# Lecture 21

# TODAY

## LOCALLY DECODABLE CODES meeting Singleton Bound

1. High Rate setting : Multiplicity codes
2. General setting : " + AEL

1. [Kopparty - Saraf - Yekhanin] 2010
2. [Kopparty - Meir - RonZewi - Saraf] 2014

Locally ~~Correctible~~ Decodable Code $C \subseteq \{[n] \to \Sigma\}$ is $(\ell, \epsilon)$-LCC

if $\exists$ Decoder $D$ s.t.

$\forall\ g : [n] \to \Sigma$ s.t. $\exists\ f \in C$ with $\delta(f,g) \leq \epsilon$

$\forall\ x \in [n]$

$$\Pr\left[D^g(x) \neq f(x)\right] \leq 1/3$$

$D$ makes $\ell$ queries to $g$.

Today: $\ell(n) = n^{o(1)}$

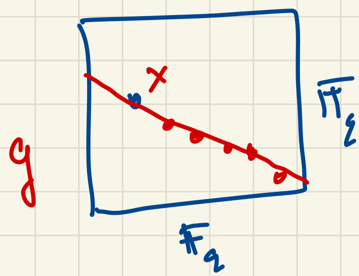
- **Focus**: $\ell = o(n)$:

- Before KSY: highest rate possible $R < \frac{1}{2}$

- Bivariate Reed Muller Codes over $\mathbb{F}_q$

- $n = q^2$ : $[n] \approx \mathbb{F}_q^2$ ; $d = (1-2\epsilon)q$
- $C = \{ f : \mathbb{F}_q^2 \to \mathbb{F}_q \mid \deg(f) \le d \}$
- $\dim(C) = \binom{d+1}{2} \approx (1-2\epsilon)^2 \cdot \frac{q^2}{2} \approx (1-\epsilon')\frac{n}{2}$
- local decoder

$\ell = q = \sqrt{n}$




---

- Summary: Rate $< \frac{1}{2}$ ; $\ell = \sqrt{n}$

- Can reduce $\ell$ with smaller rate

$$R < \frac{1}{m!} \; ; \quad \ell = n^{1/m}$$

- No ideas for improving rate!

# Multiplicity Code

**Starting Example:** Bivariate mult·2 code

- Can encode polynomial by giving its evaluations & evaluations of its derivatives.
- Specifically given $f(x,y) = \sum c_{ij} x^i y^j$

$$f_x(x,y) = \sum i\, c_{ij}\, x^{i-1} y^j$$

$$f_y(x,y) = \sum j\, c_{ij}\, x^i y^{j-1}$$

(higher order derivatives slightly diff. over finite fields ... but not order 1.)

$$\text{Encoding}(f) = \langle (f(a,b),\ f_x(a,b),\ f_y(a,b)) \rangle_{a,b \in \mathbb{F}_q}$$

Maps set of deg < d poly $\Rightarrow (\mathbb{F}_q^3)^{q^2}$

---

$\Sigma = \mathbb{F}_q^3$ ; $n = q^2$ ; $\dim k = \binom{d+1}{2} \approx \frac{d^2}{2}$

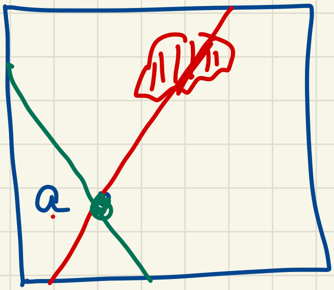
$= \frac{d^2}{6}$ elements of $\Sigma$.

what has improved? $\quad d = (1-2\epsilon)\cdot(2q)$

# Distance? $\Leftarrow$ Decoding

**Decoding:** $D^g(a)$: Pick random $b$ $(a \in \mathbb{F}_q^2)$

- $g_{a,b}(t) \triangleq g(a+tb)$




- $\deg(g_{ab}) \leq d < 2q$
- Decode how?
- key: have $g_x$ & $g_y$ also

$\Downarrow$

can compute $g'(t)$ at any point.

$\Rightarrow$ know $g$ & $g'$ at $\frac{d}{2}$ points

suffices;

can also correct $\epsilon'$-fraction errors

(Exercise: Abstract Decoding)

- Can recover $g_{a,b}(0)$ from $g_{ab}$ & $g'_{ab}$

even with $\epsilon'$-fraction corruptions.

$\Rightarrow$ can recover $f(a)$! Done?

Rate = ?

$$k = \binom{d+1}{2} \approx \frac{d^2}{2} \qquad d \approx 2q$$

$$\approx 2q^2$$

message $\in$ $\mathbb{F}_q^{2q^2} \cong \left(\Sigma\right)^{\frac{2q^2}{3}}$

$$\Sigma = \mathbb{F}_q^3 \qquad n = q^2$$

Codes of Rate $R \to \frac{2}{3}$. (beaten $\frac{1}{2}$)

——— x ———

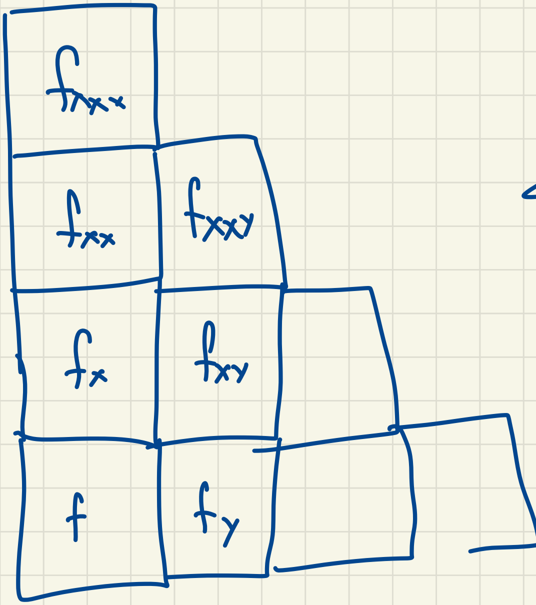
increase multiplicity:

$$(f, f_x, f_y, f_{xx}, f_{xy}, f_{yy}) \Rightarrow \Sigma = \mathbb{F}_q^6$$

$$d = 3q \Rightarrow k = \frac{9q^2}{2} \Rightarrow \Sigma^{\frac{9q^2}{12}}$$

Rate $\frac{9}{12} = \frac{3}{4}$

$\frac{\text{mult}}{m}$ .




$\binom{m+1}{2} \cdot q^2$

$\Sigma = \mathbb{F}_q^{\binom{m+1}{2}}$

$n = q^2$

$d = (m+1)q$

$m \to \infty$ $\quad R \to 1$. $\quad R = 1 - \frac{1}{m}$

~~loc~~ decodable with locality $\ell = O_m(\sqrt{n})$

---

**Better locality:** $\epsilon > 0 \Rightarrow t = \frac{1}{\epsilon}$ variables.

$\Rightarrow$ get locality $n^\epsilon$ for any const. mult. $m$.

$m = \frac{1}{\epsilon^2} \ldots \Rightarrow$ Rate $\to 1$.

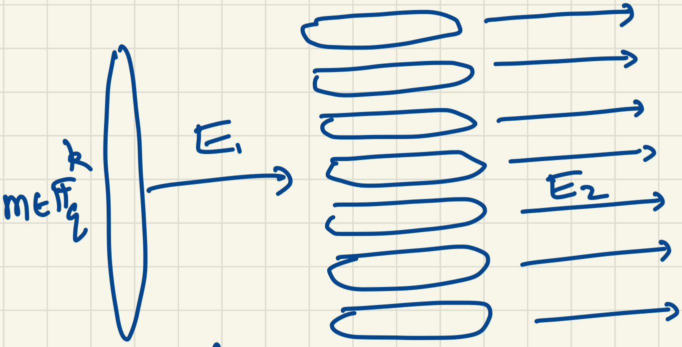
[Meir]: AEL Result/Paradigm that $R \to 1$ is everything.

<u>Next</u>: - get arbitrary rate $R$

- dist $1-R-\epsilon$
- locality $n^{o(1)}$ ; $\frac{1-R-\epsilon'}{2}$ -fraction error
- 

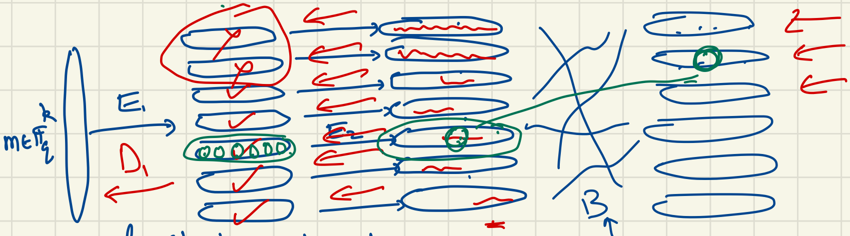
---

Tool: AEL




$E_1$ = favorite high rate codes.

= multiplicity codes. (locality $k^{o(1)}$ correcting $o(1)$-fraction error)




$\frac{1-R-\epsilon'}{2}$ fraction error

$E_1$ = favorite high rate codes.

= multiplicity codes. (locality $k^{o(1)}$ correcting $o(1)$-fraction errors)

$\epsilon$-sampler.

$E_2$ = rate $R$, distance $1-R-o(1)$.

Final Thm: Correct $\left(\frac{1-R-\epsilon}{2}\right)$-fraction errors

with locality $n^{o(1)}$ & rate $R$;

alphabet size growing with $\epsilon$,

Next Lecture: Limited Independence + Almost limited independence.