Linearity Testing

Given $f: G_1 \to G_2$ where G_1, G_2 are finite groups

<u>def</u> f is linear (homomorphism) if

$\forall x,y \in G_1 \quad f(x) +_2 f(y) = f(x+y)$

$\uparrow$ + for G_2 $\quad \uparrow$ + for G_1

<u>examples</u>

$f(x) = 0$

$f(x) = x$

$f(x) = a \cdot x \mod R$ $\quad$ for $G_1 = \mathbb{Z}_R = G_2$

$f(\bar{x}) = \bar{a} \cdot \bar{x} \mod p$ $\quad$ for $G_1 = \mathbb{Z}_p^n \quad G_2 = \mathbb{Z}_p$

$\uparrow$ $\sum a_i x_i \mod p$

Can we test linearity?

i.e. Pass f s.t. f linear

Fail f s.t. f $\frac{1}{4}$-far from any linear fctn $\Big\}$ with prob $\geq 3/4$

Proposed Test: $\leftarrow$ how big?

Do s times:

Pick $x,y \in_u G$

if $f(x) + f(y) \neq f(x+y)$ output Fail + halt

Output Pass

a useful observation:

$\forall \; a, y \in G \quad \Pr_{x \in G}[y = a + x] = \frac{1}{|G|}$ since only $x = y - a$ satisfies it

$\therefore$ if pick $x \in_u G$

then $a+x$ is also distributed uniformly in G

(write as "$a+x \in_u G$")

<u>note</u> if $G = \mathbb{Z}_2^n$

$(a_1 a_2 \dots a_n) \oplus (b_1 b_2 \dots b_n) = (a_1 \oplus b_1, a_2 \oplus b_2, \dots, a_n \oplus b_n)$

e.g. $(0\,1\,1\,0) \oplus (b_1\, b_2\, b_3\, b_4) = (\underbrace{0 \oplus b_1, 1 \oplus b_2, 1 \oplus b_3,}_{\text{distributed uniformly if } b_i\text{'s are}} 0 \oplus b_4)$

Let's just assume $G_1 = G_2$ (doesn't affect proof)

Behavior of test when f linear: ✓

Pass with prob 1

Behavior of test when f ε-far from linear:

ε-far "$\Rightarrow$" Prob each time fails $\geq \varepsilon/2$ $\Rightarrow$ need $\min\left\{\left(\frac{2}{\varepsilon}, 16\right)\right\} \cdot$ const many tests

(can get slightly better constants, important for some applications)

will prove contrapositive:

if f is s.t. $\delta \equiv \Pr[f$ fails one loop$]$

$= \Pr_{x,y}[f(x) + f(y) \neq f(x+y)] < 1/16$

then f is 2δ-close to linear

<u>def</u> $g(x) \equiv \underset{y}{\text{plurality}} [\underbrace{f(x+y) - f(y)}_{\text{y's vote for } f(x)}]$ ← break ties arbitrarily

<u>def</u> x is ρ-good if $\underbrace{\Pr_y [g(x) = f(x+y) - f(y)]}_{} \geq 1-\rho$

else ρ-bad

i.e. $> 1-\rho > \frac{1}{2}$ fraction of y's agree on their vote

x is ρ-good for $\rho < \frac{1}{2}$ $\Rightarrow$ $g(x)$ defined via majority element

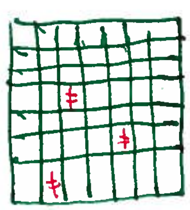
First: Show g + f agree usually

<u>Claim 1</u> $\rho < \frac{1}{2}$

$\Pr_x [x \text{ is } \rho\text{-good } \& \ g(x) = f(x)] > 1 - \delta/\rho$ $\Rightarrow$ fraction of x for which f + g agree is $> 1 - 2\delta > \frac{7}{8}$

<u>Pf of claim 1</u>

Picture of proof



~~matrix~~ fraction of "≠" entries $= \delta$

E[~~fraction~~ # "≠" entries in row] $= \delta$

Fraction rows with $> c \cdot \delta$ fraction entries has to be $< \frac{1}{c}$ by Markov's ≠ →

$\alpha_x = \Pr [f(x) \neq f(x+y) - f(y)]$

if $\alpha_x \leq \rho < \frac{1}{2}$ then x is ρ-good & $g(x) = f(x)$

Use Markov's ≠:

$$E_x[\alpha_x] = \frac{1}{|G|} \sum_{x \in G} \Pr_y [f(x) \neq f(x+y) - f(y)]$$

$$= \Pr_{x,y} [f(x) \neq f(x+y) - f(y)]$$

$$= \delta$$

so $\Pr[\alpha_x > \underset{\left(\frac{\rho}{\delta}\right)\delta}{\underset{\parallel}{\rho}}] \leq \frac{\delta}{\rho}$

Second: Show g "is a homomorphism" (at least where it is defined)

<u>Claim 2</u> $\rho < 1/4$

if x, y both ρ-good then (at least $3/4$ x's are $1/4$-good)

(1) $x+y$ is 2ρ-good

(2) $g(x+y) = g(x) + g(y)$

<u>Pf of Claim 2</u>

let $h(x+y) = g(x) + g(y)$

$\Pr_z[g(y) \neq f(y+z) - f(z)] < \rho$ since y is ρ good

$\Pr_z[g(x) \neq f(x+(y+z)) - f(y+z)] < \rho$ since x is ρ-good & $y+z \in_u G$

so $\Pr_z[h(x+y) = g(x) + g(y)$ by def

$= f(x+(y+z)) - \cancel{f(y+z)} + \cancel{f(y+z)} - f(z)] \geq 1 - 2\rho > 1/2$

union bnd using

$\Downarrow$

$g(x+y) = h(x+y)$ by def of g

$= g(x) + g(y)$ " " " h

& $x+y$ is 2ρ-good ∎

Third: show g is defined for all x

Claim 3 $\delta < 1/16$

$\forall x$, x is 4δ-good ($\frac{1}{4}$-good) & $g(x)$ defined via majority elt.

Pf. if $\exists y$ st. y & $x-y$ both 2δ-good

Claim 2 $\Rightarrow$ x is 4δ-good

& $g(x) = g(y) + g(x-y)$

but $\Pr_y[\underbrace{y \;\&\; (x-y)}_{\text{both uniform}} \text{ both } 2\delta\text{-good}] > \underbrace{1 - \big(\underbrace{\tfrac{\delta}{2\delta}}_{\text{claim 1}}\big)\cdot 2}_{\text{union bnd}} = 0$

$\Rightarrow \exists y$ st. y & $(x-y)$ both 2δ-good ■

Claim 3 $\Rightarrow$ g defined $\forall x$ as majority elt.
By claim 2, $\forall x, y$ $g(x) + g(y) = g(x+y)$
By claim 1, f & g agree $\geq 1 - 2\delta$ fraction of G ■

Improved theorem:

only need $\delta < 2/9$

(this means $O(9/2)$ many tests give < const prob of failure, instead of $O(16)$ – is this a big deal? actually it can be ...)

2/9 is tight: there are fctns that are far from linear but pass test with prob 7/9

Coppersmith's example:

$$f(x) = \begin{cases} 1 & \text{if } x = 1 \bmod 3 \\ 0 & \phantom{\text{if }} 0 \\ -1 & \phantom{\text{if }} 2 \end{cases}$$

integers over $\mathbb{Z}$

$f(x)+f(y) = 2$.
$f(x+y) = -1$

f fails when $x = y = 1 \bmod 3$
$x = y = 2 \bmod 3$ } Prob $\doteq 2/9$ ← not bad!

else passes

Closest linear fctn is $f(x) \equiv 0$ ← $\Pr[f(x) = g(x)] = 1/3$ very far!!
$\varepsilon = 2/3$

$\delta = 2/9$ is a "threshold"