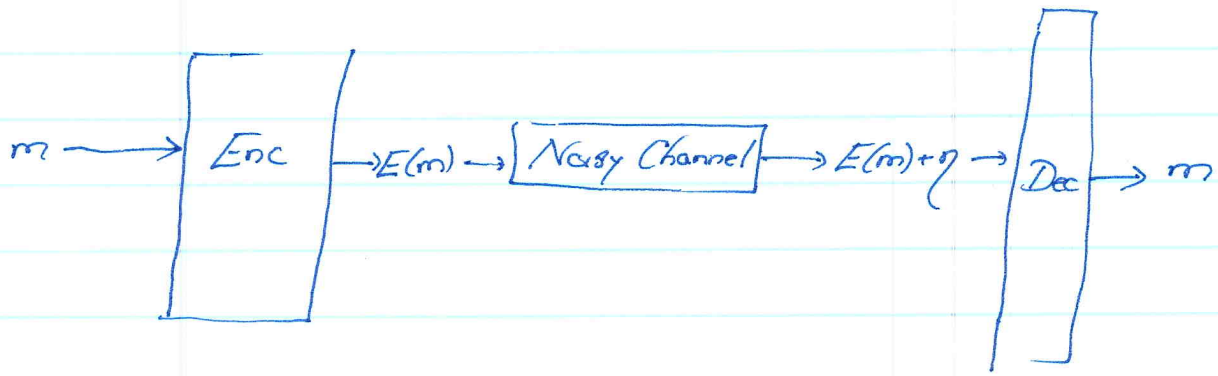
# CMSC 39600 – Lec #3 (Oct 2, 07)

**Today**

- Coding Theory – prelims
- PCP ∈ NP (poly, O(1))
  - Walsh-Hadamard Code
    - linearity testing

---

## Coding Theory




$C: \{0,1\}^k \to \{0,1\}^n$

Range $= \{C(x) \mid x \in \{0,1\}^k\}$ – set of codewords.

Hamming distance: $\Delta(x,y) = \#\{i : x_i \neq y_i\}$

fractional distance: $\delta(x,y) = \Delta(x,y)/n$

Distance of code:

$$\min_{x,y} \{\Delta(C(x), C(y))\}$$

Rate of code: $k/n$

$(n,k,d)_q$ – code; $[n,k,d]_q$ – code if linear

Distance from a code:

$$\Delta(w, C) = \min_{x} \{\Delta(w, C(x))\}$$

Unique decoding: If $\Delta(w, C) \leq d/2$, then possible

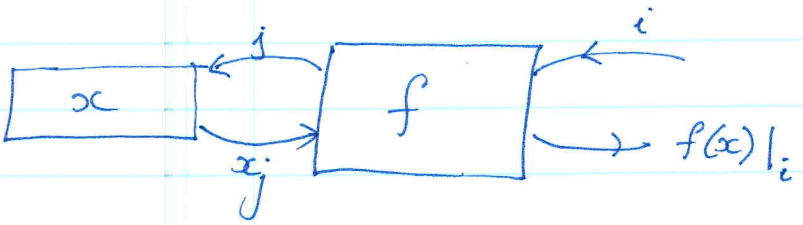
Algorithmic Questions

1. Encoding
2. Error Detection (Testing)
3. Error Correction (Decoding)

---

Sublinear time alg (for $f: \{0,1\}^k \to \{0,1\}^n$)

Not enough to read i/p
or write output.




~~Output f(x)~~ is ~~close~~ to f

~~Cannot~~ expect to do

Encoding: Not possible

Decoding: Local Decoding

Testing: Local Testing

## Walsh-Hadamard Code

$x \in \{0,1\}^k$

$f: \{0,1\}^k \to \{0,1\}$

$f$ is linear $\forall x, y$. $f(x)+f(y) = f(x+y)$

eg:

$a \in \{0,1\}^k$

$l_a : \{0,1\}^k \to \{0,1\}$

$x \longmapsto \langle a, x \rangle = \sum_{i=1}^{k} a_i x_i \pmod 2$

$\mathcal{L}_k = \{ l_a \mid a \in \{0,1\}^k \}$

Ex: $\mathcal{L}_k$ is the set of all linear functions.

## WH code

$WH: \{0,1\}^k \longrightarrow \{0,1\}^{2^k}$

$x \longmapsto l_x$

(truth table of $l_x$)

"$a^{th}$ co-ordinate" $= l_x(a) = l_a(x)$

Two interpretations:
1. Evaluation of $l_a$ at $x$
2. Evaluation of $l_x$ at $a$.

Rate - very poor $\frac{k}{2^k}$.

Distance: $\geq 2^k/2$, $\geq 1/2$.

If $x \neq y$, then $\Pr_a [ l_x(a) = l_y(a) ] = 1/2$

$l_x$ - linear

$\forall\ a, b$

$$l_x(a+b) = l_x(a) + l_x(b).$$

---

**Local Decoding:** There exists a local decoder $A$ s.t.

If $f: \{0,1\}^k \to \{0,1\}$ is $\delta$-close to HW

(i.e., $\min_a \left[ P_x \left[ f(x) \neq l_a(x) \right] \right] \leq \delta$.

then $A^f(x) = l_{a^*}(x)$ with prob $1-2\delta$

where $a^*$ is arg.min

Pf:

$$A^f(x) = f(x+r) - f(r)$$

$f(x+r) \neq l_a(x+r)$ w.p $\delta$

$f(r) \neq l_a(r)$ w.p $\delta$.

$f(x+r) \neq l_a(x+r)$ or $f(r) \neq l_a(x)$ w.p $2\delta$

With prob $\geq 1-2\delta$

$f(x+r) - f(r) = l_a(x+r) - l_a(r) = l_a(x)$

---

Local Testing of WH code:

Given $f: \{0,1\}^k \to \{0,1\}$

check if $f$ is $\begin{cases} \text{close to a WH-codeword} \\ \text{far or from WH-code} \end{cases}$

Equivalently, is $f$ close to being linear?

**Test:**

Choose $x, y \in_R \{0,1\}^k$

Accept ~~Check~~ if

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

Accept, else.

BLR Test.

---

**Thm:**

Comp: If $f$ is linear (ie, $f = l_a$ for some $a$) then BLR-Test passes w/p 1.

Sound: If $f$ is $\delta$-far from being linear, then the test rejects with probability at least $\delta$.

---

More convenient to work with $\{1,-1\}$ $\{0,1\}$

$f: \{0,1\}^n \to \{1,-1\}$

( 1 - ~~fal~~ 0 (false)
-1 - 1 (true)

$+ \to \times$ multiplication

Test.

$x, y \in_R \{0,1\}^n$

$f(x) \cdot f(y) = f(x+y)$ [Or equivalently $f(x) \cdot f(y) \cdot f(x+y) = 1$]

$f, g$ $\quad \chi_a(x) = (-1)^{\langle a,x\rangle} = (-1)^{l_a(x)}$ (linear function)

~~$\langle f,g\rangle =$~~

Properties:

$$\chi_a(x+y) = \chi_a(x)\,\chi_a(y)$$

$$\chi_{a+b}(x) = \chi_a(x)\cdot\chi_b(x)$$

---

$$\langle f,g\rangle = \mathop{\mathbb{E}}_{x\in\{0,1\}^k}[f(x)\,g(x)]$$

$$= \frac{1}{2^k}\sum_x f(x)\,g(x).$$

Properties:

$$\langle \chi_a, \chi_b\rangle = \delta_{a=b}$$

Pf: ~~$\langle \chi_a, \chi_b\rangle =$~~

$a\neq 0$, $a_i \neq 0$

$$\mathop{\mathbb{E}}_x[\chi_a(x)] = \frac{1}{2^k}\sum (-1)^{\langle a,x\rangle}$$

$$= \frac{1}{2^k}\left(\sum_{x_i=1}(-1)^{\langle a,x\rangle} + \sum_{x_i=0}(-1)^{\langle a,x\rangle}\right)$$

$$= 0.$$

$$\langle \chi_a, \chi_b\rangle = \mathop{\mathbb{E}}_x[\chi_a(x)\,\chi_b(x)] = \mathop{\mathbb{E}}_x[\chi_{a+b}(x)]$$

$$= \begin{cases} 0 & \text{if } a\neq b \\ 1 & \text{o.w.} \end{cases}$$

---

$\chi_a$ – orthonormal.

$\mathcal{F} = \{f: \{0,1\}^k \to \mathbb{R}\}$ $\qquad f+g(x) = f(x)+g(x)$

$2^k$ – dimensional space

$\chi_a$'s form an orthonormal basis for $\mathcal{F}$.

Hence, $\forall f$

$$f = \sum \hat{f}_a \chi_a \qquad \text{i.e., } f(x) = \sum \hat{f}_a \chi_a(x)$$

$$\hat{f}_a = \langle f, \chi_a \rangle = \mathop{\mathbb{E}}_x \left[ f(x) (-1)^{\langle a, x \rangle} \right]$$

$$= 1 - 2\delta(f, l_a).$$

$f = l_a$, & $\hat{f}_a = 1$

Parseval's identity.

$$\langle f, f \rangle = \sum \hat{f}_a^2$$

& (Cor: If $f$: Boolean, $\sum \hat{f}_a^2 = 1$)

---

Linearity Test

$$\Pr[\text{Test accepts}] = \Pr_{x,y} \left[ f(x) \cdot f(y) f(x+y) = 1 \right]$$

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

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

$$= \frac{1}{2} + \frac{1}{2} \mathop{\mathbb{E}}_{x,y} \left[ \sum_{a,b,c} \hat{f}_a \hat{f}_b \hat{f}_c \chi_a(x) \chi_b(y) \chi_c(x+y) \right]$$

$$= \frac{1}{2} + \frac{1}{2} \sum_{a,b,c} \hat{f}_a \hat{f}_b \hat{f}_c \mathop{\mathbb{E}}_x \left[ \chi_a(x) \chi_c(x) \right] \mathop{\mathbb{E}}_y \left[ \chi_b(y) \chi_c(y) \right]$$

$$= \frac{1}{2} + \frac{1}{2} \sum_a \hat{f}_a^3 \leq \frac{1}{2} + \frac{1}{2} \left( \max_a |\hat{f}_a| \right) \sum \hat{f}_a^2$$

$$= \frac{1}{2} + \frac{1}{2} \max_a |\hat{f}_a|$$