Today: Locally decodable codes from Reed-Muller codes.

Matching vector codes (overview)

Recall:

Reed Solomon codes

\[ RS_{\mathbb{F}}(k) : \mathbb{F}^k \rightarrow \mathbb{F}^n \]
\[ (p_0, p_1, \ldots, p_{k-1}) \rightarrow \langle p(x_1), p(x_2), \ldots, p(x_n) \rangle \]
\[ x_1, \ldots, x_n \in \mathbb{F} \]

\[ p(x) = \sum p_i x^i \]

Reed Muller codes

\[ RM(m, l) \]
\[ RM(m, l) = \langle \langle p(x) \rangle \rangle \quad | \quad \forall p \in \mathbb{F}[X_1, \ldots, X_m] \]
\[ \deg p \leq l \}

\[ (p_{0000}, \ldots, p_{1111}) \rightarrow \langle p(x_1), p(x_2), \ldots, p(x_m) \rangle \]
\[ \uparrow \text{msg} \]
\[ \text{coefficients of monomials in } X_1, X_2, \ldots, X_m \]
\[ k = \binom{m+e}{m} = \binom{m+e}{e} \quad (\text{msg size}) \]

\[ n = \left| \mathbb{F} \right|^m \quad (\text{codeword size}) \]

rel. distance : \[ 1 - \frac{e}{\left| \mathbb{F} \right|} \]

(by Schwartz-Zippel)

**Local decoding for RM**

**Alg:** on a set \( \text{dist} (f, g) \leq 5 \) for some \( g \in \text{RM} \)

- goal: output \( g(a) \). (\( a \in \#^m \))

1. pick random line passing through a \( \epsilon \)
   (i.e. pick \( b \in \mathbb{F}^m \setminus \{0\} \)
   and consider elts \( L_{a,b} = g + b + t \cdot \)
   \( t \in \mathbb{F} \)

Query \( f(\alpha + b \alpha_i), f(\alpha + b \alpha_2), \ldots, f(\alpha + b \alpha_{e+1}) \)

for some distinct \( \alpha_1, \alpha_2, \ldots, \alpha_{e+1} \in \mathbb{F} \)
2. Interpolate the values of \( f(a + b\alpha_i) \) to obtain a unique \( \ell \)-degree poly \( G \) that agrees with \( f(L(\alpha_i)) \) for every \( i \in \mathbb{N} \).

3. Output \( G(0) \): \( \left( e_i = g(0) \approx f(0) \right) \) supposed to be thin:

\[ \text{Thm: } RM(l, m) \text{ is a } \left( l + 1, \frac{1}{3(l+1)}, \frac{1}{3} \right) \text{-LDC.} \]

\[ \text{Pf: } \]

\[ \text{Obs: } \]

It may be that \( f(a) \neq g(a) \) in the coding, we care abt.

So we "vote" for a via restrictions to random lines.
Claim 1: For fixed $a \neq \mathbb{F}^n$, $L \in \mathbb{F}^n$
and for $b$ picked u.a.r from $\mathbb{F}^n / \mathbb{F}_3$.
The elt $a + \lambda b$ is u.a.r in $\mathbb{F}^n$.

Claim 2: For $g : \mathbb{F}^n \to \mathbb{F}$ of deg $\leq l$.
restriction of $f$ to line $L_{a,b} : \mathbb{F}^2 \to \mathbb{F}$
with $g(t) = f(L_{a,b}(t)) = f(a + b t)$
is a poly in 1 var of deg $\leq l$.

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

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

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

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

$\uparrow$ deg $\leq 3$

\text{1 univariate poly.}
Claim 3: Given values of a deg $l$ poly $g$ at $l+1$ pts can interpolate to find $g$ explicitly (of deg $l$). This is unique.

\[ a_1, a_2, \ldots, a_n \rightarrow \text{deg } k-1 \text{ poly that passes through } f(a_1), f(a_2), \ldots, f(a_n) \]

\[ \forall a, \alpha_i \text{ if } b \text{ is i.i.d. in } \mathbb{F}_m \text{ then } \Pr \left[ f(a + \alpha_i b) \neq g(a + \alpha_i b) \right] \leq \delta = \frac{1}{3(l+1)} \]

So by union bound, for all $\alpha_0, \ldots, \alpha_k$ \[ f(a + \alpha_i b) = g(a + \alpha_i b) \]

wp $1 - (l+1) \cdot \frac{1}{3(l+1)} = \frac{2}{3}$
So when all the \( f(a + x_i b) \) are correct
then the interpolating poly \( G \) that
passes through \( \{ f(a + x_i b) \} \) \( i \in 30, \ldots, 43 \)
is exactly the restriction of \( g \) to \( L_{a,b} \).
(by uniqueness)

Then \( G(a) = g(a + 0, b) = g(a) \lor wp \ 2/3 \).

Parameters: \#queries = \( l + 1 = \Theta(n) \)
\( l \) = \( |F| - 2 = O(1) \)
\( n = |F|^m \) \( k = \binom{m + \ell}{m} \)
\( n \equiv \Theta(k^{1/(\ell - 2)}) \)
\( b : n > k^{1+o(1/\ell)} \) \{ exp. gap \}
Issue: $\delta \to 0$ as $\deg l \to \infty$

\[
\delta = \frac{1}{3(l+1)}
\]

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

New tool:

Berlekamp-Welch: Unique decoding of RS(\textcolor{red}{l})

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

\[\text{We'll use above as black box to get LDC for } \delta = \frac{1}{100} \]

independent of $\deg l$!
LDCAlg: Given access to $f: \mathbb{F}^m \to \mathbb{F}$, and $a \in \mathbb{F}^m$; find $g(a)$ (where $\text{dist}(f,g) \leq \delta$).

1. Pick a random line through $a$.
   
   Query every $f(a + bt)$ for $t \in \mathbb{F}^n$.

   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 $\text{RS}(\mathbb{F}^e)$ codeword.

2. Decode $H$ to a $\text{RS}(\mathbb{F}^e)$ codeword $G$ using Berlekamp-Welch.

3. Output $G(0)$.
Thm: RM(m, l) is a F
\[ (|F|, \frac{1}{100}, \frac{1}{20}) \text{-LDC} \]
\[ \delta \leq 3 \]

Pf: \[ \Pr[ f(a+bt) \neq g(a+bt)] \leq \frac{1}{100} \]

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

By Markov \[ \Pr[ \text{# of errors on } f \circ L_{ab} > 20 \cdot \mathbb{E} ] < \frac{1}{20} \]
\[ \frac{|F|}{5} \]

So wp \[ \frac{19}{20} \]
\[ f \circ L_{ab} \] has \[ \leq \frac{|F|}{5} \] error

Pick \[ l = \frac{|F|}{2} \]. Then BW decodes from \[ \frac{|F|}{4} \] error
So, in particular, BW can decode (uniquely) from \( \frac{IFL}{5} \) 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 \( g \odot L \) is output, hence

\[
g(a) = g(a+0 \cdot b) = G(0) \quad \text{(Supposed to equal } f(a))
\]

---

**Parameters:**

- \( m = \Theta(n) \) vars.
- \( |IFL| = n^{1/m} \)
- \( d = \frac{|IFL|}{2} \)
- \( k = \frac{m^n}{m!} \)
- \( \text{rate} = \frac{k}{n} = \frac{1}{m! 2^m} = \Theta(1) \)
- \( |IFL|-1 = n^{1/m} \ll n \quad \text{(sublinear query complexity)} \)
Better LDCs from families of Matching Vectors.

(Thigh-level ideas)

Let $S \triangleq \mathbb{Z}/m$

Then vectors $u_1, u_2, \ldots, u_k$ are $S$-matching

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

Let $F$ be a field. Let $w$ be primitive root, so

\[w^m = 1 \quad \text{(primitive roots of unity in } F)\]

Eg: over $\mathbb{C}$

\[w = \frac{2k\bar{\omega}}{m} \quad \kappa \in \{0, \ldots, m-1\}\]

\[= \cos \frac{2k\bar{\omega}}{m} + i \sin \frac{2k\bar{\omega}}{m}.
\]

Such roots can be defined in every field.

Def: \( X_i : \mathbb{Z}_m^n \rightarrow \mathbb{F} \)
\[ X \rightarrow \langle x, u_i \rangle \]

For msg \( c \in \mathbb{F}^k \) encode it using
\[ g : \mathbb{Z}_m^k \rightarrow \mathbb{F} \]
\[ g(x) = \sum_{i=1}^{k} c_i X_i(x) \]

Local decoding: 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 \( c_j \)...
Thin (Yekhanin, Efremenko)

If $S$-MVF over $Z_m^d$ of size $k$

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

$C : \#k \to \mathbb{F}_m^n$, $n = m^d$, $r = \lfloor s \rfloor + 1$

(assuming $m \mid 1/\delta - 1$)

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

Then $\exists$ an explicit $S$-MVF in $Z_m^d$ of size

$$\exp \left( \frac{(\log d)^{t^3}}{\log \log d^{t^3}} \right)$$

for sets of size $2^{t-1}$.

Imply: 4-query LDC of length

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

$\Rightarrow$ subexp!!!

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