Today

- Decoding the Reed-Muller Code.

CSS.318.1
Coding Theory
Lecture 18 (2022-11-2)
Instructor: Prahladh Harsha.

Reed-Muller code

- $\mathbb{F}$ - finite field of size q
- m - ambient dimension
- r - degree

$$RM_q(m,r) = \left\{ Eval(p)\big|_{\mathbb{F}^m} \;/\; p \in \mathbb{F}_{\le r}[X_1, X_2 \ldots, X_m] \right\}$$

General version: Eval on a product set S^m

Today: $S = \mathbb{F}^m$

Block length = $|\mathbb{F}^m| = q^m$

Dimension: $k_q(m,r) = \left| \left\{ (e_1, e_2, \ldots, e_m) \;/\; 0 \le e_i \le q-1,\ e_i \in \mathbb{Z},\ \sum e_i \le r \right\} \right|$

($r < q$: $k_q(m,r) = \binom{m+r}{r}$

$q = 2$: $k_2(m,r) = \binom{m}{\le r}$)

Distance: Schwartz-Zippel Lemma.

SZ Lemma: $p \in \mathbb{F}_{\le r}[X_1 \dots X_m]$; $p \neq 0$

$$\Pr_{\alpha \leftarrow \mathbb{F}^m}[p(\alpha) \neq 0] \ge \frac{1}{q^a}\left(1 - \frac{b}{q}\right)$$ where

$r = (q-1)a + b$

$\Rightarrow 0 \le b < q-1$.

$$\delta_q(m, r) = \frac{1}{q^a}\left(1 - \frac{b}{q}\right)$$

$$\Delta_q(m, r) = (q-b)\, q^{m-a-1}$$

Decoding Problem: Given $f : \mathbb{F}^m \to \mathbb{F}$ & error parameter e find all poly $p \in \mathbb{F}_{\le r}[X_1 \dots X_m]$ s.t. $\Delta(f, p) \le e$.

Unique Decoding : $e < \Delta_q(m, r)/2$.

Today : 3 Algorithms

Local { (1) Reed's Majority Decoder ($q = 2$)
(2) Local Unique Decoder ($e < \Delta_q(m, r)/2$)

Global. { (3) Reduction to Reed-Solomon code [Pellikaan-Wu]

—

I Reed's Majority Decoder for $RM_2(m, r)$

$$\Delta_2(m, r) = 2^{m-r}$$

Unique Decoder: Recovers p if $\varepsilon < \Delta_2(m,k)/2$.

$$p(x_1 \dots x_m) = \sum_{\substack{S : S \subseteq [m] \\ |S| \le k}} p_S \underbrace{\prod_{i \in S} x_i}_{x^S} = \sum_{\substack{S : S \subseteq [m] \\ |S| \le k}} p_S x^S$$

Fact: $\sum_{a \in \mathbb{F}_2^m} x^S(a) = \begin{cases} 1 & \text{if } S = [m] \\ 0 & \text{otherwise.} \end{cases}$

Proposition: $p \in \mathbb{F}_{\le k}[x_1 \dots x_m]$; $S \subseteq [m]$; $|S| = k$

$b \in \mathbb{F}_2^{m-k}$

$$\sum_{a \in \mathbb{F}_2^m : a|_{\bar{S}} = b} P(a) = p_S$$

Pf: Define $p_b \in \mathbb{F}_{\le k}[x_1 \dots x_k]$

$$p^b(a) = P(S \leftarrow a ; \bar{S} \leftarrow b)$$

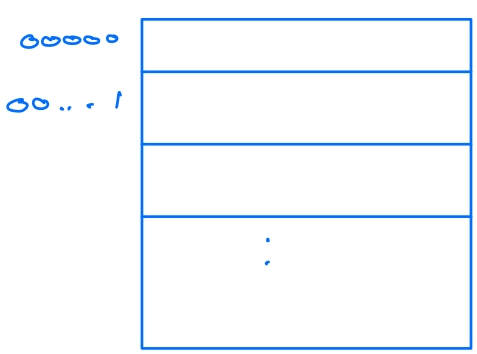
$$P(x) = \sum_{T \subseteq [m] : T \le k} p_T x^T$$

$$p^b(x) = p_S x^S + \sum_{T : T \subseteq S} x^T \sum_{\substack{U : U \in [m] \\ |U| \le k \\ U \cap S = T}} p_U b^{U \setminus T}$$

$$= p_S x^S + \sum_{\substack{T : T \subseteq S \\ |T| < k}} x^T c_T$$

$$\sum_{a \in \mathbb{F}_2^m : a|_{\bar{S}} = b} P(a) = \sum_{a \in \mathbb{F}_2^k} p^b(a) = p_S$$

$\square$



P_S can be extracted from the subcube

$S^b = \{(S \leftarrow a; \bar{S} \leftarrow b) \mid a \in \mathbb{F}_2^r\}$ for any $b \in \mathbb{F}_2^{m-r}$

Since $e < 2^{m-r}/2$, at most $e < 2^{m-r-1}$ subcubes can have errors.

Hence, a majority of the subcubes are correct.

Can extract all the deg r coefficients exactly using above method.

Share the homogenous deg r component from the recd word f and proceed.

Reed's Majority Decoder:

Given: $f: \mathbb{F}_2^m \to \mathbb{F}_2$ s.t $\exists\ p \in \mathbb{F}_2[x_1 .. x_m]$

$\Delta(f, p) = e < 2^{m-r}/2$.

Algorithm:

1. Set $t \leftarrow r$

   $f_t \leftarrow f$

   $p \leftarrow 0$

2. While $t \geq 0$ do

   (a) For each $S \subseteq [m]$ such that $|S| = t$

$$\left\{ \text{Set } P_S \leftarrow \underset{b \in \mathbb{F}_2^{m-t}}{\text{majority}} \left\{ \sum_{a \in \mathbb{F}_2^m : a|_S = b} f_t(a) \right\} \right.$$

$$\left. \text{Set } P \leftarrow P + P_S X^S \right.$$

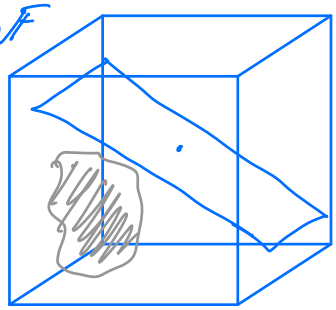
(b) $t \leftarrow t-1$

(c) $f_t \leftarrow f_{t+1} - \sum_{S : |S| = t+1} P_S X^S$

3. Output P.

II Algorithm for all fields $\mathbb{F}_q$.

$f : \mathbb{F}_q^m \to \mathbb{F}$



$\mathbb{F}_q^m$

$\Delta(f,P) \le e < \frac{1}{3} q^{m-s} \ll \Delta_q(m)/2$

$z \in \mathbb{F}_q^m$

Idea: Look at the restriction of the $f(P)$ on a random affine subspace A of dim s containing the point z.

Distribution of pts in $A \setminus z$ for random A is the uniform dist over $\mathbb{F}_q^m \setminus \{z\}$

$- \Pr_A [\exists \text{ an erroneous pt in } A \setminus \{z\}] \le (q^s - 1) \frac{e}{q^m}$

$< e / q^{m-s} < 1/3$

· (δ - small enough, then this error is small.)

- We also need 2 different poly of deg $\leq r$ have distance at least 2 over $\mathbb{F}_2^s$.

This is true provided

$$r < s(q-1).$$

Prop: $P_1, P_2 \in \mathbb{F}_{\leq r}[X_1 \dots X_s]$, $P_1 \neq P_2$ & $r < s(q-1)$

$$\Delta(P_1, P_2) \geq 2.$$

Hence, we choose $s = \left\lceil \frac{r+1}{q-1} \right\rceil$

Local Decoder.

Input $\begin{cases} f: \mathbb{F}_q^m \to \mathbb{F}, \ \exists\, p \cdot \Delta(f,p) < \frac{1}{3} q^{m-s}. \text{ where } s = \left\lceil \frac{r+1}{q-1} \right\rceil \\ z \in \mathbb{F}_q^m \end{cases}$

Algorithm: Pick a random affine subspace A of dim s that contains z.
Read $f|_A$, interpolate to obtain $p(z)$.

Remarks on #errors handled:

$r = a(q-1) + b$. $\quad \Delta_q(m, r) = (q-b)q^{m-a-1}$

$b = \left\lceil \frac{r+1}{q-1} \right\rceil$; $\quad r < b(q-1)$

$r = b(q-1) - t$

where $1 \le t < q-1$

$\Delta_q(m, r) = (t+1)\, q^{m-b}$

#errors handled: $\frac{q^{m-b}}{3} \in \left[\frac{\Delta_q(m,r)}{3q},\ \frac{\Delta_q(m,r)}{3} \right]$

III Reduction to Reed-Solomon code.

[Pellikaan-Wu '04]

Isomorphism

$\mathbb{F}_q^m \longleftrightarrow \mathbb{F}_{q^m}$

$\left(Tr(\eta_1 z), Tr(\eta_2 z), \ldots, Tr(\eta_m z)\right) \longleftrightarrow z$

$Tr : \mathbb{F}_{q^m} \to \mathbb{F}_q$

$z \mapsto z + z^q + z^{q^2} + \ldots + z^{q^{m-1}}$

$\eta_1, \eta_2, \ldots \eta_m$ – $\mathbb{F}_q$-independent elements in $\mathbb{F}_{q^m}$

RM

$p \in \mathbb{F}_{\le r}[x_1, \ldots x_m]$ $\qquad \tilde{p}(z) = p\left(Tr(\eta_1 z), \ldots Tr(\eta_m z)\right)$

Special Cases:

1. $r < q$: $\deg(\tilde{p}) = r q^{m-1} < q^m$ (since $r < q$)

$$\text{Eval}(\tilde{p}) \in \underbrace{RS_{\mathbb{F}_{q^m}}\left[\mathbb{F}_{q^m}, r q^{m-1}\right]}_{\text{distance} = 1 - \frac{r}{q} = \text{distance of RM code.}}$$

$$RM_q(m, r) \subseteq RS_{\mathbb{F}_q^m}\left[\mathbb{F}_{q^m}, r q^{m-1}\right]$$

Furthermore, the distance is the same.

2. $q = 2$. $\tilde{p}(z) \triangleq p\left(\text{Tr}(\eta_1 z), \text{Tr}(\eta_2 z), \ldots, \text{Tr}(\eta_m z)\right)$ $\pmod{z^{2^m} - z}$

Any monomial of $\tilde{p}$ before reduction by mod $z^{2^m} - z$ is of the form $z^{2^{i_1} + 2^{i_2} + \ldots + 2^{i_k}}$; $k \le r$, $0 \le i_j \le m-1$

On reduction by mod $z^{2^m} - z$ each such monomial becomes of the form $z^{2^{j_1} + 2^{j_2} + \ldots + 2^{j_\ell}}$ where $\ell \le r$, $j_1 \ldots j_\ell$ are distinct, $0 \le j_i \le m-1$

Hence $\deg(\tilde{p}) \leq 2^{m-1} + 2^{m-2} + \dots + 2^{m-r}$

$= (2^m - 1) - (2^{m-r} - 1)$

$= 2^m - 2^{m-r}$

In this case also

$$RM_2(m,r) \subseteq RS_{\mathbb{F}_{2^m}}\left[\mathbb{F}_{2^m}, 2^m - 2^{m-r}\right]$$

distance are the same.

In fact, more generally

$$RM_q(m,r) \subseteq RS_{\mathbb{F}_{q^m}}\left[\mathbb{F}_{q^m}, q^m - \Delta_q(m,r)\right]$$

$q = 2$.

$RS_{\mathbb{F}_{q^m}}[\mathbb{F}_{q^m}] \supseteq$ BCH $\supseteq RM_q(m,r)$