Lecture 12

- Linearity testing & self correcting
- Basics of Fourier Analysis on Boolean cube

Linear Functions

$f: G \to H$

G is finite group

H " " "

def. f is "linear" (homomorphism) if

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

$+_H$ is "plus" in group H

$+_G$ is "plus" in group G

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

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

$f_{\vec{a}}(x) = \sum a_i x_i \bmod 2$ for $G = \mathbb{F}_2^n$ $H = \mathbb{F}_2$

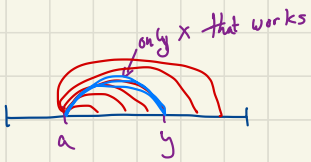
def f is "ε-linear" if $\exists$ linear g s.t. f & g agree on $\geq 1-\varepsilon$ fraction of inputs.

Notation note that the following are equivalent statements:

- f & g agree on $\geq 1-\varepsilon$ fraction of inputs
- $\frac{|\{x \mid f(x)=g(x), x \in G\}|}{|G|} \geq 1-\varepsilon$
- $\Pr_{x \in G}[f(x)=g(x)] \geq 1-\varepsilon$

First let's see some useful things about linear fctns:

A useful observation:



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

since only $x = y - a$ satisfies equation

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

then $a + x$ is also unif dist in G $(a + x \in_R G)$

(but not independent)

example:

If $G = \mathbb{F}_2^n$ with operation

$$(a_1 \cdots a_n) + (b_1 \cdots b_n) = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n)$$

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

is distributed uniformly if b_i's are

why?
- each coord uniform
- b_i's indep $\Rightarrow$ $a_i \oplus b_i$'s indep too!

Self-Correcting: also known as "random self-reducibility"

Given $f: G \to G$ s.t. $\exists$ linear $g: G \to G$

s.t. $\Pr_{x \in_R G}[f(x) = g(x)] \geq 7/8$ ← not given g, just f!!!

this just means $f \neq g$ agree on $\geq 7/8$ of inputs

Can compute $g(x)$ $\forall x$!

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

Pick $y \in_R G$

$\text{answer}_i \leftarrow f(y) + f(x-y)$ ⇐ note: $x-y$ is unif dist over group by observation

Output most common value for answer_i

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

Pf.

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

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

since both y & $x-y$ are uniform over G & by assumption on f

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

by union bound, both are equal with prob $\geq 3/4$

$\Rightarrow$ most common value $= g(x)$ with prob $\geq 1 - \beta$ (Chernoff)

Average case complexity implication:

as far as randomized complexity goes, it can't be that $\exists$ set of $< 1/8$ of inputs on which f is really hard to compute.

Linearity Testing

def. "linearity tester"

given: query access to fct f & parameter ε

requirements:

- if f linear, $\Pr[\text{tester passes}] = 1$
- if f not ε-linear, $\Pr[\text{tester fails}] \geq 3/4$ (arbitrary constant)

note: if f not linear, but $\frac{\varepsilon}{2}$-close, behavior not specified

How hard is it to test that f is ε-linear?

do we need to try all x, y, $x+y$ tuples?

Proposed test:

Pick random x, y

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

repeat how many times?

Question

$$\mathcal{F} \leftarrow \{ f \mid \forall x,y \; f(x)+f(y) = f(x+y) \}$$

$$\mathcal{G} \leftarrow \{ f \mid \text{For most } x,y \; f(x)+f(y) = f(x+y) \}$$

are $\mathcal{F}$ & $\mathcal{G}$ essentially the same functions?

not exactly since could take linear fctn & change in one place & still get member of $\mathcal{G}$

more formally:

$\forall g \in \mathcal{G}$, does there exist $f \in \mathcal{F}$ s.t.

g & f agree on $> 1-\varepsilon$ fraction of inputs?

(i.e. g is ε-linear)

Want to relate $\delta \equiv$ prob of failing test to $\varepsilon \equiv$ closeness of g

How do we test when domain is $\mathbb{Z}_p$?

Do $O(?)$ times

pick $x, y \in_u \mathbb{Z}_p$

If $f(x) + f(y) \neq f(x+y)$ output "fail" & halt

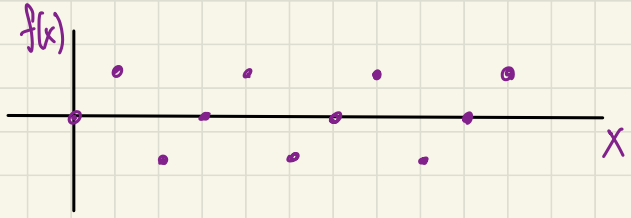
Output "pass"

Possible difficulty: (Coppersmith's example)

Tough function f

$f: \mathbb{Z}_p \to \mathbb{Z}_p$

$\forall x \in \mathbb{Z}_p \quad f(x) = \begin{cases} 1 \\ 0 \\ -1 \end{cases}$ if $x \equiv \begin{matrix} 1 \\ 0 \\ 2 \end{matrix} \mod 3$



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

f is "far" from g: $\Pr_x[f(x) \neq g(x)] = 2/3$

but f does pretty well at linearity test:

f fails for $x \equiv y \equiv 1 \mod 3$ $x+y \equiv 2 \mod 3$ $1+1 \neq -1$

$x \equiv y \equiv 2 \mod 3$ $x+y \equiv 1 \mod 3$ $-1+-1 \neq 1$

e.g. $x \equiv y \equiv 1 \mod 3$ $\quad 2 \mod 3$

$f(x) + f(y) \stackrel{?}{=} f(x+y)$

$1 + 1 \neq -1$

but f passes all other x, y!

$\Rightarrow \delta_f \equiv \Pr_{x,y}[f(x)+f(y) \neq f(x+y)] = 2/9$ ← passes a lot

"failure probability of test"

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

Good news:

$2/9$ is a "threshold"

if $\delta_f < 2/9$, f must be δ_f-close to linear (known thm)

We will prove stronger bound for Boolean fctns

need tools: Fourier analysis over Boolean cube

Characterizing linear fctns over Boolean cube

What are linear fctns mapping $\{0,1\}^n \to \{0,1\}$?

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

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

how many linear fctns? 2^n

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

for $A \subseteq \{1..n\}$

set of indices that are 1 in $\bar{a}$

The great change of notation:

(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

addition

$\longrightarrow$

×	1	−1
1	1	−1
−1	−1	1

multiplication

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

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

now linearity corresponds to

$$f(a) + f(b) = f(a \oplus b) \longrightarrow f(a) \cdot f(b) = f(a \odot b)$$

$\oplus$: coordinatewise add, $(x_1 \cdots x_n) + (y_1 \cdots y_n) = (x_1 + y_1, \cdots x_n + y_n)$

$\odot$: coordinatewise mult, $(x_1 \cdots x_n) \cdot (y_1 \cdots y_n) = (x_1 y_1, \cdots, x_n y_n)$

Linear fctns are now:

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

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

Parity fctns

Express event that test passes as algebraic fctn:

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

$f(x) \cdot f(y) = f(x \circ y)$ ⇕ test accepts

" " rejects ⇕ $f(x) \cdot f(y) \neq f(x \circ y)$

⇕

0/1 indicator var

$$\frac{1 - f(x)\, f(y)\, f(x \circ y)}{2} = \begin{cases} 0 & \text{if accepts} \\ 1 & \text{o.w.} \end{cases}$$

Now we have a new way to express rejection probability:

rejection probability

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

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

Fourier Analysis on Boolean Cube

want basis to describe all fctns. $f: \{\pm 1\}^n \to \{\pm 1\}$

1st idea: "input/output table"

indicator fctns

nok: these are orthonormal!!

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

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

can express g as lin comb of basis vectors

$g(a)$: scalar; $e_a(x)$: basis fctn evaluated at x

e.g.

x	$f(x)$
0	1
1	-1

$g(x) = +1 \cdot e_0(x) + (-1) e_1(x)$

2nd idea:

(Recall) Notation change:

$\{0,1\} \to \{\pm 1\}$

$+ \to \times$

$f(a)+f(b)=f(a+b) \to f(a)\cdot f(b)=f(a \circ b)$

↖ coordinatwise mult

Linear fctns:

$S \subseteq \{1..n\}$

parity fctns

for $x \in \{\pm 1\}^n$, $\chi_S(x) = \prod_{i \in S} x_i$

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

Fact parity (linear) fctns $\{\chi_S\}$ is orthonormal basis w.r.t. inner product!

Proof of fact:

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

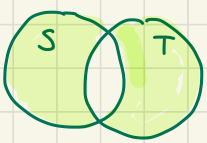
  ($\chi_S(x) = \pm 1$, so $(\chi_S(x))^2 = +1$)

- if $S \neq T$:

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

if $i \in S \cap T$ then $x_i \cdot x_i = 1$ "drops out" so can ignore

$S \Delta T$:



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

nonempty since $S \neq T$ so pick $j \in S \Delta T$

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

$x^{\oplus j} = x$ with jth bit flipped

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

equal

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

One is $+1$ the other is -1 so sum to 0

$$= 0$$

Orthogonal!

So $\{\chi_S\}$ is an orthonormal basis

Thm f is uniquely expressible as linear comb. of χ_S.

Def. $\hat{f}(S) \equiv \langle f, \chi_S \rangle$

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

Fourier Coefficients of f

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

Fourier coefts of linear fctns:

Fact f linear $\Leftrightarrow$ $\exists\ S \subseteq [n]$ s.t. $\hat{f}(S) = 1$ ← one is really big

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

e.g. if $f(x) = x_1 \cdot x_2$

$f(x) = 0 \cdot \chi_\emptyset + 0 \cdot \chi_{\{1\}} + 0 \cdot \chi_{\{2\}} + 1 \cdot \chi_{\{1,2\}}$