Today: · Locally decodable codes from Reed Muller codes
· Matching vector codes (overview)

Recall:

Reed Solomon codes $\quad RS_{\mathbb{F}}(k) : \mathbb{F}^k \longrightarrow \mathbb{F}^n$

$$\underbrace{(p_0, p_1, \ldots p_{k-1})}_{\text{msg}} \longrightarrow \underbrace{\langle p(\alpha_1), p(\alpha_2) \ldots p(\alpha_n) \rangle}_{\text{codeword.}}$$

$\alpha_1, \ldots \alpha_n \in \mathbb{F}$

$$p(x) = \sum p_i x^i$$

Reed Muller codes $\quad RM(m, \ell)$

$$RM(m,\ell) = \left\{ \langle p(\alpha) \rangle_{\alpha \in \mathbb{F}^m} \;\middle|\; p \in \mathbb{F}[x_1 \ldots x_m] \right.$$
$$\left. \deg p \leq \ell \right\}.$$

$$(p_{0000}, \ldots, p_{LLL\ldots L}) \longrightarrow \langle p(\alpha_1), p(\alpha_2), \ldots p(\alpha_{|\mathbb{F}|^m}) \rangle$$

↑ msg is coefficients of monomials in $x_1, x_2, \ldots x_m$

$$K = \binom{m+\ell}{m} = \binom{m+\ell}{\ell} \quad \text{(msg size)}$$

$$n = |F|^m \quad \text{(codeword size: evaluate msg poly over entire domain)}$$

rel. distance : $1 - \ell / |F|$

(by Schwartz-Zippel)

<u>Local decoding for RM</u>:

Alg: on a f st $\text{dist}(f, g) \le \delta$ for some $g \in RM$

goal: output $g(a)$. $(a \in \mathbb{F}^m)$

1. pick random line passing through $\underline{a}$

(i.e. pick $b \xleftarrow{u.a.r.} \mathbb{F}^m / \{0\}$

and consider elts $L_{a,b} = \{ a + bt \mid t \in \mathbb{F} \}$

Query $f(a + b\alpha_1), f(a + b\alpha_2), \ldots, f(a + b\alpha_{\ell+1})$

for some distinct $\alpha_1, \alpha_2, \ldots \alpha_{\ell+1} \in \mathbb{F}$

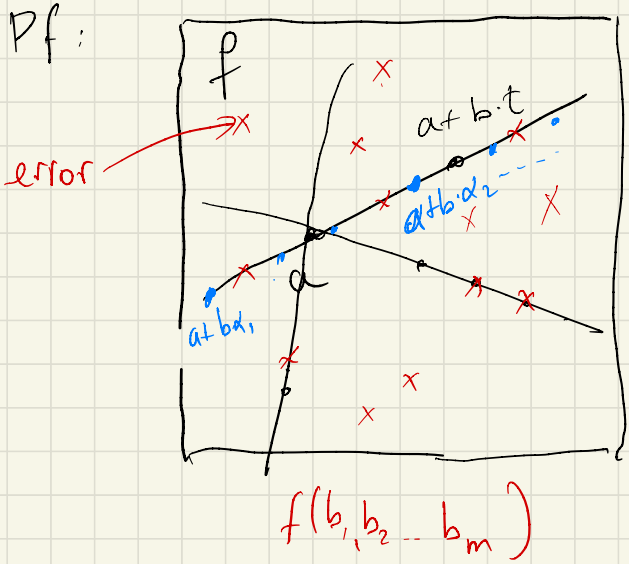
2. Interpolate the values of $f(a+b\alpha_i)$ to obtain a unique ℓ-degree poly $\underline{G}$ that agrees with $f(L(\alpha_i))$ for every $i \in [\ell+1]$.

3. Output $\underline{G(0)}$. $\left(= \underline{g(0)} \simeq \underline{f(0)} \right)$

supposed to be

Thm: $RM(\ell, m)$ is a $\left(\ell+1, \underbrace{1/3(\ell+1)}_{\delta}, \underbrace{1/3}_{\varepsilon}\right)$-LDC.

Pf:



$\mathbb{F}^m$

Obs:

It may be that

$f(a) \neq g(a)$

the codew. we care abt.

So we "vote" for a via restrictions to random lines

<u>Claim 1</u>: For fixed $a \in \mathbb{F}^m$, $\alpha \in \mathbb{F}^*$ and for b picked u.a.r from $\mathbb{F}^m / \{0\}$. the elt $a + \alpha b$ is u.a.r in $\mathbb{F}^m$

<u>Claim 2</u>: For $g : \mathbb{F}^m \to \mathbb{F}$ of deg ℓ restriction of f to line $L_{a,b} : \mathbb{F}_q \to \mathbb{F}_q$

with $g_{L_{ab}}(t) = f(L_{a,b}(t)) = f(a + bt)$

is a poly in 1 var of deg $\leq \ell$.

Eg: $p(x_1, x_2) = x_1^2 x_2 + x_2^3 + 1$, $a = (5,1)$, $b = (4,3)$

$$L_{a,b} = \{ (5,1) + t(4,3) \}_{t \in \mathbb{F}}$$

$$p \circ L_{ab}(t) = p(5 + 4t, 1 + 3t)$$

$$= (5+4t)^2 (1+3t) + (1+3t)^3 + 1$$

↑ · deg ≤ 3

· 1 variate poly.

<u>Claim 3</u>: Given values of a deg ℓ poly g at $\ell+1$ pts can interpolate to find g explicitly (of deg ℓ). This is unique.

$\rightarrow$ deg $k-1$ poly that passes throug $f(\alpha_1)\ f(\alpha_2) \ldots f(\alpha_k)$

$\forall\ a,\ \alpha_i$ if b is nar in $\mathbb{F}^m / \{0\}$

then $\Pr\left[f(a+\alpha_i b) \neq g(a+\alpha_i b) \right] \leq \delta = \frac{1}{3(\ell+1)}$

So by union bound,

for all $\alpha_0 \ldots \alpha_\ell$ $\quad f(a+\alpha_i b) = g(a+\alpha_i b)$

wp $1 - (\ell+1) \cdot \frac{1}{3(\ell+1)} = 2/3$.

So when all the $f(a+\alpha_i b)$ are correct

then the interpolating poly G that

passes through $\{f(a+\alpha_i b)\}_{i\in\{0,\dots,\ell\}}$

is exactly the restriction of g to $L_{a,b}$.
(by uniqueness)

Then $G(0) = g(a+0\cdot b) = g(a)$ ✓

wp $2/3$.

Parameters : #queries $= \ell+1 = \Theta(1)$

$|\mathbb{F}| =$ constant $= O(1)$

$\ell = |\mathbb{F}| - 2 = O(1)$

$n = |\mathbb{F}|^m \qquad k = \binom{m+\ell}{m}$

$\Rightarrow n = 2^{O(k^{1/|\mathbb{F}|-2})}$

lb : $n > k^{1+O(1/\ell)}$

exp. gap

Issue: $\delta \to 0$ as $\deg \ell \to \infty$

$$\delta = \frac{1}{3(\ell+1)}$$

Can we get $\delta = \frac{1}{100}$?

New tool:

Berlekamp-Welch: Unique decoding of $RS(\ell)$

Given received vector $\langle r_1 \ldots r_n \rangle$ that is within $\frac{1}{2}(n-\ell)$ from a $RS(\ell)$ codeword c find c in $\text{poly}(n, \log|\mathbb{F}|)$ time.

We'll use above as black-box to get LDC for $\delta = 1/100$

independent of $\deg \ell$!

LDC Alg: Given access to $f: \mathbb{F}^m \to \mathbb{F}$, and $a \in \mathbb{F}^m$; find $g(a)$ (where $\mathrm{dist}(f,g) \le \delta$, $g \in RM(\ell)$)

1. Pick a rand line through a.

   Query every $f(a+bt)$, $t \in \mathbb{F}^*$

   let H be the $|\mathbb{F}|$-length vector collecting these values.

   H is the received vector from Berlekamp Welch because $g(a+bt)$ is a $RS(\ell)$ codeword.

2. Decode H to a $RS(\ell)$ codeword G using Berlekamp Welch

3. Output $G(0)$

Thm: $RM_{\mathbb{F}}(m, \ell)$ is a

$$\left(|\mathbb{F}|, \underset{\delta}{\frac{1}{100}}, \underset{\varepsilon}{1/20} \right) \text{-LDC}$$

Pf: $\Pr_t\left[f(a+bt) \neq g(a+bt) \right] \leq 1/100$

So $\mathbb{E}_{a,b}\left[\#\text{ of errors on } f \circ L_{a,b} \right] \leq \frac{|\mathbb{F}|}{100}$

By Markov $\Pr_{a,b}\left[\#\text{ of errors on } f \circ L_{a,b} \geq \underbrace{20 \cdot \mathbb{E}[\ ]}_{= |\mathbb{F}|/5} \right] < \frac{1}{20}$

So wp $\frac{19}{20}$ $f \circ L_{ab}$ has $\leq |\mathbb{F}|/5$ error

Pick $\ell = |\mathbb{F}|/2$. Then BW decodes from $\frac{|\mathbb{F}|}{4}$ error

So in particular BW can decode (uniquely) from $\frac{|\mathbb{F}|}{5}$ error. Let G be the decoded poly.

By uniqueness, we must have $G(t) = g(a+bt), \forall t$.

So when decoding succeeds, the unique poly $g \circ L$ is output, hence

$$g(a) = g(a + 0 \cdot b) = G(0)$$ (supposed to equal $f(a)$)

Parameters: $m = \Theta(1)$ vars.

$|\mathbb{F}| = n^{1/m}$ $\quad d = |\mathbb{F}|/2$

$$k \approx \frac{\ell^m}{m!} \; ; \quad \text{rate} = k/n = \frac{1}{m!\,2^m} = \Theta(1)$$

queries: $|\mathbb{F}| - 1 = n^{1/m} \ll n$

(sublinear query complexity)

Better LDCs from families of Matching Vectors.

(high-level ideas)

Let $S \subseteq \mathbb{Z}_m$

Then vectors $u_1, v_1, u_2, v_2 \ldots u_k\ v_k$ are S-matching (S-MVF)

if $\begin{cases} \langle u_i, v_j \rangle = 0 & \text{if } i = j \\ \langle u_i, v_j \rangle \in S & \text{if } i \neq j \end{cases}$

Let $\mathbb{F}$ be a field. Let w be primitive root, so

$w^m = 1$ (primitive roots of unity in $\mathbb{F}$)

Eg: over $\mathbb{C}$ $\quad w = e^{2k\pi i/m} \quad k \in \{0, \ldots m-1\}$.

$= \cos \frac{2k\pi}{m} + i \sin 2k\pi/m$.

Such roots can be defined in every field.

Def: $\chi_i : \mathbb{Z}_m^n \to \mathbb{F}$

$$x \longrightarrow \omega^{\langle x, u_i \rangle}$$

For msg $c \in \mathbb{F}^k$ encode it using

$$g : \mathbb{Z}_m^k \to \mathbb{F}$$

$$g(x) = \sum_{i=1}^{k} c_i \chi_i(x)$$

<u>Local decoding</u>: Given oracle access to f, to find c_j

- pick x u.a.r. $\mathbb{Z}_m^n$
- query $f(x), f(x+v_j), f(x+2v_j) \ldots f(x+(m-1)v_j)$

  (i.e. a line through x of slope v_j)

...

Can solve lin system for c_j...

Thm (Yekhanin, Efremenko)

If S-MVF over $\mathbb{Z}_m^d$ of size k

then $\exists$ a $(r, \delta, 1-r\delta)$ LDC

$$C : \mathbb{F}^k \to \mathbb{F}^n, \quad n = m^d \quad r = |S|+1$$

(assuming $m \mid |\mathbb{F}|-1$)

Thm (Grolmusz '99) Let $m = p_1 p_2 \cdots p_t$ dist primes.

Then $\exists$ an explicit S-MVF in $\mathbb{Z}_m^d$ of size

$$\exp\left(\Omega\left(\frac{(\log d)^t}{(\log\log d)^{t-1}}\right)\right)$$ for sets of size $2^t - 1$.

<u>Imply</u>: 4-query LDC of length

$$n = \exp\left(\exp\left(\sqrt{\log k \log\log k}\right)\right) = \exp(k^{o(1)})$$

subexp!!!

(RM can give 4-query LDC with $n = \exp(k^{1/3})$