CS 860 Topics in Coding Theory Oct. 30th, 2025

Lecture 15

Lecturer: Elena Grigorescu *Scribe: Kylee Schram*

Summary: Introduce Local decoding. Testing membership in Hadamard code → testing linearity. We also briefly discuss origins of property testing and other applications.

0.1 Local Decoding

The algorithms we have seen so far are for classical codes, and are linear time or worse. Now we will look at sublinear codes.

Let w be a received word. We can't read all of it, because maybe that takes too much time or space. Define $\mathcal{A}$ which can query w at an index, and return the value of w at that index.

We would like to know if a received word w is in the **Had** code:

- w is δ - far if $dist(w, \mathbf{Had}) \geq \delta 2^n$
- w is δ - close otherwise

0.2 Property Testing

Definition 1 *Code C is $(q, 1-\epsilon_1, \epsilon_2, \delta)$-locally testable if $\exists$ random algorithm $\mathcal{A}$ with query (oracle) access to input w such that:*

- $\mathcal{A}^w$ *makes q queries*
- ***completeness:*** *if w in C then* $\Pr[A^w accepts] \geq 1 - \epsilon_1$
- ***soundness:*** *if w is δ-far from C then* $\Pr[A^w accepts] \leq \epsilon_2$

$\epsilon_1 = 0$ is one-sided with perfect completeness

$\mathcal{A}$ is an adaptive algorithm if query q_i depends on prior queries. An algorithm that makes all queries at once and then looks at all answers together is one-way non-adaptive.

Theorem 2 ***Had*** *is $(3, 1, \delta, \delta)$-locally testable, where*
Had$=\{C_a : \mathbb{F}_2^n \to \mathbb{F}_2 | C_a(x) =< a, x >\}$

Proof Idea

WTS: we can make an algorithm $\mathcal{A}$ with 3 queries such that:

- if w is a linear function, accept with probability 1
- else if w is δ-far (wrt Hamming distance), then $\mathcal{A}$ accepts with probability $< \delta$

How can we test for linearity in 3 queries? If w is linear, then $f(x) + f(y) = f(x + y)$
Test:

Given query access to function f (let this be w from above, change of notation), pick $x, y \in \mathbb{F}_2^n$ uniformly random.

- check if f(x) + f(y) = f(x+y)
- if so, accept
- else reject

Now we need to show that $\mathcal{A}$ has the accept/reject probabilities we want.
We need some ideas from Fourier analysis, which we refresh below. ■

0.3 Refresh: Fourier Analysis

When looking at $C : \mathbb{F}_2^n \to \mathbb{F}_2$, it was useful to embed into $\mathbb{R}$, $c(x) \to (-1)^{c(x)}$.
Gives c_a lin $\to (-1)^{c_a(x)}$
$c_a(x) + c_a(y) = c_a(x + y) \to (-1)^{c_a(x)} + (-1)^{c_a(y)} = (-1)^{c_a(x+y)}$
Now we list some identities/facts we might like to use later:

- Hadamard maps to orthonormal basis
- $\chi_a(x) = (-1)^{x \cdot a}$
- $\{\chi_a\}_{a \in \mathbb{F}_2^n}$ is an orthonormal basis $\mathbb{R}^{2^n}$
- $\chi_0(x) = 1, \forall x$
- $\mathbb{E}_{x \in \mathbb{F}_2^n}[\chi_a(x)] = \begin{cases} 1 & a = 0 \\ 0 & else \end{cases}$
- linearity of characters:
  $\chi_a(x)\chi_b(x) = \chi_{a+b}(x)$
  $\chi_a(x)\chi_a(y) = \chi_a(x + y)$
- $f, g : \mathbb{F}_2^n \to \{\pm 1\}$
- inner product $< f, g >= \mathbb{E}_{x \in \mathbb{F}_2^n}[f(x) \cdot g(x)]$
- $< f, f >= \|f\|^2$
- $f(x) = \sum_{\alpha \in \mathbb{F}_2^n} \hat{f}_\alpha \cdot \chi_\alpha(x)$
- $\hat{f}_\alpha =< f, \chi_a > \in [-1, 1]$
- Parsifal: $< f, f >= \Sigma_\alpha \hat{f}_\alpha^2 = \mathbb{E}[f^2(x)] = 1$

0.4 Back to the proof

We want to look at the distance between candidate f and the set of all characters for linear functions.

Claim 3 $< f, g >= 1 - 2d(f, g)$

Proof

$$< f, g > = \frac{1}{2^n} \sum (x)g(x) \tag{1}$$
$$= \frac{1}{2^n}(\#x|f(x) = g(x)) - (\#x|f(x) \neq g(x)) \tag{2}$$
$$= \frac{1}{2^n}(2^n - 2(\#x|f(x) \neq g(x))) \tag{3}$$
$$= 1 - 2d(f, g) \tag{4}$$

■

Corollary 4 *Distance between f and χ_α, an arbitrary character:*

$$d(f, \{\chi_\alpha\}) = \min_\alpha \frac{1}{2} - \frac{1}{2}\hat{f}_\alpha \tag{5}$$
$$= \frac{1}{2} - \frac{1}{2} \max_\alpha \hat{f}_\alpha \tag{6}$$

Proof

$$d(f, \chi_\alpha = \frac{1}{2} - \frac{1}{2} < f, \chi_\alpha \tag{7}$$
$$= \frac{1}{2} - \frac{1}{2}\hat{f}_\alpha \tag{8}$$

■

Recall that deciding memebership in **Had** is the same as deciding if f is a linear function. Then, we WTS:

Proof Idea

If f is δ-far, Pr[test accepts] $< \delta$

Usually easier to show: If the test accepts wp $> \delta$, then f is δ-close.

Then, we want to write the probability as a function of Fourier coefficients.

Define $I_{\alpha,\beta} = \begin{cases} 0 & f(\alpha)f(\beta) = f(\alpha + \beta) \\ 1 & else \end{cases}$

$I_{\alpha,\beta} = \frac{1}{2} - \frac{1}{2}f(\alpha)f(\beta)f(\alpha + \beta)$

If $f(\alpha)f(\beta) = f(\alpha + \beta)$, the product is 1 for the second term, then the result is 0.

Then:

$$\Pr[\text{test reject}] = \mathbb{E}_{\alpha,\beta}[I_{\alpha,\beta}] = \frac{1}{2} - \frac{1}{2}\mathbb{E}[f(\alpha)f(\beta)f(\alpha + \beta)] \tag{9}$$

Now we write Fourier coefficients for the expectation. ■

Claim 5 $\mathbb{E}[f(\alpha)f(\beta)f(\alpha+\beta)] = \sum_{\alpha\in\mathbb{F}_n^2} \hat{f}_\alpha^3$

Proof

$$\mathbb{E}_{\alpha,\beta}[(\sum_{\alpha\in\mathbb{F}_n^2} \hat{f}_a\chi(\alpha))(\sum_b \hat{f}_b\chi_b(\beta))(\sum_c \hat{f}_c\chi_c\alpha+\beta)] \tag{10}$$

$$= \mathbb{E}_{\alpha,\beta} \sum_{abc} \hat{f}_a\hat{f}_b\hat{f}_c\chi_a(\alpha)\chi_b(\beta)\chi_c(\alpha+\beta) \tag{11}$$

$$= \sum_{abc} \hat{f}_a\hat{f}_b\hat{f}_c\mathbb{E}_{\alpha,\beta}[\chi_a(\alpha)\chi_b(\beta)\chi_c(\alpha)\chi_c(\beta)] \tag{12}$$

$$= \sum_{abc} \hat{f}_a\hat{f}_b\hat{f}_c\mathbb{E}_{\alpha,\beta}[\chi_{a+c}(\alpha)\chi_{b+c}(\beta)] \tag{13}$$

$$= \sum_{abc} \hat{f}_a\hat{f}_b\hat{f}_c(\mathbb{E}_\alpha\chi_{a+c}(\alpha))(\mathbb{E}_\beta\chi_{b+c}(\beta)) \tag{14}$$

From property:

$$\mathbb{E}_{x\in\mathbb{F}_2^n}[\chi_a(x)] = \begin{cases} 1 & if a = 0 \\ 0 & else \end{cases}$$

1 iff (a +c) = 0, 0 else, and similar for 1 iff (b+c) = 0, 0 else. Then if $a \neq c$, everything is 0, and if $b \neq c$, everything is 0. Then the surviving terms are when a=b=c, so we let all subscripts on the fs be a and finally get:

$$= \sum_a \hat{f}^3$$

■

Recall we WTS if Pr[T rejects] $< \delta$, then $d(f, \{\chi_a\}_a) < \delta$.
Substituting the summation we just made, we can rewrite:

Claim 6 *if* $\frac{1}{2}\sum_a \hat{f}_a^3 < \delta$, *then* $\frac{1}{2} - \frac{1}{2}\max_a \hat{f}_a < \delta$

Once we prove this claim, we are done.

Proof
$\max_a \hat{f}_a \geq \hat{f}_b \forall b$
Multiply both sides by $\hat{f}_b^2$:
$\max_a \hat{f}_a \sum_b \hat{f}_b^2 \geq \hat{f}_b^3$
By parsifal, sum over b term = 1:
$\max_a \hat{f}_a \geq \hat{f}_b^3$
■

0.5 Applications of Property Testing and Self Correction

Property testing comes from program verification, where we can ask things like "does the program do what it's supposed to" as "does the program have property xyz". This was the initial strategy, before the Fourier version.

Definition 7 *Self-Correction - Example*

f may be equal to a linear function "on-average". We want to recover the correct value at points whp.

- repeat and take majority vote:
- for $i = 1....s = \log \frac{1}{p}$:
  - pick y uniform random
  - compute $f(y) + f(y + \alpha) = a_n s_i$
- output $maj_i(a_n s_i)$

Claim 8 $\Pr[Alg\ output = g(\alpha)] = 1 - p$

Proof

$$\Pr_y[f(y) \neq g(y)] \leq \frac{1}{8} \tag{15}$$

$$\Pr_{y+\alpha}[f(\alpha + y) \neq g(\alpha + y)] \leq \frac{1}{8} \tag{16}$$

$$\text{By union bound:} \tag{17}$$

$$\Pr[f(y) + f(\alpha + y) \neq g(y) + g(\alpha + y)] < \frac{1}{4} \tag{18}$$

■