

Question 1

Recall Chebyshev inequality: $\forall t > 0$, for mean μ and standard deviation $\sigma \neq 0$, $\Pr[|X - \mu| \geq t \cdot \sigma] \leq \frac{1}{t^2}$

a) Use Chebyshev to prove that for $X \geq 0$
 $\Pr[X = 0] \leq \frac{\sigma^2}{\mu^2}$

Solution (Sketch)

Simple direct application of Chebyshev for $t = \frac{\mu}{\sigma}$ gives you the bound.

b) Now, prove a tighter bound using Cauchy Schwartz
for $X \geq 0$, $\Pr[X = 0] \leq \frac{\sigma^2}{\mathbb{E}[X^2]}$

Solution

For $X \geq 0$ and $Y = 1_{\{X > 0\}}$ (the indicator function)

Apply Cauchy-Schwarz to get

$$\mathbb{E}[X] = \mathbb{E}[XY] \leq \sqrt{\mathbb{E}[X^2]} \cdot \sqrt{\Pr[X > 0]}$$

$$\Rightarrow \Pr[X > 0] \geq \frac{(\mathbb{E}[X])^2}{\mathbb{E}[X^2]}$$

$$\text{So } \Pr[X = 0] = 1 - \Pr[X > 0] \leq \frac{\sigma^2}{\mathbb{E}[X^2]}$$

Question 2:

a) We call $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ an affine function if $f(x) = a \cdot x + b$ for some $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$.
Show that f is affine iff $f(x) + f(y) + f(z) = f(x+y+z)$
 $\forall x, y, z \in \mathbb{F}_2^n$.

Solution:

Assume $f(x) = a \cdot x + b$ for some $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$

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

$$\begin{aligned} f(x) + f(y) + f(z) &= (a \cdot x + b) + (a \cdot y + b) + (a \cdot z + b) \\ &= a \cdot (x + y + z) + b + 2b \stackrel{0}{\rightarrow} (\because b \in \mathbb{F}_2) \\ &= a \cdot (x + y + z) + b \\ &= f(x + y + z) \end{aligned}$$

Conversely, assume $f(x+y+z) = f(x) + f(y) + f(z) \forall x, y, z$

Then, for $z=0$

$$f(x+y) = f(x) + f(y) + f(0) \quad \forall x, y \in \mathbb{F}_2^n$$

Take $g(x) = f(x) + f(0)$

$$\begin{aligned} \text{Then, } g(x) + g(y) &= f(x) + f(y) + \underbrace{f(0) + f(0)}_{0 \text{ } (\because f(0) \in \mathbb{F}_2)} \\ &= f(x+y) + f(0) \\ &= g(x+y) \quad (\because f(0) = -f(0)) \\ &\quad \forall x, y \in \mathbb{F}_2^n \end{aligned}$$

$\Rightarrow g$ is linear

$\Rightarrow g$ is affine $\therefore f$ is affine.

(b) Let $f: \mathbb{F}_2^n \rightarrow \mathbb{R}$. Suppose $x, y, z \sim \mathbb{F}_2^n$ independently and uniformly. Show that

$$\mathbb{E}[f(x) f(y) f(z) f(x+y+z)] = \sum_s \hat{f}(s)^4.$$

Solution:

$$\begin{aligned} & \mathbb{E}_{x,y,z} [f(x) f(y) f(z) f(x+y+z)] \\ &= \mathbb{E}_{x,y} [f(x) f(y) \mathbb{E}_z [f(z) \cdot f(x+y+z)]] \\ &= \mathbb{E}_{x,y} [f(x) f(y) (f * f)(x+y)] \\ &= \mathbb{E}_x [f(x) \mathbb{E}_y [f(y) (f * f)(x+y)]] \\ &= \mathbb{E}_x [f(x) f * f * f(x)] \\ &= \sum_{s \in \mathbb{F}_2^n} \hat{f}(s) \cdot \widehat{(f * f * f)}(s) = \sum_{s \in \mathbb{F}_2^n} (\hat{f}(s))^4 \end{aligned}$$

(c) Give a 4-query test for a function $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ with the following property: if the test accepts with probability $1-\epsilon$ the f is ϵ -close to being affine.

Solution:

Instead of $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, consider $g: \mathbb{F}_2^n \rightarrow \{-1, +1\}$ such that

$$g(x) = (-1)^{f(x)}$$

It's equivalent to test g .

The test just samples $x, y, z \sim \mathbb{F}_2^n$ independently and queries g on x, y, z & $x+y+z$.
If $g(x+y+z) = g(x)g(y)g(z)$ then output 1

else output N.

Analyzing the test:

$$\Pr[\text{test above accepts } g] = \mathbb{E}_{x,y,z} \left[\frac{1}{2} + \frac{1}{2} g(x)g(y)g(z)g(x+y+z) \right]$$

(indicator
for whether
test accepts or not)

$$= \frac{1}{2} + \frac{1}{2} \mathbb{E} [g(x)g(y)g(z)g(x+y+z)]$$

$$= \frac{1}{2} + \frac{1}{2} \sum_{s \in \mathbb{Z}_m} \hat{g}(s)^4 \quad (\text{use b'})$$

$$\leq \frac{1}{2} + \frac{1}{2} \max_{s \in \mathbb{Z}_m} \{ \hat{g}(s)^2 \} \sum_{s \in \mathbb{Z}_m} \hat{g}(s)^2$$

$\downarrow$
 $= 1$
(Parseval)

$$= \frac{1}{2} + \frac{1}{2} \max_{s \in \mathbb{Z}_m} \{ \hat{g}(s)^2 \}$$

$\downarrow$
Why? Think!

$$\leq \frac{1}{2} + \frac{1}{2} \max_{s \in \mathbb{Z}_m} \{ |\hat{g}(s)| \} \rightarrow \textcircled{1}$$

$$\hat{g}(s) = \langle g, \chi_s \rangle = 1 - 2 \text{dist}(g, \chi_s) \quad (\text{showed this in class}) \rightarrow \textcircled{2}$$

Using the fact that the max is attained at some $s^* \in \mathbb{Z}_m$ & if $\Pr[\text{test accepts } g] \geq 1 - \epsilon$

$\Rightarrow$ for this $s^* \in \mathbb{Z}_m$, $\textcircled{1}$ & $\textcircled{2}$ give:

$$1 - 2\epsilon \leq \max_{s \in \mathbb{Z}_m} \{ |\hat{g}(s)| \} = |1 - 2 \text{dist}(g, \chi_{s^*})|$$

If $1 - 2 \text{dist}(g, \chi_{s^*}) \geq 0$, then we get
 $\text{dist}(g, \chi_{s^*}) \leq \epsilon$

If $1 - 2 \text{dist}(g, \chi_{s^*}) < 0$, then $|1 - 2 \text{dist}(g, \chi_{s^*})| = 2 \text{dist}(g, \chi_{s^*}) - 1$

$$\Rightarrow 2 \operatorname{dist}(g, \chi_{S^*}) - 1 \geq 1 - 2\varepsilon$$

$$\Rightarrow \operatorname{dist}(g, \chi_{S^*}) \geq 1 - \varepsilon$$

$$\Rightarrow \underbrace{1 - \operatorname{dist}(g, \chi_{S^*})}_{\parallel} \leq \varepsilon$$

$$\operatorname{dist}(g, -\chi_{S^*})$$

∴ g is ε -close to an affine function.

Question 3:

Let $f: \mathbb{R}_2 \rightarrow \{t, 1\}$ and suppose $\operatorname{dist}(f, \chi_{S^*}) = \delta$.
Show that $|\hat{f}(S)| \leq 2\delta$, $\forall S \neq S^*$.

Solution:

$$\hat{f}(S) = \mathbb{E}_X [f(X) \chi_S(X)]$$

$$= \Pr[f(X) = \chi_S(X)] - \Pr[f(X) \neq \chi_S(X)]$$

$$= 1 - 2 \operatorname{dist}(f, \chi_S)$$

$$\forall S \neq S^*, \langle \chi_S, \chi_{S^*} \rangle = 0 \Rightarrow \operatorname{dist}(\chi_S, \chi_{S^*}) = \frac{1}{2}$$

By triangle inequality, we have $\forall S \neq S^*$

$$\stackrel{= \frac{1}{2}}{\operatorname{dist}(\chi_S, \chi_{S^*})} \leq \operatorname{dist}(\chi_S, f) + \underbrace{\operatorname{dist}(f, \chi_{S^*})}_{\delta \text{ (given)}}$$

$$\Rightarrow \operatorname{dist}(\chi_S, f) \geq \frac{1}{2} - \delta \quad \forall S \neq S^*$$

$$\Rightarrow \hat{f}(S) \leq 2\delta \quad \forall S \neq S^*$$

Question 4:

Write the number of roots (including repeated roots) of the following polynomials:

1) $p(x) = x^q - x \in \mathbb{F}_q[x]$

Answer

Exactly q roots.

$$p(x) = x(x^{q-1} - 1)$$

this has exactly $q-1$ roots $\because \mathbb{F}_q^*$ is a multiplicative group of order $q-1$.

2) $r(x) = (x^4+1)(x^2+1) \in \mathbb{F}_9[x]$

Answer : 6 roots

Solⁿ 1 Consider the polynomial

$$\begin{aligned} x^9 - x &= x(x^8 - 1) \\ &\underbrace{\text{has 9 roots by part 1)}}_{\text{has 9 roots by part 1)}} = x(x^4 + 1)(x^4 - 1) \\ &= x(x^4 + 1) \underbrace{(x^2 + 1)(x^2 - 1)}_{\text{factor of } x^2 - x} \end{aligned}$$

$\because x$ has 1 root & $(x^2 - 1)$ has 2 roots, the factor $(x^4 + 1)(x^2 + 1)$ must have $9 - 3 = 6$ roots.

Solⁿ 2 Since it is a small field, you can check if $\mathbb{F}_9$ elements below are roots $\because$
 $\{a + bX : a, b \in \mathbb{F}_3\} \quad (\because \mathbb{F}_9 = \{\mathbb{F}_3[X] \bmod (x^2 + 1)\})$