Problem IX.1 FLAG-TD 05-09-23

C, a linear code

$C_3 = \{(w, w, w) \in \mathbb{F}_2^{192} \mid w \in \mathbb{F}_2^{64}\}$

$k = 64, \quad n = 192$

$d_{min}(C_3)$

simplest w would be, $w = 0 \ldots 1$.

$\mathcal{E}(k) = (0, \ldots, 1, 0 \ldots 1, 0 \ldots 1)$

$\text{height}(\mathcal{E}(w)) = 3$.

$d_{min}(C_3) = 3 \leq 129$ $\quad \forall C, \ d_{min}(C) \leq n - k + 1$.

rate $\frac{k}{n} = \frac{1}{3}$.

reciene r,

encoded word $c = \mathcal{E}(w)$

hweight ~~height~~ $(r - c)$ is minimal. $\rightarrow$ maximum likelihood decoding

let $r = (\overbrace{0 \ldots 0}^{\bar{w}_1}, \overbrace{0 \ldots 1}^{\bar{w}_2}, \overbrace{0 \ldots 1}^{\bar{w}_2})$

if we know $\underset{\text{error}}{e} \leq 1$, we can easily obtain the correct code by majority vote.

~~if $r \leq 2$~~

if $e \leq 2$, not sure which is correct code. either $\bar{w}_1$ and $\bar{w}_2$ can be correct.

So, maximum likelihood decoding only works if $e \leq \left\lfloor \frac{d_{min}}{2} \right\rfloor$

Reed - Solomon codes

$k \le n \le q$

k : length of word
n : dimention.

Choose $(X_1, \dots, X_n) \in \mathbb{F}_q^n$ distinct points.

vector
le $\underline{W} = (w_0, \dots, w_{k-1}) \in \mathbb{F}_q^k$

$W = \sum_{i=0}^{k-1} w_i X^i \in \mathbb{F}_q[X]$

$\mathcal{E}(W) = (W(X_1), \dots, W(X_n)) \in \mathbb{F}_q^n$

$(\mathbb{F}_q, n, k, \underline{X})$

$RS_{\mathbb{F}_q, n, k, \underline{X}} = \{ \mathcal{E}(\underline{W}), W \in \mathbb{F}_q^k \}$.

1. it define the sub-vector space dimention of k embeded in vector space dimention n.

$d_{min}(RS) = d = n-k+1$

$deg(W) = k-1. \rightarrow$ at most $k-1$ root.

$\tilde{W}$: word that maximzes zeros in $\mathcal{E}(\tilde{W})$

hweight
~~height~~ $(\mathcal{E}(\tilde{W})) = n-(k-1) = n-k+1$.

$d_{min}(RS) = n-k+1$

$X_1, \dots, X_{k-1}$ roots of $\tilde{W}$

$\bar{e} = \left\lfloor \frac{\dim(RS)}{2} \right\rfloor$

$\mathcal{E}(W) = (0, - 0, W(X_k), -, W(X_n))$.

FLAG-TD 05-09-23

$\underline{w} \in \mathbb{F}_q^k$, word.

$C = \mathcal{E}(w) = (w(x_1), \ldots, w(x_n)) \in \mathbb{F}_q^n$

$\underline{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.

$e \leq \bar{e}$: bound on # errors

$|\{i \mid w(x_i) \neq y_i\}| \leq \bar{e}$

$y = c \rightarrow O(M(k) \log(k))$ using fast polynomial interpolation.

$e = 1$.

$P(x_i) = y_i$: true for all $i \in \{1, \ldots, n\}$, except i.

error is in y_1 ...

interpolate using $(y_2, \ldots, y_n)$.

$P(x)$, $\deg(P(x)) = n-2$.

worst case, $\rightsquigarrow O(n\, M(k) \log(k).)$ $\rightarrow$ perform fast interpolation n times.

if $e = 2$ $\rightsquigarrow O(n^2\, M(k) \log(k))$

$$\bar{e} \le \left\lfloor \frac{d_{min}}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor.$$

- error - locator polynomial.

$$\Lambda(x) = \prod_{i \mid y_i \ne w(x_i)} (X - x_i)$$

- master polynomial.

$$\cdot\ G(X) = \prod_{1 \le i \le n} (X - x_i)$$

R : interpolation polynomial. ~~$R(x_i)$~~ $R(x_i) = y_i$ $\rightarrow$ $deg(R) < n$.

3. for $i \in \{1, -, n\}$.

$$\Lambda(x_i) y_i = \Lambda(x_i) w(x_i).$$ $\rightarrow$ n equations.

$$\Lambda = \sum_{i=0}^{e} \lambda_i X^i \quad , \quad W = \sum_{i=0}^{K-1} W_i X^i$$

~~$\Lambda(x_i) y_i =$~~ ~~$\lambda_0 w_0 + (\lambda_1 w_0$~~

let $\underline{O}(X) = \Lambda(X) w(X)$.

unknown : $(\lambda_0, -, \lambda_{\bar{e}-1})$
$(W_0, -, W_{k-1})$

$\Lambda(x_i) y_i = \underline{O}(x_i)$ $\rightarrow$ n equations

unknown $\begin{cases} (W_0, — W_{e+k-2}) \\ (\lambda_0, — \lambda_{n-k/2}). \end{cases}$ $deg(O(x)) \le \frac{e+k-\cancel{2}^{3}}{2}$ $\left\lfloor \frac{n+k}{2} \right\rfloor$ unknowns.

sum of degree of two polynomials.

we need more equations than unknown to able to solve system.

$$\frac{n-k}{2} + \frac{n-k-3}{2} = n-k - 3/2.$$

unknowns, which is still smaller than n.

let's go over again

$$\Lambda(x_i)y_i = \underbrace{\Lambda(x_i)W(x_i)}_{Q(x_i)} \quad n \text{ quadratic equations}$$

ℓ unknown $\begin{cases} (\lambda_0 - \lambda_{e-1}) & e \\ (W_0 - W_{k-1}) & k \end{cases}$

let $Q(x) = \Lambda(x)W(x)$

$\cancel{\deg(Q)}$ $\deg(Q(x)) \cancel{k} < e+k$

unknowns $\left.\begin{cases} (\lambda_0 - \lambda_{e-1}) \\ (W_0 - W_{e+k-1}) \end{cases}\right\}$ $e + e + k = 2e + k$

$$\Lambda(x) = \begin{bmatrix} 1 & x_1 & \cdots & x_1^{e-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{e-1} \end{bmatrix} \begin{bmatrix} \lambda_0 \\ \vdots \\ \lambda_{e-1} \end{bmatrix} = \begin{bmatrix} \Lambda(x_0) \\ \vdots \\ \Lambda(x_n) \end{bmatrix}$$

$$D(y) = \begin{pmatrix} y_0 & & & 0 \\ & y_1 & & \\ & & \ddots & \\ 0 & & & y_n \end{pmatrix}$$

$$D(y) \cdot \Lambda(x) = \begin{bmatrix} \Lambda(x_0)y_0 \\ \vdots \\ \Lambda(x_n)y_n \end{bmatrix}$$