

both unif distributed but dependent

Output most common answer

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

<u>Pf</u>. main idea: if f "correct" ($=g$) on y & $x-y$ then answer$_i = g(x)$

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

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

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

union bnd

$\Rightarrow$ each $\text{answer}_i = g(x)$ with prob $\geq 3/4$

Chernoff $\Rightarrow$ Claim $\blacksquare$

How to test linearity?

Proposed test:

how many times do we need

Do $O(?)$ times

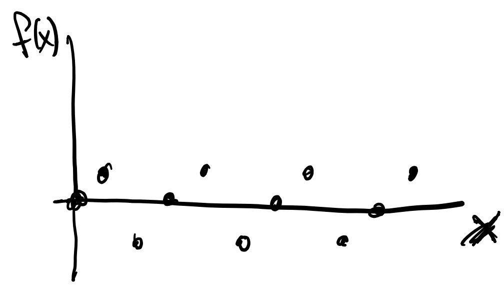
Pick $x, y \in_R G$

if $f(x)+f(y) \neq f(x+y)$ fail & halt

Accept

Possible difficulty: "tough" fctn f

$$\forall x \in \mathbb{Z}_p \quad f(x) \equiv \begin{cases} 1 & \text{if } x \equiv 1 \bmod 3 \\ 0 & \phantom{\text{if } x \equiv {}} 0 \\ -1 & \phantom{\text{if } x \equiv {}} 2 \end{cases}$$



closest linear g to f is $g(x) = 0 \ \forall x$

$$\frac{\# \, x \text{ s.t. } g(x) = f(x)}{\# \, x} \approx \frac{1}{3}$$

f ~~fails~~ good for $x \equiv y \equiv 1 \bmod 3$
$x \equiv y \equiv 2 \bmod 3$

$x \equiv y \equiv 1 \bmod 3$:

$$f(x) + f(y) \stackrel{?}{\equiv} f(\underbrace{x+y}_{2 \bmod 3})$$

$$1 + 1 \not\equiv -1$$

f passes for all other x, y pairs

failure prob of test

$$\delta_f \equiv \Pr_{x,y}[f(x) + f(y) \neq f(x+y)]$$

$$= 2/q \quad \leftarrow \text{low but } f \text{ far from linear}$$

Good news: $2/q$ is a "threshold"

if you know $\delta_f < 2/q$ then it must be δ- close to linear

(Known theorem)

We prove stronger thm for Boolean fctns

Fourier Analysis over Boolean Cube

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

inner product $\quad x \cdot y = \sum_{i=1}^{n} x_i y_i \mod 2$

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

for fixed $a \in \{0,1\}^n$

2^n linear fctns

can use set notation:

$A \subseteq \{1 \ldots n\}$

is set of indices that are 1

$$L_A(x) = \sum_{i \in A} x_i$$

equivalent + convenient

Notation change:

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

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \rightsquigarrow \begin{array}{c|cc} \times & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array}$$

i.e. $a \to (-1)^a$

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

addition $\to$ multiplication

Now linearity: $f(a \odot b) = f(a) \cdot f(b)$

$\uparrow$ coordinatewise mult

$(a_1 \ldots a_n) \odot (b_1 \ldots b_n)$
$= (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n)$

Linear fctns:

<u>def</u> $S \subseteq \{1..n\}$

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

Parity fctns

Write event that a test passes as algebraic fctn:

new linearity test: $f(x \odot y) = f(x) \cdot f(y)$

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

$\Updownarrow$

indicator var $\left\{ \frac{1 - f(x) f(y) \cdot f(x \odot y)}{2} = \begin{cases} 0 & \text{if accept} \\ 1 & \text{if rejects} \end{cases} \right.$

$$\boxed{\begin{aligned} \text{rejection prob of } f \quad \delta_f &\equiv \Pr[f(x) \cdot f(y) \neq f(x \oplus y)] \\ &= E\left[\frac{1 - f(x)\cdot f(y)\cdot f(x\oplus y)}{2}\right] \end{aligned}}$$

---

more on Fourier Analysis:

$G = \{g \mid g : \{\pm 1\}^n \to \mathbb{R}\}$ 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 idea for basis: "input/output table"

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

then $\forall g$: $g(x) = \sum_a g(a) e_a(x)$

orthonormal!

2^{nd} basis:

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

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

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

normal

2) $S \neq T$

$\langle \chi_S, \chi_T \rangle = \frac{1}{2^n} \sum_x \chi_S(x) \chi_T(x)$

if $i \in S \cap T$
$x_i \cdot x_i = 1$ drops out

$= \frac{1}{2^n} \sum_x \chi_{\underbrace{S \Delta T}}(x)$ nonempty since $S \neq T$

pick $j \in S \Delta T$

$= \frac{1}{2^n} \sum_{\substack{\text{pairs} \\ x, x^{\oplus j}}} \chi_{S\Delta T}(x) + \chi_{S \Delta T}(x^{\oplus j})$

$x^{\oplus j}$ = x with j^{th} bit flipped sum to 0 $\quad = $

$$= \frac{1}{2^n} \sum_{\substack{\text{pairs} \\ x,\, x^{\oplus j}}} \underbrace{x_j \prod_{i \in (S \Delta T) \setminus j} x_i + \bar{x}_j \prod_{i \in (S \Delta T) \setminus j} x_i}_{=0}$$

$$= \frac{1}{2^n} \sum_{\text{pairs}} 0$$

$$= 0 \quad \blacksquare \qquad \Rightarrow \chi_S \;\&\; \chi_T$$

orthogonal

<u>Thm</u> f uniquely expressible as lin comb of χ_S since $\{\chi_S\}$ is orthonormal basis.