Lecture 07

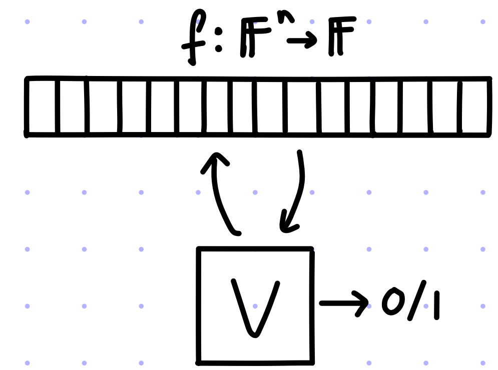
Linearity Testing

Warmup 1: All-Zero Testing

A function $f:\mathbb{F}^n \to \mathbb{F}$ is ALL-ZERO if $\forall x \in \mathbb{F}^n$ $f(x)=0$.

QUESTION: is there a $O(1)$-query test V s.t. $\forall f:\mathbb{F}^n \to \mathbb{F}$

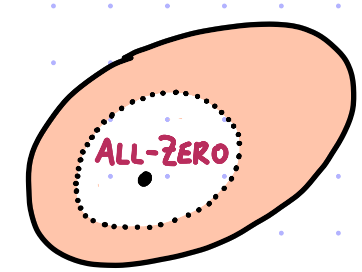
- COMPLETENESS: if f is ALL-ZERO then $\Pr[V^f=1]=1$
- SOUNDNESS: if f is not ALL-ZERO then $\Pr[V^f=1] \leq 1/2$



ANSWER: No. (If f is $\neq 0$ at a single location, how can a $O(1)$-query V detect this?)

RELAXED QUESTION: is there a $O(1)$-query test V s.t. $\forall f:\mathbb{F}^n \to \mathbb{F}$

- COMPLETENESS: if f is ALL-ZERO then $\Pr[V^f=1]=1$
- SOUNDNESS: if f is far from ALL-ZERO then $\Pr[V^f=1] \leq 1/2$



We use (relative) Hamming distance: $\Delta(f,g) := \Pr_{x\in\mathbb{F}^n}[f(x)\neq g(x)]$ and $\Delta(f,S) := \min_{g\in S} \Delta(f,g)$.

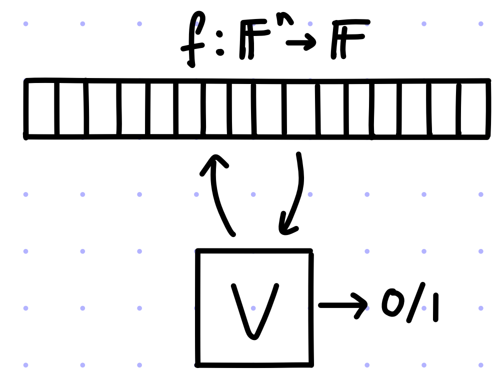
ANSWER: YES! $V_0^f :=$ sample random $x \in \mathbb{F}^n$ and check that $f(x)=0$

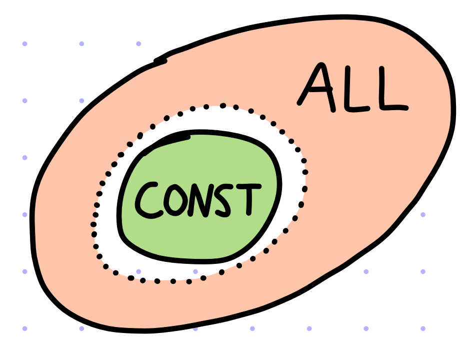
- if f is ALL-ZERO then $\Pr[V^f=1] = \Pr_x[f(x)=0]=1$
- if $\Delta(f,\text{ALL-ZERO}) \geq \delta$ then $\Pr[V^f=1] = 1-\Pr[V^f=0] = 1-\Pr_x[f(x)\neq 0] = 1-\Delta(f,\text{ALL-ZERO}) \leq 1-\delta$.

Warmup 2: Constant Testing

Define the set $\mathrm{CONST} := \{ f : \mathbb{F}^n \to \mathbb{F} : \exists c \in \mathbb{F} \text{ s.t. } \forall x \in \mathbb{F}^n \ f(x) = c \}$ (constant functions).

We cannot expect to distinguish (with small error) $f \in \mathrm{CONST}$ vs $f \notin \mathrm{CONST}$ by querying f at few locations.





What about distinguishing $f \in \mathrm{CONST}$ vs $\Delta(f, \mathrm{CONST}) \geq \delta$?

$V^f :=$ Sample random $x \in \mathbb{F}^n$ and check that $f(x) = f(0^n)$.

- If $f \in \mathrm{CONST}$ then $\exists c \in \mathbb{F}$ s.t. $\forall x \in \mathbb{F}^n \ f(x) = c$

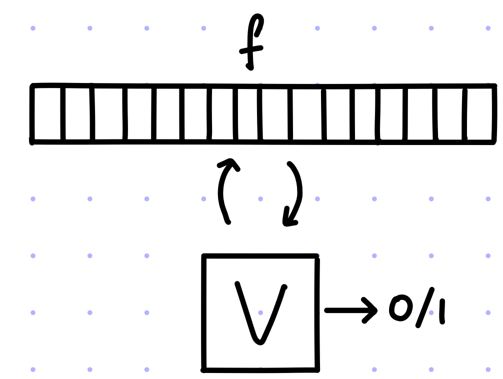
  so $\Pr[V^f = 1] = \Pr_x[f(x) = f(0^n)] = \Pr_x[c = c] = 1$.

- If $\Delta(f, \mathrm{CONST}) \geq \delta$ then
$$\begin{aligned} \Pr[V^f = 1] &= 1 - \Pr[V^f = 0] \\ &= 1 - \Pr_x[f(x) \neq f(0^n)] \\ &\leq 1 - \min_{c \in \mathbb{F}} \Pr_x[f(x) = c] \\ &= 1 - \Delta(f, K) \leq 1 - \delta. \end{aligned}$$

Proximity Testing

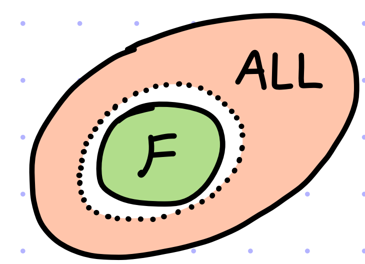
Both warmups are examples of problems in PROPERTY TESTING.

A PROPERTY is a set of functions $\mathcal{F} = \{f : D \to \Sigma\}$.



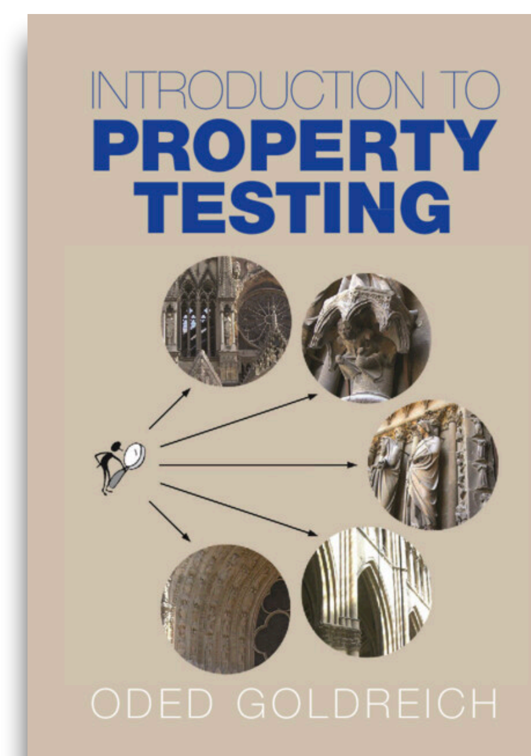
def: V is a test for the property $\mathcal{F}$ with proximity error ε if

- COMPLETENESS: $\forall f \in \mathcal{F} \quad \Pr[V^f = 1] = 1$
- SOUNDNESS: $\forall \delta \in [0,1] \ \forall f$ with $\Delta(f, \mathcal{F}) \geq \delta \quad \Pr[V^f = 1] \leq \varepsilon(\delta)$



The distance Δ is usually (relative) Hamming distance.

Sometimes Δ is ℓ_p distance (e.g. when $\Sigma = [0,1]$) or other metrics.



MAIN GOAL: minimize the query complexity q of the test V

In warmup 1: $\mathcal{F} = \{\text{ALL-ZERO}\}$, $\varepsilon(\delta) = 1 - \delta$, $q = 1$

In warmup 2: $\mathcal{F} = \text{CONST}$, $\varepsilon(\delta) = 1 - \delta$, $q = 2$

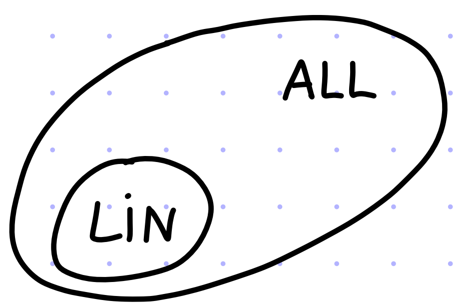
See Goldreich's book for an introduction to property testing. ⟶

Today we are interested in testing an algebraic property:

LINEARITY TESTING

Linear Functions

A function $f : \mathbb{F}^n \to \mathbb{F}$ is linear if $\exists c \in \mathbb{F}^n$ s.t. $f(x) = \sum_{i=1}^{n} c_i x_i$.



$\mathrm{ALL} = \{ f : \mathbb{F}^n \to \mathbb{F} \}$ $\qquad |\mathrm{ALL}| = |\mathbb{F}|^{|\mathbb{F}|^n}$

$\mathrm{LIN} = \{ f : \mathbb{F}^n \to \mathbb{F} \text{ is linear} \}$ $\qquad |\mathrm{LIN}| = |\mathbb{F}|^n$

The set LIN is known as the HADAMARD CODE.

LIN is a linear error-correcting code (since LIN is an $\mathbb{F}$-linear space).

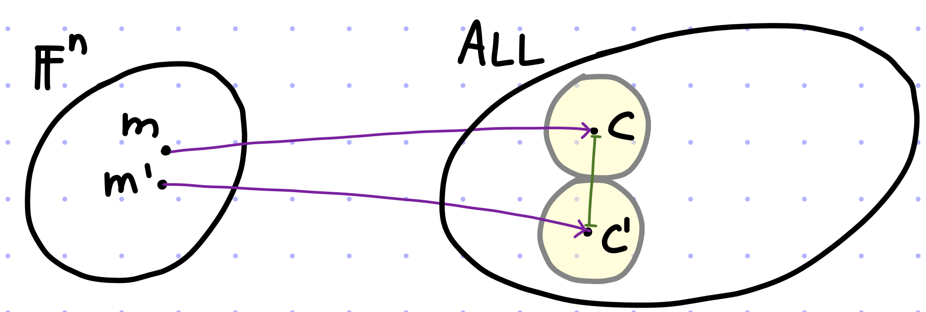
A message $m \in \mathbb{F}^n$ is mapped to the codeword $c := (\langle a, m \rangle)_{a \in \mathbb{F}^n}$.

Parameters of the code: message length $= n$

block length $= |\mathbb{F}|^n$

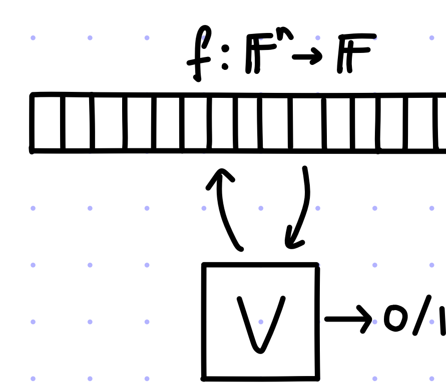
relative distance $= 1 - \frac{1}{|\mathbb{F}|}$

$\left(\forall \text{ distinct } f, g \in \mathrm{LIN} \ \Pr_{x \leftarrow \mathbb{F}^n}[f(x) = g(x)] \leq \frac{1}{|\mathbb{F}|}\right)$

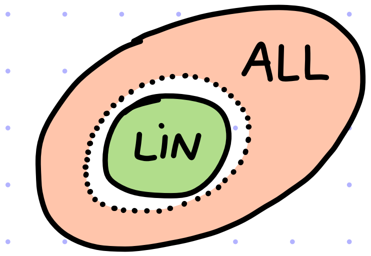


We CANNOT distinguish (with small error) $f \in \mathrm{LIN}$ vs $f \notin \mathrm{LIN}$ by querying f at few locations.

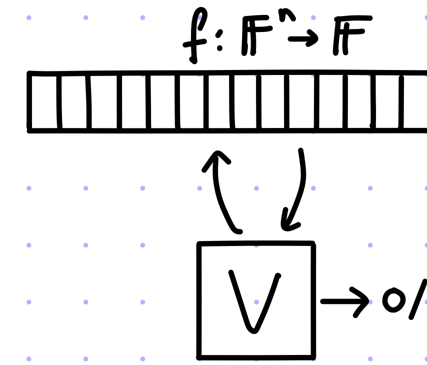
If $f \notin \mathrm{LIN}$ differs in 1 location from $\bar{f} \in \mathrm{LIN}$, no $O(1)$-query test V detects that $f \notin \mathrm{LIN}$ with constant soundness error.



Linearity Testing



GOAL: decide between "$f \in \mathrm{LIN}$" and "f is far from LIN".



<u>def:</u> V is a LINEARITY TEST (for the field $\mathbb{F}$) with proximity error ε if

- COMPLETENESS: $\forall f \in \mathrm{LIN} \;\; \Pr[V^f = 1] = 1$
- SOUNDNESS: $\forall \delta \in [0,1] \; \forall f$ with $\Delta(f, \mathrm{LIN}) \geq \delta \;\; \Pr[V^f = 1] \leq \varepsilon(\delta)$

(relative) Hamming distance

EXAMPLE: $V^{f: \mathbb{F}^n \to \mathbb{F}}$:= Sample random $x \in \mathbb{F}^n$ and check that $f(x) = \sum_{i=1}^n f(e_i) x_i$. $n+1$ queries

- if $f \in \mathrm{LIN}$ then $\exists c \in \mathbb{F}^n$ s.t. $f(x) = \sum_{i=1}^n c_i x_i$

  so $\Pr[V^f = 1] = \Pr_x\left[f(x) = \sum_{i=1}^n f(e_i) x_i\right] = \Pr_x\left[\sum_{i=1}^n c_i x_i = \sum_{i=1}^n c_i x_i\right] = 1$.

- if $\Delta(f, \mathrm{LIN}) \geq \delta$ then

  $\Pr[V^f = 1] = 1 - \Pr[V^f = 0] = 1 - \Pr_x\left[f(x) \neq \sum_{i=1}^n f(e_i) x_i\right] \leq 1 - \min_{g \in \mathrm{LIN}} \Pr_x[f(x) \neq g(x)] = 1 - \Delta(f, \mathrm{LIN}) \leq 1 - \delta$.

PROBLEM: query complexity is LARGE

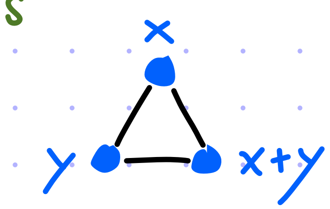
In fact everything we did so far is TRIVIAL: queries $= \left\{\begin{array}{l}\text{queries to determine} \\ \text{which function } f \in \mathcal{F}\end{array}\right\} \cup \{1 \text{ random query}\}$

- no queries for ALL-ZERO
- 1 query for CONST
- n queries for LIN

Q: Is there a non-trivial (eg. constant query) linearity test?

The Blum-Luby-Rubinfeld Test

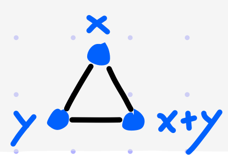
The idea is to leverage DUALITY: $f \in \mathrm{LIN} \leftrightarrow \overbrace{\forall x,y \in \mathbb{F}^n \;\; f(x)+f(y)=f(x+y)}^{|\mathbb{F}|^{2n} \text{ local constraints}}$



The BLR test for linearity:

$V_{\mathrm{BLR}}^{f:\mathbb{F}^n \to \mathbb{F}} :=$ 1. Sample $x,y \in \mathbb{F}^n$

2. Check that $f(x)+f(y)=f(x+y)$



randomness: $2n$ field elements

queries: 3 locations of f

Completeness: if $f \in \mathrm{LIN}$ then $\forall x,y \in \mathbb{F}^n \;\; f(x)+f(y) = f(x+y)$ so $\Pr[V_{\mathrm{BLR}}^f = 1] = 1$

Soundness: non-trivial. (An example of a LOCAL-TO-GLOBAL PHENOMENON.)

theorem: $\Pr[V_{\mathrm{BLR}}^f = 0] \geq \min\{1/6, \frac{1}{2} \cdot \Delta(f, \mathrm{LIN})\}$

Equivalently:

$\Pr[V_{\mathrm{BLR}}^f = 1] \leq \max\{5/6, 1 - \frac{1}{2}\Delta(f, \mathrm{LIN})\}$

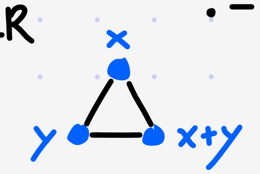
Intuition:

- if f is linear then each $y \in \mathbb{F}^n$ "votes" for the same value of x: $\forall y \in \mathbb{F}^n$, $f(x+y) - f(y) = f(x)$
- if f is not linear then we can still consider, for every x, the most popular value:

the plurality correction $g_f : \mathbb{F}^n \to \mathbb{F}$ is $g_f(x) := \arg\max_{v \in \mathbb{F}} \left| \{ y \in \mathbb{F}^n \mid v = f(x+y) - f(y) \} \right|$

Proof overview

$V_{BLR}^{f:\mathbb{F}^n \to \mathbb{F}} :=$ 1. Sample $x, y \in \mathbb{F}^n$



2. Check that $f(x)+f(y)=f(x+y)$

theorem: $\Pr\left[V_{BLR}^f = 0\right] \geq \min\left\{1/6, \frac{1}{2}\cdot \Delta(f, \mathrm{LIN})\right\}$

The plurality correction is

$$g_f : \mathbb{F}^n \to \mathbb{F} \quad \text{where} \quad g_f(x) := \arg\max_{v \in \mathbb{F}} \left| \left\{ y \in \mathbb{F}^n \,\middle|\, v = f(x+y) - f(y) \right\} \right|$$

- Part 1: $\Pr[V_{BLR}^f = 0] \geq \frac{1}{2}\cdot\Delta(f, g_f)$ far from plurality correction → many bad triangles
- Part 2: $\Pr[V_{BLR}^f = 0] < \frac{1}{6} \to g_f \in \mathrm{LIN}$ few bad triangles → plurality correction is linear

Conclusion:

- If $\Pr[V_{BLR}^f = 0] \geq 1/6$ then we are done.
- If $\Pr[V_{BLR}^f = 0] < 1/6$ then (by Part 2) g_f is linear and (by Part 1) we get

$$\Pr\left[V_{BLR}^f = 0\right] \geq \frac{1}{2}\cdot\Delta(f, g_f) \geq \frac{1}{2}\cdot\Delta(f, \mathrm{LIN}). \quad \blacksquare$$

Analysis of BLR Test - Part 1

The plurality correction of f is $g_f(x) := \arg\max_{v \in \mathbb{F}} \left| \{ y \in \mathbb{F}^n \mid v = f(x+y) - f(y) \} \right|$.

If g_f is far from f then V^f_{BLR} rejects with high probability:

claim: $\Pr[V^f_{BLR} = 0] \geq \frac{1}{2} \cdot \Delta(f, g_f)$.

But $\Delta(f, g_f) = 0 \not\Rightarrow \Pr[V^f_{BLR} = 0] = 0$.
Exercise: find a counterexample.

proof: Define $S := \{ x \in \mathbb{F}^n \mid \Pr_{y \leftarrow \mathbb{F}^n}[f(x) \neq f(x+y) - f(y)] \geq \frac{1}{2} \}$.

For every $x \notin S$, $\Pr_{y \leftarrow \mathbb{F}^n}[f(x) = f(x+y) - f(y)] > \frac{1}{2}$ (more than half of y's vote for $f(x)$), so $f(x) = g_f(x)$.

Hence $\Delta(f, g_f) \leq \frac{|S|}{|\mathbb{F}|^n}$ ($\forall x$ if $f(x) \neq g(x)$ then $x \in S$).

$$
\begin{aligned}
\text{So } \Pr[V^f_{BLR} = 0] &= \Pr_x[x \in S] \cdot \Pr_{x,y}[V^f_{BLR} = 0 \mid x \in S] + \Pr_x[x \notin S] \cdot \Pr_{x,y}[V^f_{BLR} = 0 \mid x \notin S] \\
&\geq \frac{|S|}{|\mathbb{F}|^n} \cdot \min_{x \in S} \left\{ \Pr_y[f(x) \neq f(x+y) - f(y)] \right\} + 0 \\
&\geq \frac{|S|}{|\mathbb{F}|^n} \cdot \frac{1}{2} \geq \Delta(f, g_f) \cdot \frac{1}{2}.
\end{aligned}
$$

$\blacksquare$

Analysis of BLR Test - Collision Lemma

We show that few bad triangles imply many votes for the plurality correction.

<u>claim:</u> $\forall x \in \mathbb{F}^n \quad \Pr_{y \leftarrow \mathbb{F}^n}[g_f(x) = f(x+y) - f(y)] \geq 1 - 2 \cdot \Pr[V_{BLR}^f = 0]$.

<u>proof:</u> $\Pr_{y \leftarrow \mathbb{F}^n}[g_f(x) = f(x+y) - f(y)] = \max_{v \in \mathbb{F}} \Pr_{y \leftarrow \mathbb{F}^n}[v = f(x+y) - f(y)]$

$\sum_i p_i^2 \leq \max_i \{p_i\} \cdot \sum_i p_i$

$$\geq \sum_{v \in \mathbb{F}} \Pr_{y \leftarrow \mathbb{F}^n}[v = f(x+y) - f(y)]^2$$

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

$$\geq 1 - 2 \cdot \Pr[V_{BLR}^f = 0].$$

We now analyze the COLLISION PROBABILITY.

Note that $f(x+y) - f(y) \neq f(x+z) - f(z) \leftrightarrow f(x+y) + f(z) \neq f(x+z) + f(y)$

$\rightarrow f(x+y) + f(z) \neq f(x+y+z)$ OR $f(x+z) + f(y) \neq f(x+y+z)$.

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

$$\leq \Pr_{y,z}[f(x+y) + f(z) \neq f(x+y+z)] + \Pr_{y,z}[f(x+z) + f(y) \neq f(x+y+z)]$$

$\leq 2 \cdot \Pr[V_{BLR}^f = 0]$ (because $(x+y, z)$ and $(x+z, y)$ are random in $\mathbb{F}^n \times \mathbb{F}^n$). ■

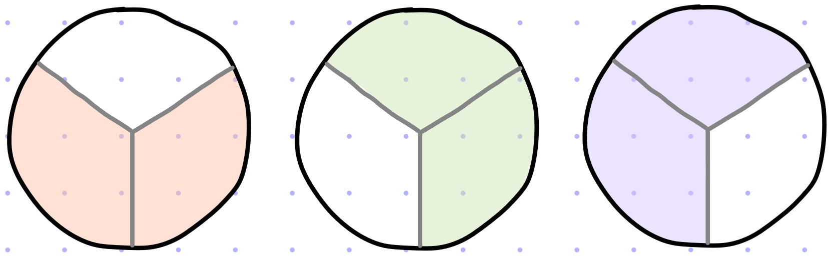
Analysis of BLR Test - Part 2

<u>claim:</u> if $\Pr[V_{BLR}^{f} = 0] < \frac{1}{6}$ then $g_f \in LIN$

<u>proof:</u> Fix $x, y \in \mathbb{F}^n$. We show that $g_f(x) + g_f(y) = g_f(x+y)$.

- $\Pr_z[g_f(x) = f(x+z) - f(z)] \overset{\text{collision lemma}}{\geq} 1 - 2 \cdot \Pr[V_{BLR}^{f} = 0] > \frac{2}{3}$
- $\Pr_z[g_f(y) = f(z) - f(z-y)] \underset{\text{rename } z-y \text{ to } z}{=} \Pr_z[g_f(y) = f(y+z) - f(z)] \overset{\text{collision lemma}}{\geq} 1 - 2 \cdot \Pr[V_{BLR}^{f} = 0] > \frac{2}{3}$
- $\Pr_z[g_f(x+y) = f(x+z) - f(z-y)] \underset{\text{rename } z-y \text{ to } z}{=} \Pr_z[g_f(x+y) = f(x+y+z) - f(z)] \overset{\text{collision lemma}}{\geq} 1 - 2 \cdot \Pr[V_{BLR}^{f} = 0] > \frac{2}{3}$

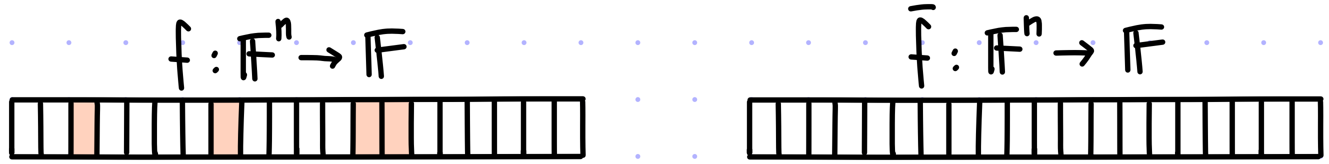
Hence $\exists z^* \in \mathbb{F}^n$ s.t. $\left\{ \begin{array}{lll} g_f(x) & = f(x+z^*) & - f(z^*) \\ g_f(y) & = f(z^*) & - f(z^*-y) \\ g_f(x+y) & = f(x+z^*) & - f(z^*-y) \end{array} \right\}$.



We conclude that $g_f(x) + g_f(y) = f(x+z^*) - f(z^*-y) = g_f(x+y)$. ■

Local Correction of Linear Functions

Suppose that $f : \mathbb{F}^n \to \mathbb{F}$ is ε-close to linear: $\exists \bar{f} \in \mathrm{LIN}$ s.t. $\Delta(f, \bar{f}) \leq \varepsilon$.



GOAL: given $x \in \mathbb{F}^n$ and oracle access to f, output $\bar{f}(x)$.

SOLUTION: leverage the fact that $\forall y \in \mathbb{F}^n \quad \bar{f}(x) = \bar{f}(x+y) - \bar{f}(y)$.

$A^f(x)$: Sample $y \in \mathbb{F}^n$ and output $f(x+y) - f(y)$.

<u>claim:</u> $\Pr[A^f(x) \neq \bar{f}(x)] \leq 2 \cdot \varepsilon$

<u>proof:</u> Since y is random in $\mathbb{F}^n$, we know that:

- $\Pr_y[f(y) \neq \bar{f}(y)] \leq \varepsilon$
- $\Pr_y[f(x+y) \neq \bar{f}(x+y)] \leq \varepsilon$

We conclude that $\Pr_y[f(x+y) - f(y) \neq \bar{f}(x)] = \Pr_y[f(x+y) - f(y) \neq \bar{f}(x+y) - \bar{f}(y)]$

$$\leq \Pr_y[f(y) \neq \bar{f}(y) \vee f(x+y) \neq \bar{f}(x+y)] \leq 2\varepsilon.$$

■

Local Correction of Linear Functions [2/2]

We can reduce error via REPETITION:

most frequent value in the set

$A^f(x,t)$: Sample $y_1,\dots,y_t \in \mathbb{F}^n$ and output $\mathrm{plurality}_{i\in[t]}\{f(x+y_i)-f(y_i)\}$.

<u>claim:</u> if $\bar{f} \in \mathrm{LIN}$ and $\Delta(f,\bar{f}) \le \varepsilon < \frac{1}{4}$ then $\Pr[A^f(x,t) \ne \bar{f}(x)] \le 2\cdot e^{-\frac{t}{4}\cdot(\frac{1}{2}-2\varepsilon)^2}$.

<u>proof:</u> By a CONCENTRATION argument.

Recall (one version of) the Chernoff Bound:

Let $(z_i)_{i\in[t]}$ be independent random variables in $[0,1]$.

Define $z := \frac{1}{t}\sum_{i\in[t]} z_i$. Then $\forall \gamma \ge 0$ $\Pr[|z-\mathbb{E}[z]| \ge \gamma] \le 2\cdot e^{-\frac{t}{4}\cdot\gamma^2}$.

Define $z_i :=$ "$f(x+y_i)-f(y_i) \ne \bar{f}(x)$". Note that $\mathbb{E}[z] \le 2\cdot\varepsilon < \frac{1}{2}$.

If $\mathrm{plurality}_{i\in[t]}\{f(x+y_i)-f(y_i)\} \ne \bar{f}(x)$ then $\sum_{i\in[t]} z_i \ge t/2$.

Hence $\Pr[A^f(x,t) \ne \bar{f}(x)] \le \Pr[\sum_{i\in[t]} z_i \ge t/2] = \Pr[z \ge 1/2]$

$$= \Pr[z-\mathbb{E}[z] \ge 1/2 - \mathbb{E}[z]]$$

$$\le \Pr[|z-\mathbb{E}[z]| \ge 1/2-\mathbb{E}[z]] \le 2\cdot e^{-\frac{t}{4}\cdot(1/2-\mathbb{E}[z])^2} \le 2\cdot e^{-\frac{t}{4}\cdot(1/2-2\varepsilon)^2}. \quad \blacksquare$$

$\mathbb{E}[z] < \frac{1}{2}$

Chernoff Bound

Homomorphism Testing

The analysis we saw is the COMBINATORIAL ANALYSIS of the BLR test.

It extends, essentially with no changes, to achieve HOMOMORPHISM TESTING.

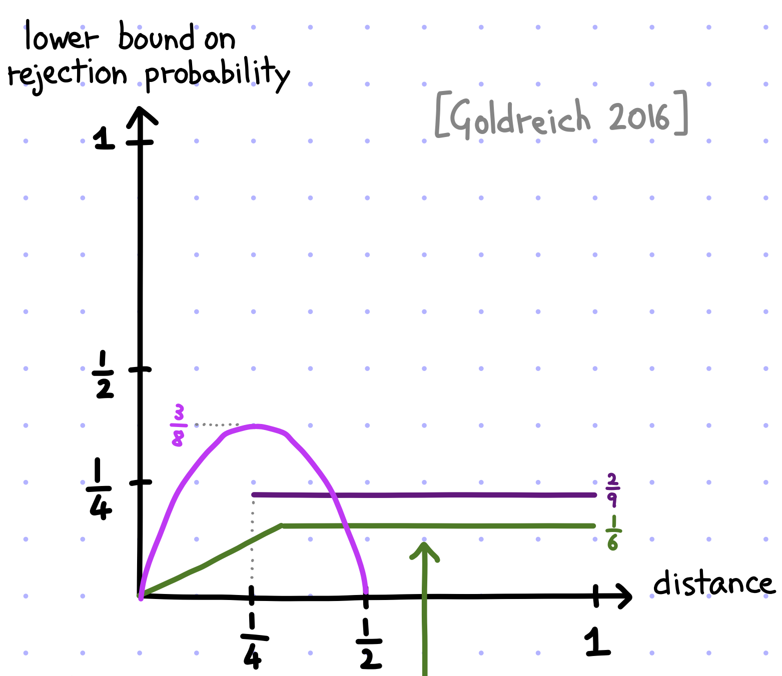
Let G,H be groups. The set of group homomorphisms from G to H is

$$\mathrm{HOM}(G,H) := \{ f: G \to H \mid \forall x,y \in G \ \ f(x) +_H f(y) = f(x +_G y) \}.$$

Example:
$\mathrm{Hom}((\mathbb{F}^n,+),(\mathbb{F},+)) = \mathrm{LIN}$

The BLR test extends naturally:

$V_{\mathrm{BLR}}^{f:G\to H}$:= 1. Sample $x,y \in G$.
2. Check that $f(x) +_H f(y) = f(x +_G y)$.



Completeness: if $f \in \mathrm{HOM}(G,H)$ then $\Pr[V_{\mathrm{BLR}}^f = 1] = 1$

Soundness: $\Pr[V_{\mathrm{BLR}}^f = 0] \geq \min\{\frac{1}{6}, \frac{1}{2}\cdot \Delta(f, \mathrm{HOM}(G,H))\}$ ← today's analysis

The lower bound can be somewhat improved (see diagram).

OPEN: determine the function $\varepsilon: [0,1] \to [0,1]$ s.t. $\Pr[V_{\mathrm{BLR}}^f = 0] = \varepsilon(\Delta(f, \mathrm{HOM}(G,H)))$.

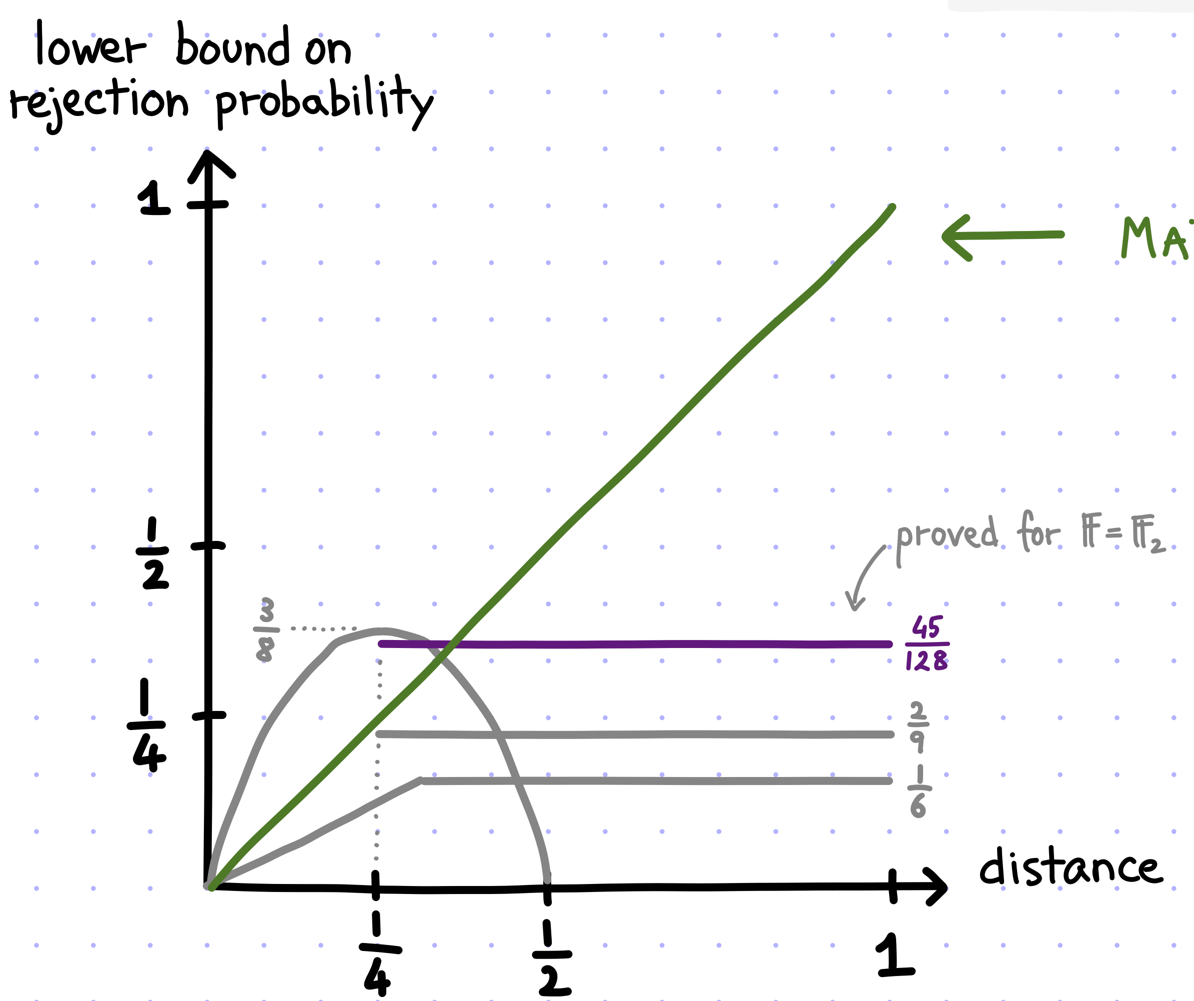
Improved Analysis for Finite Fields

A different analysis, for linear functions over finite fields, achieves an improved bound.

theorem: $\forall f: \mathbb{F}^n \to \mathbb{F},\ \Pr[V_{BLR}^{f} = 0] \geq \Delta(f, \mathrm{LIN})$

$V_{BLR}^{f:\mathbb{F}^n \to \mathbb{F}}$:= 1. Sample $x, y \in \mathbb{F}^n$ and $a, b \in \mathbb{F} \setminus \{0\}$.

2. Check that $a f(x) + b f(y) = f(ax + by)$.



MAIN TOOL: Fourier analysis

Improved Analysis for Finite Fields

theorem: $\forall f: \mathbb{F}^n \to \mathbb{F},\ \Pr[V_{BLR}^f = 0] \geq \Delta(f, LIN)$

$V_{BLR}^{f:\mathbb{F}^n \to \mathbb{F}} :=$

1. Sample $x, y \in \mathbb{F}^n$ and $a, b \in \mathbb{F} \setminus \{0\}$.
2. Check that $a f(x) + b f(y) = f(ax + by)$.

We outline the proof approach.

Let $q = p^e$ be the prime-power size of $\mathbb{F}$.

field trace map $Tr: \mathbb{F}_q \to \mathbb{F}_p$

$Tr(x) := \sum_{i=0}^{e-1} x^{p^i} \bmod p$

For $\alpha \in \mathbb{F}_q^n$, the character function $\chi_\alpha: \mathbb{F}_q^n \to \mathbb{C}$ is $\chi_\alpha(x) := \omega_p^{Tr(\langle \alpha, x \rangle)}$.

p-th root of unity $\omega_p := e^{\frac{2\pi i}{p}}$

(If $q = p$ then $Tr(x) = x$ so χ_α simplifies to $\chi_\alpha(x) = \omega_p^{\langle \alpha, x \rangle}$.)

The set $\{\chi_\alpha\}_{\alpha \in \mathbb{F}_q^n}$ is an orthonormal basis for the functions $\{g: \mathbb{F}_q^n \to \mathbb{C}\}$

with the inner product $\langle g, h \rangle := \mathbb{E}_{x \leftarrow \mathbb{F}_q^n}[g(x)\overline{h(x)}]$.

complex conjugate

Hence, every $g: \mathbb{F}_q^n \to \mathbb{C}$ can be written uniquely as $g(x) = \sum_{\alpha \in \mathbb{F}_q^n} \hat{g}(\alpha) \chi_\alpha(x)$

where $\{\hat{g}(\alpha)\}_{\alpha \in \mathbb{F}_q^n} := \{\langle g, \chi_\alpha \rangle\}_{\alpha \in \mathbb{F}_q^n}$ are g's Fourier coefficients.

Useful for derivations:

- Parseval's identity: $\langle g, g \rangle = \sum_{\alpha \in \mathbb{F}_q^n} \hat{g}(\alpha)\overline{\hat{g}(\alpha)} = \sum_{\alpha \in \mathbb{F}_q^n} |\hat{g}(\alpha)|^2$
- Plancherel's identity: $\langle g, h \rangle = \sum_{\alpha \in \mathbb{F}_q^n} \hat{g}(\alpha)\overline{\hat{h}(\alpha)}$

Improved Analysis for Finite Fields

The Fourier set of $f:\mathbb{F}_q^n \to \mathbb{F}_q$ is $\Phi(f) := \{\varphi_c : \mathbb{F}_q^n \to \mathbb{C} \,,\; \varphi_c(x) := \omega_p^{\mathrm{Tr}(c\cdot f(x))}\}_{c\in\mathbb{F}_q^*}$.

Note that $|\Phi(f)| = q-1$.

EXAMPLE: If $\ell:\mathbb{F}_q^n \to \mathbb{F}_q$ is the linear function $\ell(x) = \langle\alpha, x\rangle$ then $\Phi(f) = \{\chi_{c\alpha}\}_{c\in\mathbb{F}_q^*}$.

Note that $\hat{\chi}_{c\alpha}(c\alpha) = 1$ and, $\forall \beta\in\mathbb{F}_q^n\setminus\{c\alpha\}$, $\hat{\chi}_{c\alpha}(\beta) = 0$. ⊛

The distance between two functions can be expressed in terms of their Fourier sets:

lemma: $\forall f,g:\mathbb{F}_q^n \to \mathbb{F}_q$ with Fourier sets $\{\varphi_c\}_{c\in\mathbb{F}_q^*}$ and $\{\gamma_c\}_{c\in\mathbb{F}_q^*}$

$$\Delta(f,g) = \Pr_{x\leftarrow\mathbb{F}_q^n}[f(x)\neq g(x)] = 1 - \frac{1}{q}\cdot\Big(1 + \sum_{c\in\mathbb{F}_q^*}\langle\varphi_c,\gamma_c\rangle\Big).$$

Let $f:\mathbb{F}_q^n \to \mathbb{F}_q$ with Fourier set $\{\varphi_c\}_{c\in\mathbb{F}_q^n}$.

The distance to linear functions is

Plancherel's identity & ⊛:

$$\langle\varphi_c, \chi_{c\alpha}\rangle = \sum_{\beta\in\mathbb{F}_q^n}\hat{\varphi}_c(\beta)\overline{\hat{\chi}_{c\alpha}(\beta)} = \hat{\varphi}_c(c\alpha)$$

$$\Delta(f,\mathrm{LIN}) = \min_{\alpha\in\mathbb{F}_q^n}\Big\{1 - \frac{1}{q}\cdot\Big(1 + \sum_{c\in\mathbb{F}_q^*}\langle\varphi_c,\chi_{c\alpha}\rangle\Big)\Big\} = 1 - \frac{1}{q}\Big(1 + \max_{\alpha\in\mathbb{F}_q^n}\sum_{c\in\mathbb{F}_q^*}\langle\varphi_c,\chi_{c\alpha}\rangle\Big) = 1 - \frac{1}{q}\Big(1 + \max_{\alpha\in\mathbb{F}_q^n}\sum_{c\in\mathbb{F}_q^*}\hat{\varphi}_c(c\alpha)\Big).$$

Then more analysis yields the desired bound:

$$\Pr[V_{BLR}^f = 1] = \frac{1}{q}\Big(1 + \frac{1}{(q-1)^2}\sum_{\alpha\in\mathbb{F}_q^n}\Big(\sum_{c\in\mathbb{F}_q^*}\hat{\varphi}_c(c\alpha)\Big)^3\Big) \leq \frac{1}{q}\Big(1 + \max_{\alpha\in\mathbb{F}_q^n}\sum_{c\in\mathbb{F}_q^*}\hat{\varphi}_c(c\alpha)\,\frac{1}{(q-1)^2}\sum_{\alpha\in\mathbb{F}_q^n}\Big(\sum_{c\in\mathbb{F}_q^*}\hat{\varphi}_c(c\alpha)\Big)^2\Big)$$

most of the work

$$\leq \frac{1}{q}\Big(1 + \max_{\alpha\in\mathbb{F}_q^n}\sum_{c\in\mathbb{F}_q^*}\hat{\varphi}_c(c\alpha)\cdot 1\Big) = 1 - \Delta(f,\mathrm{LIN}).$$

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_q^n}\hat{\varphi}_c(c\alpha)\hat{\varphi}_d(d\alpha) &= \sum_{\alpha\in\mathbb{F}_q^n}\sum_{x,y\in\mathbb{F}_q^n} q^{-2n}\varphi_c(x)\varphi_d(y)\,\omega_p^{-\langle c\alpha,x\rangle-\langle d\alpha,y\rangle}\\ &= q^{-n}\sum_{x\in\mathbb{F}_q^n}\varphi_c(x)\varphi_d(-cd^{-1}x)\\ &\leq q^{-n}\sum_{x\in\mathbb{F}_q^n}|\varphi_c(x)\varphi_d(-cd^{-1}x)|\\ &= q^{-n}\cdot q^n = 1\end{aligned}$$

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_q^n}\Big(\sum_{c\in\mathbb{F}_q^*}\hat{\varphi}_c(c\alpha)\Big)^2 &= \sum_{c\in\mathbb{F}_q^*}\sum_{d\in\mathbb{F}_q^*}\Big(\sum_{\alpha\in\mathbb{F}_q^n}\hat{\varphi}_c(c\alpha)\hat{\varphi}_d(d\alpha)\Big)\\ &\leq \sum_{c\in\mathbb{F}_q^*}\sum_{d\in\mathbb{F}_q^*}1 = (q-1)^2\end{aligned}$$

Improved Analysis for Finite Fields

The special case $q=2$ corresponds to linearity testing for boolean functions $f: \mathbb{F}_2^n \to \mathbb{F}_2$.

The analysis of the BLR test simplifies to an elegant and concise computation, now via Fourier analysis of boolean functions.

Theorem 1.30. *Suppose the BLR Test accepts $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with probability $1-\epsilon$. Then f is ϵ-close to being linear.*

Proof. In order to use the Fourier transform we encode f's output by $\pm 1 \in \mathbb{R}$; thus the acceptance condition of the BLR Test becomes $f(\boldsymbol{x})f(\boldsymbol{y}) = f(\boldsymbol{x}+\boldsymbol{y})$. Since

$$\tfrac{1}{2} + \tfrac{1}{2} f(\boldsymbol{x})f(\boldsymbol{y})f(\boldsymbol{x}+\boldsymbol{y}) = \begin{cases} 1 & \text{if } f(\boldsymbol{x})f(\boldsymbol{y}) = f(\boldsymbol{x}+\boldsymbol{y}), \\ 0 & \text{if } f(\boldsymbol{x})f(\boldsymbol{y}) \neq f(\boldsymbol{x}+\boldsymbol{y}), \end{cases}$$

we conclude

$$\begin{aligned}
1-\epsilon = \mathbf{Pr}[\text{BLR accepts } f] &= \mathop{\mathbf{E}}_{\boldsymbol{x},\boldsymbol{y}}[\tfrac{1}{2} + \tfrac{1}{2} f(\boldsymbol{x})f(\boldsymbol{y})f(\boldsymbol{x}+\boldsymbol{y})] \\
&= \tfrac{1}{2} + \tfrac{1}{2} \mathop{\mathbf{E}}_{\boldsymbol{x}}[f(\boldsymbol{x}) \cdot \mathop{\mathbf{E}}_{\boldsymbol{y}}[f(\boldsymbol{y})f(\boldsymbol{x}+\boldsymbol{y})]] \\
&= \tfrac{1}{2} + \tfrac{1}{2} \mathop{\mathbf{E}}_{\boldsymbol{x}}[f(\boldsymbol{x}) \cdot (f * f)(\boldsymbol{x})] && \text{(by definition)} \\
&= \tfrac{1}{2} + \tfrac{1}{2} \sum_{S \subseteq [n]} \widehat{f}(S) \widehat{f * f}(S) && \text{(Plancherel)} \\
&= \tfrac{1}{2} + \tfrac{1}{2} \sum_{S \subseteq [n]} \widehat{f}(S)^3 && \text{(Theorem 1.27).}
\end{aligned}$$

We rearrange this equality and then continue:

$$\begin{aligned}
1-2\epsilon &= \sum_{S \subseteq [n]} \widehat{f}(S)^3 && (1.10) \\
&\leq \max_{S \subseteq [n]} \{\widehat{f}(S)\} \cdot \sum_{S \subseteq [n]} \widehat{f}(S)^2 \\
&= \max_{S \subseteq [n]} \{\widehat{f}(S)\} && \text{(Parseval).}
\end{aligned}$$

But $\widehat{f}(S) = \langle f, \chi_S \rangle = 1 - 2\mathrm{dist}(f, \chi_S)$ (Proposition 1.9). Hence there exists some $S^* \subseteq [n]$ such that $1-2\epsilon \leq 1-2\mathrm{dist}(f, \chi_{S^*})$; i.e., f is ϵ-close to the linear function χ_{S^*}. $\square$

Source: Analysis of Boolean Functions
Ryan O'Donnell, 2014

Bibliography

Linearity Testing

- [BLR 1990]: Self-testing/correcting with applications to numerical problems, by Manuel Blum, Michael Luby, and Ronitt Rubinfeld.
- [Goldreich 2017]: Introduction to property testing, by Oded Goldreich.
- [BCHKS 1996]: Linearity testing in characteristic two, by Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos A. Kiwi, Madhu Sudan. Tighter analysis using Fourier
- [GS 2002]: Locally testable codes and PCPs of almost-linear length, by Oded Goldreich, Madhu Sudan.
- [Goldreich 2016]: Lecture notes on linearity (group homomorphism) testing, by Oded Goldreich.
- (▸A comedy of errors), by Ronitt Rubinfeld.