lec 14

Error Correction : Berlekamp-Welch

Def: Add redundancy to our data so that if data gets corrupted, we can then recover the original data.

Two extrems

① For every bit, repeat it 100 times →
if majority is 0 → 0
〃 〃 〃 1 → 1

② For every 4 bits, we just send one extra bit

	# of 1's	add
1101	3	$\boxed{1}1101$
0011	2	$\boxed{0}0011$

add

---

plaintext ≡ Messege

Encryption fun ≡ Encoding Map ⟶ $\Sigma^{k} \xrightarrow{k<n} \Sigma^{n}$

Decryption fun ≡ Decoding Map

Ciphertext ≡ Codeword

Adversary ≡ Jammer

Corrupted info ≡ Noisy data

Corrupted channel ≡ Noisy channel

k: dimention

n: block length

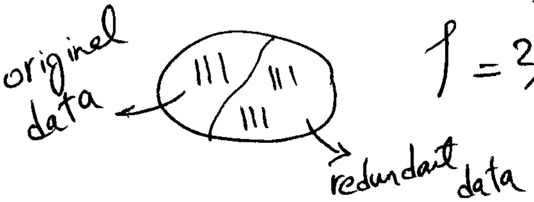
Σ: alphabet

$|\Sigma|$: q $0,1 \rightarrow q=2$

$\text{Rate} = \frac{k}{n}$ $10 \rightarrow 30$

$R = 1/3$

$f = 2/3$



Berlekamp_Welch Alg

Setting: Alice wishes to communicate with Bob over a noisy channel. Her message is $m_1 \dots m_t$.

problem: is that some messages are corrupted during transmission due to channel noise.

active adv. setting in our secret sharing protocols

#So, Bob receives exactly as many messages as Alice transmits. However, k of them are corrupted. Assuming that Bob has no idea which "k".

$f(x) \longrightarrow$ original SS poly $\in \mathbb{Z}_q[x] \longrightarrow deg = t-1$

shares/messages $\longrightarrow f(1) = m_1, \dots, f(t) = m_t$

#To guard against "k" general errors, Alice must transmit "2k" additional messages.

$m_1, m_2, \dots m_{t+2k} \longrightarrow m_i = f(i)$ for $1 \leqslant i \leqslant t+2K$

we know "t+k" of these messages/shares are uncorrupted

$$\underbrace{t \quad k}_{\text{uncorrupted}} \quad \underbrace{k}_{\text{corrupted}}$$

Example:

1	2	3	4
3	1	5	0
m_1	m_2	m_3	m_4

Alice

$\longrightarrow$

1	2	3	4	5	6
3	1	5	0	6	1

message with redundancy

1	2	3	4	5	6
2	1	5	0	6	1
X					

$\longrightarrow$ $t=4, deg=3$

$k=1 \longrightarrow 2k+t=6$

From Bob's viewpoint: he has to reconstruct the poly $f(x)$ from "$t+2k$" shares $f(1), f(2), \dots, f(t+2k)$.

Bob is given $t+2k$ shares with the assumption that there is a poly of degree $t-1 \in \mathbb{Z}_q[x]$ where

① $g(i) = f(i)$ for "$t+k$" points

$1 \leqslant i \leqslant t+2k$

② let $e_1, \dots e_k$ be the "k" locations at which errors occurred. As a result: $f(e_i) \neq g(e_i)$ for $1 \leqslant i \leqslant k$.

Consider an error-locater poly $E(x) = (x-e_1)(x-e_2)\cdots(x-e_k)$

$\searrow$ $\deg = k$

Beatiful observation $\longrightarrow$ $\boxed{f(i)E(i) = g(i)E(i)} \longrightarrow$?

$1 \leqslant i \leqslant n+2k$

ⓐ At point "i" which no error occured since $f(i) = g(i)$

ⓑ At point "i" which an error occured since $E(i) = 0$

$$E(x) = \overset{\boxed{1}}{()}x^k + b_{k-1}x^{k-1} + b_{k-2}x^{k-2} + \cdots + b_0$$

$$Q(x) = a_{t+k-1}x^{t+k-1} + a_{t+k-2}x^{t+k-2} + \cdots + a_0$$

$$f(x)\,E(x) = Q(x)$$

$f(x)$: deg: $t-1$; $E(x)$: deg: k; $Q(x)$: deg: $t+k-1$

$\longrightarrow$ I can construct a linear system of equations & find the locations of errors.

Example of Berlekamp-Welch Alg.

$$f(x) = x^2 + x + 1 \longrightarrow (1,3),\ (2,0),\ (3,6),\ (4,0),\ (5,3)$$

$\boxed{\mathbb{Z}_7}$

$$\left.\begin{array}{l} deg = t-1 = 2 \longrightarrow t = 3 \\ K = 1 \end{array}\right\} \longrightarrow 2K+t \text{ shares} = 2+3 = \underline{5}$$

$\downarrow$

VSS # of you want to tolerate 't' errors

$K=t \longrightarrow 2(t)+t = 3t$ shares must be generated

$$\underbrace{\boxed{3}\ \boxed{0}\ \boxed{6}\ \boxed{0}\ \boxed{3}}_{f(x)} \longrightarrow \underbrace{\overset{\times 1}{\boxed{2}}\ \overset{2}{\boxed{0}}\ \overset{3}{\boxed{6}}\ \overset{4}{\boxed{0}}\ \overset{5}{\boxed{3}}}_{g(x)} \quad t < n/3$$

$$Q(x) = f(x) * E(x) \longrightarrow Q(x) = g(x) * E(x)$$

$$Q(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \longrightarrow deg = 3 = \underset{3}{t} + \underset{1}{K} - 1$$

$$E(x) = b_0 + \underset{1}{x} \longrightarrow deg = 1 = K$$

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 = g(x)\,(b_0 + x) \longrightarrow 5 \text{ equations with } 5 \text{ unknowns } a_0, a_1, a_2, a_3, b_0$$

$$\left.\begin{array}{l} x=1 \\ g(1)=2 \end{array}\right\} \rightarrow a_0 + a_1 + a_2 + a_3 = 2\,(b_0+1) \rightarrow a_3 + a_2 + a_1 + a_0 + 5b_0 = 2 \quad (\text{Mod } 7)$$

$$(2,0) \longrightarrow a_3 + 4a_2 + 2a_1 + a_0 = 0 \quad (\text{Mod } 7)$$

$$(3,6) \longrightarrow 6a_3 + 2a_2 + 3a_1 + a_0 + b_0 = 4 \quad \text{"}$$

$$(4,0) \longrightarrow a_3 + 2a_2 + 4a_1 + a_0 = 0 \quad \text{"}$$

$$(5,3) \longrightarrow 6a_3 + 4a_2 + 5a_1 + a_0 + 4b_0 = 1 \quad \text{"}$$

Find $\underline{b_0}$ by <u>cramer's rule</u> by two determinant $\longrightarrow b_0 = -1 \longrightarrow e_1 = 1$

$$E(x) = (x - e_1)$$

$$\boxed{a_3 = 1,\ a_2 = 0,\ a_1 = 0,\ a_0 = 6} \rightarrow Q(x) = x^3 + 6 \xrightarrow{\text{location of errors}} f(x) = \frac{Q(x)}{E(x)} = \frac{x^3+6}{x-1} = x^2 + x + 1$$