

19/10/23 Schwartz-Zippel - de Nello - Lipfor

Thm:- [schwartz-zippel]  $\rightarrow$  multilinear.

Let  $f: \{0,1\}^n \rightarrow \mathbb{R}$  of  
deg d.

Then  $\Pr_{x \sim \{0,1\}^n} [f(x) \neq 0] \geq \frac{1}{2^d}$

## Linearity testing

What is a linear function?

$$f: \{0,1\}^n \rightarrow \{0,1\}$$

$$\{0,1\}^n \equiv \mathbb{F}_2^n$$

$$u, v \in \mathbb{F}_2^n \quad u \oplus v \in \mathbb{F}_2^n$$

$$0 \cdot 0 = 0$$

$\Rightarrow$  Defn:-  $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  is

said to be linear.

$$(1) \quad f(x \oplus y) = f(x) \oplus f(y)$$

$\forall x, y \in \mathbb{F}_2^n$

$$\mathbb{F}_2 = \{ \{0, 1\}, +, *\}$$

$$\left. \begin{array}{l} 0 \oplus 0 = 0 \\ 1 \oplus 1 = 0 \\ 1 \oplus 0 = 1 \end{array} \right\} \quad \begin{array}{l} 0 \cdot 0 = 0 \\ 1 \cdot 1 = 1 \end{array}$$

$$(2) \quad f(x) = \sum_{i \in S} x_i \quad \text{for}$$

Some  $S \subseteq [n]$ .

$$= \bigoplus_{i \in S} x_i$$

Are these equivalent?

$$(2) \Rightarrow (1)$$

$$f(x+y) = \sum_{i \in S} (x+y)_i$$

$$= \sum_{i \in S} x_i + y_i$$

$$= \sum_{i \in S} x_i + \sum_{i \in S} y_i$$

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

$$\textcircled{1} \Rightarrow \textcircled{2}$$

$$x = (x_1, \dots, x_n) = x_1 e_1 + x_2 e_2 + \dots + x_n e_n$$

$e_i$  = 0-1 vector of length n  
c.f. 1 at i<sup>th</sup> position  
and 0 everywhere

$$f(x) = f(x_1 e_1 + x_2 e_2 + \dots + x_n e_n)$$

$$= \sum_{i=1}^n x_i f(e_i)$$

$$= \sum_{i \in T} x_i$$

$$T := \{j \mid f(e_j) = 1\}$$

# ⇒ Property testing.

Let  $f: \{0,1\}^n \rightarrow \{0,1\}$

$g: \{0,1\}^n \rightarrow \{0,1\}$

$$\text{dist}(f, g) := \Pr_x [f(x) \neq g(x)]$$

uniform over  $\{0,1\}^n$

A property  $P$  is just a  
subset of functions.

e.g. the set of all linear  
functions.

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

$f \in ? \mathcal{P}$

$$\text{dist}(f, \mathcal{P}) = \min_{g \in \mathcal{P}} \text{dist}(f, g)$$

when  $f \in \mathcal{P}$

$$\text{dist}(f, \mathcal{P}) = 0 =$$

$$\text{dist}(f, \mathcal{P}) \geq 1 - \varepsilon$$

Defn: A property tester

with  $q(\varepsilon)$  queries is

a randomized algorithm

that has the following property

(1) if  $f \in P$  then

algorithm accepts  $f$

with prob  $\geq \frac{2}{3}$

(2) if  $\text{dist}(f, P) \geq \epsilon$

then algorithm accepts

$f$  with prob  $\leq \frac{1}{3}$ .

$$(1') f(x+y) = f(x) + f(y)$$

for "most" pairs of  $x$  and  $y$

②  $f(x) = \sum_{i \in S} x_i$  for

"most" inputs  $x$ .

②  $\Rightarrow$  ① doable

①  $\Rightarrow$  ② do now!

BLR - Linearity testing

→ Choose  $x \sim \mathbb{F}_2^n$  uniformly at random

choose  $y \sim \mathbb{F}_2^n$  //

Define  $z = x \oplus y$

Accept if  $f(z) = f(x) + f(y)$ .

Obs!- if  $f$  is linear.

Then  $\Pr [\text{BLR accepts } f] = 1$ .

Question!- What if  $\text{dist}(f, \text{linear})$  is large?

$$0 \equiv \text{False} \equiv 1$$

$$1 \equiv \text{True} \equiv -1$$

( $\oplus$ )

\*

$$(0 \oplus 1) = 1 \quad -1 \oplus -1 = 1.$$

$$f: \{\pm 1\}^n \rightarrow \{\pm 1\}$$

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

$$\Sigma = (x_1y_1, x_2y_2, \dots, x_ny_n)$$

BLR accepts  $f$

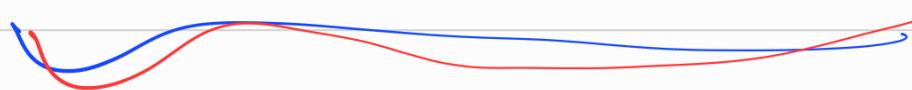
$$\text{iff } f(x) \cdot f(y) \cdot f(z) = 1.$$

$$\Pr_{x,y} [\text{BLR accepts } f]$$

$$= \Pr_{x,y} [f(x) \cdot f(y) \cdot f(z) = 1]$$

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

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



$$\mathbb{E}_{x,y} [f(x) f(y) f(z)]$$

$$= \mathbb{E}_{x,y} \left[ \left( \sum_{S \subseteq [n]} \hat{f}(S) \prod_{i \in S} x_i \right) \cdot \left( \sum_{T \subseteq [n]} \hat{f}(T) \cdot \prod_{i \in T} y_i \right) \cdot \left( \sum_{U \subseteq [n]} \hat{f}(U) \cdot \prod_{i \in U} z_i \right) \right]$$

$$= \mathbb{E}_{x,y} \left[ \sum_{S, T, U \subseteq [n]} \hat{f}(S) \cdot \hat{f}(T) \cdot \hat{f}(U) \cdot \prod_{i \in S} x_i \cdot \prod_{i \in T} y_i \cdot \prod_{i \in U} z_i \right]$$

$$= \mathbb{E}_{x,y} \left[ \sum_{S, T, U \subseteq [n]} \hat{f}(S) \cdot \hat{f}(T) \cdot \hat{f}(U) \cdot \prod_{i \in S} x_i \cdot \prod_{i \in T} y_i \cdot \prod_{i \in U} x_i y_i \right]$$

$$= \mathbb{E}_{x,y} \left[ \sum_{S, T, U \subseteq [n]} \hat{f}(S) \cdot \hat{f}(T) \cdot \hat{f}(U) \cdot \prod_{i \in S \Delta U} x_i \cdot \prod_{i \in T \Delta U} y_i \right]$$

Symmetric difference

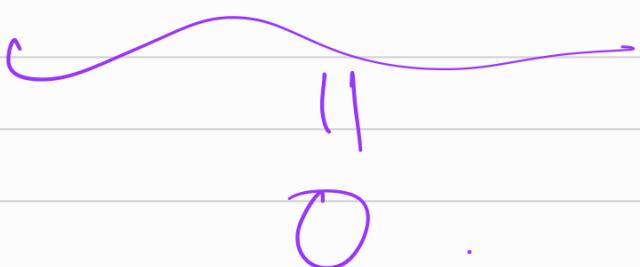
$$= \sum_{S, T, U \subseteq [n]} \hat{f}(S) \cdot \hat{f}(T) \cdot \hat{f}(U) \cdot \prod_{\substack{x_i, y_i \\ i \in S \Delta U \\ i \in T \Delta U}} \mathbb{E}_{x_i} [\prod x_i] \cdot \mathbb{E}_{y_i} [\prod y_i]$$

if  $S \Delta U = \emptyset$   
 $T \Delta U = \emptyset$

$$\Rightarrow S = T = U$$

$$= \mathbb{E}_x \left[ \prod_{i \in S \Delta U} x_i \right] \cdot \mathbb{E}_y \left[ \prod_{i \in T \Delta U} y_i \right]$$

if  $S \Delta U \neq \emptyset$   
or  $T \Delta U \neq \emptyset$



$$= \sum_{S \subseteq [n]} \hat{f}(S)^3$$

$$S_0 \quad \mathbb{E}_{x,y} [f(x) \cdot f(y) \cdot f(z)] = \sum_{S \subseteq [n]} \hat{f}(S)^3$$

Recall

$$\Pr[\text{BLR accepts } f] =$$

$$\frac{1}{2} + \frac{1}{2} \mathbb{E}_{x,y} [f(x) \cdot f(y) \cdot f(z)]$$

$$= \frac{1}{2} + \frac{1}{2} \sum_{S \subseteq [n]} \hat{f}(S)^3$$

$\uparrow$  if  $\Pr[\text{BLR accepts } f] \geq 1 - \varepsilon$

then  $\exists S \subseteq [n]$  s.t.

$$\text{dist}(f, \chi_S) \leq \varepsilon$$

$$\hat{f}(s) = E_x [f(x) \cdot \chi_s(x)]$$

$$= \Pr_x [f(x) = \chi_s(x)]$$

$$= \Pr_x [f(x) \neq \chi_s(x)]$$

$$= (-\Pr_x [f(x) \neq \chi_s(x)])$$

$$= -\Pr_x [f(x) \neq \chi_s(x)]$$

$$2 - 2 \text{dist}(f, \chi_s).$$

if  $\text{dist}(f, \chi_s) \leq \underline{\epsilon}$

$$\Rightarrow \hat{f}(s) \geq 1 - 2\underline{\epsilon} =$$

$\Pr[\text{BLR accepts}]$

$$1 - \underline{\epsilon} \leq$$

$$\leq \frac{1}{2} + \frac{1}{2} \sum_{S \subseteq [n]} \hat{f}(s)^3$$

$$2 - 2\varepsilon \leq 1 + \sum_{S \subseteq [n]} \hat{f}(S)^3$$

$$1 - 2\varepsilon \leq \sum_{S \subseteq [n]} \hat{f}(S)^3$$

$$\leq \left\{ \max_S \hat{f}(S) \right\}^3 \sum_{T \subseteq [n]} \hat{f}(T)^2$$

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