Some Cool things we can do:

① Estimate sum of powers of degree 1 Fourier Coeffs of a fctn.

$\hat{f}(S)$ for $|S|=1$:

$\hat{f}(\{i\})$ denote as $\hat{f}(i)$

What is $\sum_{i=1}^{n} \hat{f}(i)^p$?

A random process:

Pick $X^{(1)} X^{(2)} \dots X^{(p-1)} \in \{\pm 1\}^n$

Pick noise vector μ s.t. each entry

is $+1$ with prob $\frac{1}{2} + \frac{1}{2}\eta$

-1 " " $\frac{1}{2} - \frac{1}{2}\eta$

$y \leftarrow f(X^{(1)}) f(X^{(2)}) \cdots f(X^{(p-1)}) f(X^{(1)} \odot X^{(2)} \odot \dots \odot X^{(p-1)} \odot \mu)$

Output y

Claim $E[y] = \sum_{S \subseteq [n]} \eta^{|S|} \hat{f}(S)^p$

Pf. since $f(x) = \sum_S \hat{f}(S)\chi_S(x)$

$$E[y] = E\Big[\sum_{S_1, S_2, \dots S_{p-1}, S_p} \hat{f}(S_1)\cdots\hat{f}(S_{p-1})\hat{f}(S_p)\chi_{S_1}(x^{(1)})\chi_{S_2}(x^{(2)})\cdots\chi_{S_{p-1}}(x^{(p-1)}) \cdot \chi_{S_p}(x^{(1)} \odot \cdots x^{(p)} \odot y)\Big]$$

$$= \sum_{S_1, S_2, \dots S_{p-1}, S_p} \hat{f}(S_1)\cdots\hat{f}(S_p)\, E\Big[\chi_{S_1 \Delta S_p}(x^{(1)})\chi_{S_2 \Delta S_p}(x^{(2)})\cdots\chi_{S_{p-1}\Delta S_p}(x^{(p-1)})\chi_{S_p}(y)\Big]$$

all independent so expectation of product = product of expectations

note if $S_1 = S_2 = \dots = S_p$ then $S_i \Delta S_p = \emptyset$ so $E[\chi_{S_i \Delta S_p}(x)] = 1$

$$\therefore E[\chi_{S_p}(y)] = 1 \cdot \Pr\Big[\prod_{i \in S_p} y_i = 1\Big] + (-1)\cdot \Pr\Big[\prod_{i \in S_p} y_i = (-1)\Big]$$

$$= \eta^{|S_p|}$$

proof by induction on $|S_p|$

Else some $S_i \Delta S_p \neq \emptyset$

$$\therefore E[\chi_{S_i \Delta S_p}(x)] = 0$$

$$= \sum_S \hat{f}(S)^p \cdot \eta^{|S|}$$

∎

Plan for estimating $\sum \hat{f}(i)^p$:

Chernoff/Hoeffding ⇓ use $O(\frac{1}{\eta^4})$ samples

1) estimate $E[f(x^{(1)}) f(x^{(2)}) \cdots f(x^{(p)})] = \hat{f}(\emptyset)^p$ ← i.e. use $\eta = 0$

to additive $\pm \eta^2$

2) estimate $E[f(x^{(1)}) f(x^{(2)}) \cdots f(x^{(p-1)}) f(x^{(1)} \circ \cdots \circ x^{(p-1)} \circ y)]$

$$= \sum_S \eta^{|S|} \hat{f}(S)^p$$

But ② − ① $= \underbrace{\sum_{|S|>0} \eta^{|S|} \hat{f}(S)^p}_{\equiv \gamma}$ ← we have estimate to within $\pm \eta^2$

Claim $\frac{\gamma}{\eta}$ is good estimate of $\sum_{|S|=1} \hat{f}(S)^p$

Why?

$$\sum_{|S|=1} \eta \hat{f}(S)^p = \sum_{|S|>0} \eta^{|S|} \hat{f}(S)^p - \sum_{|S|>1} \eta^{|S|} \hat{f}(S)^p$$

$$\frac{\sum_{|S|=1} \eta \hat{f}(S)^p}{\eta} \qquad \frac{\gamma}{\eta} \qquad \leq \eta^2 \sum_{|S|>1} |\hat{f}(S)^p|$$

$$\leq \eta^2 \sqrt{\sum_{|S|>1} \hat{f}(S)^2} \sqrt{\sum_{|S|>1} \left(\hat{f}(S)^{p-1}\right)^2}$$

$\sqrt{\sum_{|S|>1} \hat{f}(S)^2} \leq 1$ by Boolean Parseval

$\sqrt{\sum_{|S|>1} \left(\hat{f}(S)^{p-1}\right)^2} \leq \sum_{|S|>1} \hat{f}(S)^2$ since $|\hat{f}(S)| \leq 1$

$$\leq \eta^2 \sqrt{\sum_{|S|>1} \hat{f}(S)^2}$$

$$\leq \eta^2$$

So it is an additive estimate to within $\pm \eta$!!

⇒ for $p \geq 2$ can estimate $\sum_{|S|=1} \hat{f}(S)^p$ to w/in additive $\pm \eta$

with $O(p/\eta^4)$ queries

② Estimate max degree 1 Fourier coefficient

Fact if $\forall i \quad \hat{f}(i) < \alpha$

then $\sum_{|S|=1} \hat{f}(S)^4 = \sum_{i=1}^{n} \hat{f}(i)^4 < \alpha^2 \sum_{i=1}^{n} \hat{f}(i)^2 \le \alpha^2$

def τ-regular fctn : $\forall i \quad |\hat{f}(i)| < \tau$

Thm $\exists$ $O(\frac{1}{\tau^{16}})$-query test s.t.

1) if $\exists i$ s.t. $|\hat{f}(i)| \ge \tau$ then $\Pr[\text{reject}] \ge 3/4$ (Fail if not τ-regular)

2) if $\forall i$ s.t. $|\hat{f}(i)| < \frac{\tau^2}{4}$ then $\Pr[\text{accept}] \ge 3/4$ (Pass if $\frac{\tau^2}{4}$-regular)

Pf

Algorithm:

estimate $\sum_i \hat{f}(i)^4$ to w/in $\pm \frac{\tau^4}{4}$

accept if estimate $\le \frac{\tau^4}{2}$

Behavior:

if $\exists i$ s.t. $|\hat{f}(i)| \ge \tau$ then $\sum \hat{f}(i)^4 \ge \tau^4$

so estimate $\ge \tau^4 - \frac{\tau^4}{4} = \frac{3\tau^4}{4}$

$\Rightarrow$ algorithm accepts (unless estimate has really large error)

if $\forall i \quad |\hat{f}(i)| < \frac{\tau^2}{4}$ then $\sum \hat{f}(i)^4 \le \frac{\tau^4}{16}$ by note

so estimate $\le \frac{\tau^4}{16} + \frac{\tau^4}{4} = \frac{5\tau^2}{16} < \frac{\tau^4}{2}$

so reject ∎

estimate max degree $\Rightarrow$ dictator test

<u>def</u> f is a "dictator" if $f = \chi_{\{i\}} = \chi_i$ for some i

so $\hat{f}(i) = 1$

$\hat{f}(j) = 0$ for $j \neq i$

I can use const τ to test.

...

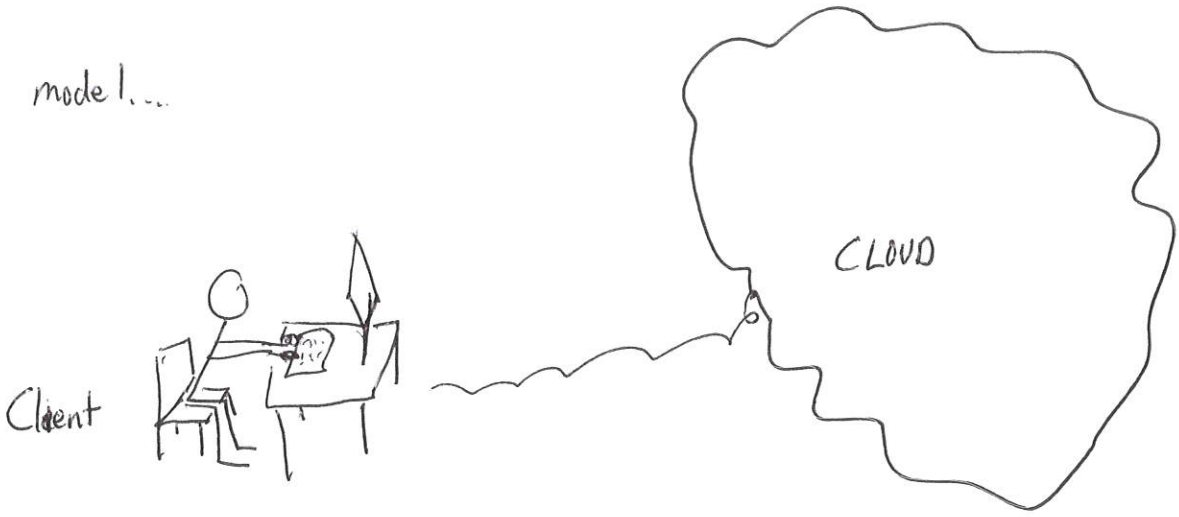
Lots of other dictator tests,
but this one is close to Hastad's test

Pick $x, y \in \{\pm 1\}^n$

$w \in \{\pm 1\}^n$ s.t. $\Pr[w_i = 1] = \delta$

Accept if $f(x)\, f(y)\, f(x \circ y \circ w) = 1$

Another model...



- Client sends computation on LARGE DATA SET to cloud
- Cloud returns result
- Why should the client trust it?

Can use Interactive proofs, IP probabilistically checkable proofs, ... PCP

Today:

- Client sends x to cloud
- Cloud writes $f(x)$ + proof that $f(x)$ is approximately correct in some

Example 1

How many website hits?

Setting: Cloud Prover wants to convince Client that $\geq k$ clicks were made to Client's website.

Goal: Given proof,
If # clicks $\geq k$, Client should pass
If # clicks $\leq (1-\varepsilon)k$, Client should fail
} with prob $\geq 3/4$

Proof.

proof = list of k click descriptions ← assume client can verify any description for "fake" or "real" in $O(1)$ steps
+ ? (duplicate detection)

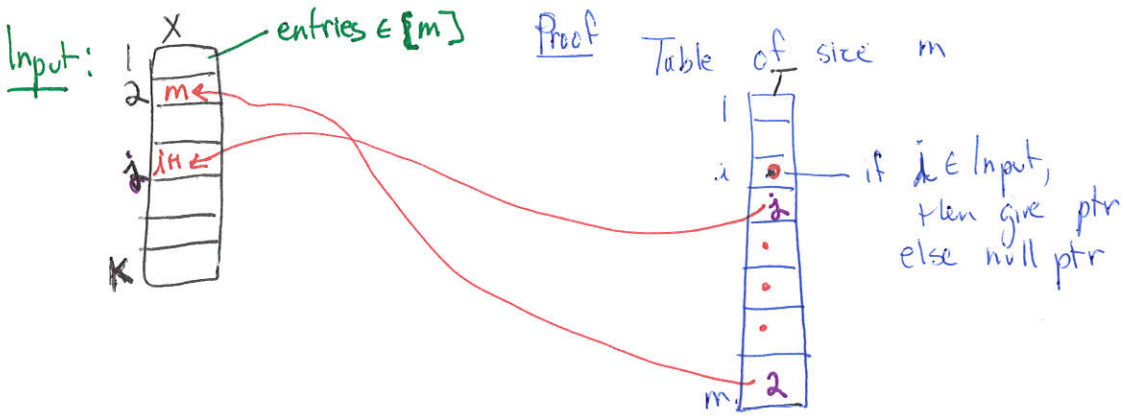
Clients Protocol:

not enough! what about duplicates? →

1) Check $\leq \frac{\varepsilon}{2}k$ click descriptions are fake — $O(\frac{1}{\varepsilon})$ queries

2) check $\leq \frac{\varepsilon}{2}k$ duplicates — $O(\frac{1}{\varepsilon})$ queries

How to check for duplicates?



Protocol

Repeat $O(1/\varepsilon)$ times
Pick random $j \in [k]$
$\ell \leftarrow X[j]$
look at locn $T(\ell)$:
if $T(\ell)$ contains j Pass & continue
else fail & halt

Proof of correctness:

if all k entries of X distinct, will always PASS
if $\exists \geq \varepsilon k$ duplicates,
$\Pr[j$ is a duplicate, & not in $T] \geq \varepsilon$
$\Rightarrow$ Fail ▨

Example 1'

Does G have cut of size $\geq k$?

proof =
- array A of size n
  $A[i] = 0$ for nodes i on "left"
  1 "right"
- array B of k edges that cross cut

Client: - verifies that B contains $\geq (\varepsilon/2)k$ legal cut edges wrt A's cut
- verifies that B contains $\leq \frac{\varepsilon}{2}k$ duplicates

Example 2

Bin packing

Setting $X_1 \dots X_n \in [B]$

k bins of size B

Prover I can fit all of $X_1 \dots X_n$ in k bins

Goal given proof

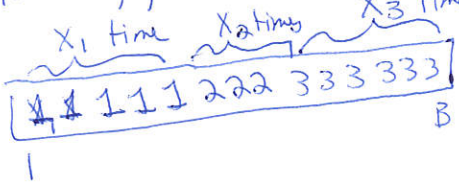
if all X_i's fit in k bins, pass

if $\leq (1-\varepsilon) n$ X_i's fit in k bins Fail

Proof k arrays $[1..B]$

in each array, put X_i's for that bin

ie. if $X_1 X_2 X_3$ assigned to bin 1



Protocol:

Check $\geq (1-\varepsilon) k$ X_i's are allocated space $O\left(\frac{B}{\varepsilon}\right)$ queries